Abgeordnetenhaus BERLIN

Drucksache 19/0859
01.02.2023

19. Wahlperiode

Vorlage – zur Kenntnisnahme –

Stellungnahme des Senats zum Bericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2021

Der Senat von Berlin
SenInnDS – I AbtL 1
Tel. (9223) 2066

An das
Abgeordnetenhaus von Berlin

über Senatskanzlei G Sen

V o r l a g e
des Senats von Berlin
- zur Kenntnisnahme -

über Stellungnahme des Senats zum Bericht der Berliner Beauftragten für Datenschutz und Informationsfreiheit für das Jahr 2021

Der Senat legt nachstehende Vorlage dem Abgeordnetenhaus zur Besprechung vor:

Nach § 12 Abs. 1 Berliner Datenschutzgesetz sowie § 18 Abs. 3 Berliner Informationsfreiheitsgesetzes erstattet die Beauftragte für Datenschutz und Informationsfreiheit dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis ihrer Tätigkeit. Der Senat hat dazu nach § 12 Abs. 2 des Berliner Datenschutzgesetzes eine Stellungnahme herbeizuführen und legt diese hiermit dem Abgeordnetenhaus vor.

Berlin, den 24. Januar 2023

Der Senat von Berlin

Franziska Giffey

Regierende Bürgermeisterin

Iris Spranger

Senatorin für Inneres, Digitalisierung und Sport

Stellungnahme des Senats

zum Bericht der

Berliner Beauftragten für

Datenschutz und

Informationsfreiheit

für das

Jahr 2021

(nach § 12 Abs.2 Berliner Datenschutzgesetz)

Inhaltsverzeichnis

Vorwort

Das Jahr 2021 war in vielerlei Hinsicht eine Fortsetzung des Jahres 2020. Während wir jedoch 2020 von der Corona-Pandemie und ihren Auswirkungen auf die Gesellschaft überrascht wurden, trat 2021 eine weitgehende Gewöhnung an den Ausnahmezustand ein. Anfänglich als Übergangslösungen gedachte Maßnahmen, wie z. B. das Arbeiten von zu Hause aus, die Durchführung von Videokonferenzen oder das Unterrichten unserer Kinder im „Homeschooling“, verstetigten sich und wurden zum selbstverständlichen Bestandteil unseres Alltags. Schnell wurde deutlich, dass die neue gesellschaftliche Realität viele Bezugspunkte zum Datenschutz hat. Mit der zunehmenden Digitalisierung der gesellschaftlichen Prozesse haben sich auch vielfältige Möglichkeiten eröffnet, die Menschen – oftmals unbemerkt – bis in den Kernbereich ihrer privaten Lebensgestaltung hinein auszuforschen. Private, unbeobachtete Bereiche sind jedoch Grundvoraussetzung für die freie Entfaltung der Persönlichkeit und somit für eine demokratisch aufgestellte und den Grundrechten verpflichtete Gesellschaft.

Einige der Probleme wurden bereits letztes Jahr angegangen und konnten in diesem Jahr abschließend geklärt werden. Ein gutes Beispiel dafür ist der Einsatz digitaler Lehr- und Lernmittel in den Berliner Schulen. Lange Zeit stand dieser in Ermangelung von datenschutzkonformen Regelungen im Schulgesetz auf äußerst wackeligen Füßen. Mit den von uns vorgeschlagenen Änderungen enthält das Gesetz jetzt eine Rechtsgrundlage, die die Verarbeitung personenbezogener Daten von Schüler:innen und Lehrkräften beim Einsatz digitaler Lehr- und Lernmittel explizit erlaubt. Für die Schulen wurde damit endlich die nötige Rechtssicherheit geschaffen. Eine weitere Entlastung haben die Schulen dadurch erfahren, dass die Zuständigkeit für die (Vor-) Auswahl von datenschutzgerechten digitalen Werkzeugen nunmehr zentral durch die Senatsverwaltung für Bildung erfolgt. Damit verfügt Berlin im Bundesvergleich nunmehr über eines der modernsten Schulgesetze, das den digitalen Unterricht datenschutzgerecht ermöglicht.

Beim Einsatz von Videokonferenzsystemen konnten wir ebenfalls einige Verbesserungen verzeichnen. Wir haben unsere Hinweise dazu überarbeitet und unsere Unterstützung für Verantwortliche bei der Auswahl datenschutzkonformer Dienste weiter ausgebaut. Bei manchen Anbieter:innen konnten wir so

datenschutzrechtliche Fortschritte erzielen. Gleichzeitig mussten wir jedoch ausgerechnet in der öffentlichen Verwaltung erhebliche Rechtsverstöße bei der Nutzung von Videokonferenzsystemen feststellen. Gerade die öffentliche Verwaltung sollte sich hier ihrer Vorreiterinnenrolle bewusst sein und in besonderem Maße auf die Einhaltung datenschutzrechtlicher Regeln achten.

Das Vertrauen der Bürger:innen in die öffentliche Verwaltung ist maßgeblich abhängig von der Transparenz ihres Handelns. Dafür muss sich die Verwaltung weiter öffnen. Vor diesem Hintergrund haben wir uns stark dafür eingesetzt, dass das veraltete Berliner Informationsfreiheitsgesetz modernisiert wird. Die Vorlage eines Entwurfs für ein Berliner Transparenzgesetz auf Arbeitsebene wurde von uns dementsprechend zunächst ausdrücklich begrüßt. Nachdem im Gesetzgebungsverfahren, entgegen der von uns geübten Kritik, umfangreiche Bereichsausnahmen eingebracht wurden, haben wir es nicht bedauert, dass der Gesetzentwurf kurz vor Ende der Legislaturperiode im Abgeordnetenhaus gescheitert ist. Wir hoffen, dass das Vorhaben zeitnah erneut aufgegriffen und vom Gesetzgeber in einem Transparenzgesetz umfassende Regelungen für eine moderne und transparente Verwaltung geschaffen werden.

In seiner Schrems II-Entscheidung hat der Europäische Gerichtshof festgestellt, dass personenbezogene Daten von EU-Bürger:innen nicht mehr auf Basis des „EU-US Privacy Shield“ in die USA übermittelt werden können. Für die Nutzung von Standarddatenschutzklauseln als Grundlage für Datenübermittlungen hat er zudem hohe Anforderungen gestellt. Ein Jahr nach diesem wegweisenden Urteil haben wir im Rahmen einer länderübergreifenden Kontrolle Datenübermittlungen durch Unternehmen in Staaten außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums überprüft. Dabei mussten wir feststellen, dass zahlreiche Unternehmen selbst die grundlegenden Anforderungen aus der Schrems II-Entscheidung immer noch nicht umgesetzt haben. Wir sind davon überzeugt, dass dies in vielen Fällen in einem kooperativen Dialog mit den betreffenden Unternehmen nachgeholt werden kann. Dort wo dies jedoch nicht möglich ist, werden wir über kurz oder lang mit den uns zur Verfügung stehenden aufsichtsbehördlichen Maßnahmen reagieren müssen.

Unser ganz besonderes Anliegen ist es, Kinder und Jugendliche frühzeitig für die elementare Bedeutung des Datenschutzes zu sensibilisieren und ihnen die

erforderlichen Kenntnisse und Kompetenzen zum Schutz ihrer Person in der digitalen Welt zu vermitteln. Wir haben daher unser medienpädagogisches Angebot erweitert. Für Grundschulen bieten wir z. B. ein neues Workshop-Format als Unterrichtseinheit an. Darin können die Schüler:innen spielerisch entdecken, was personenbezogene Daten sind, warum und durch wen sie verarbeitet werden, wieso sie schützenswert sind und insbesondere, wie sie sich sicher im Internet bewegen können. Die große Nachfrage hat uns gezeigt, dass in den Schulen ein großes Bedürfnis besteht, Kinder medienpädagogisch über die Gefahren und ihre Rechte im digitalen Zeitalter aufzuklären.

Angesichts einer zunehmenden Digitalisierung unserer Gesellschaft – die pandemiebedingt nochmals einen immensen Schub erfahren hat – sind viele der davon Betroffenen verunsichert. Oftmals ist der gesellschaftliche Transformationsprozess, in dem wir uns befinden, auch mit der Angst vor Veränderungen besetzt. Dass sich viele Bürger:innen angesichts dessen auch verstärkt Gedanken über den Schutz ihrer persönlichen Daten machen, zeigt die hohe Anzahl an Beratungsersuchen und Beschwerden, die uns auch dieses Jahr wieder erreicht hat. Dabei kann das Neue auch eine Chance für mehr Partizipation, Inklusion und Transparenz sein. Um hier die nötige Akzeptanz bei den Betroffenen herzustellen, muss der Datenschutz bei der Umsetzung von Digitalisierungsprojekten unbedingt von Anfang an mitgedacht werden.

Berlin, im Mai 2022
Volker Brozio
Kommissarischer Dienststellenleiter

1 Schwerpunkte

1.1 Internationaler Datenverkehr ein Jahr nach „Schrems II“

Ein Jahr nach dem Urteil „Schrems II“ des Europäischen Gerichtshofs (EuGH)[1] zeigt ein von uns gemeinsam mit anderen Aufsichtsbehörden eingeholtes Rechtsgutachten, dass die meisten der bisher üblichen Datenexporte in die USA nicht mehr zulässig sind – und dass der Einsatz US-verflochtener Dienstleister:innen sogar dann kritisch ist, wenn diese die Daten in Europa verarbeiten. Diverse von uns geführte Einzelverfahren wie auch eine konzertierte Prüfung vieler deutscher Aufsichtsbehörden zeigen, dass zahlreiche Unternehmen sogar die offensichtlichen Anforderungen des Urteils immer noch nicht umgesetzt haben.

Mit seinem Urteil hatte der EuGH den Beschluss der EU-Kommission für ungültig erklärt, nach dem die Regelungen des „Privacy Shield“ die Übermittlung personenbezogener Daten in die USA erlaubten. Für die Nutzung von Standardvertragsklauseln hatte der EuGH hohe Anforderungen aufgestellt.[2]

a) Prüfungen von Amts wegen und aufgrund von Beschwerden sowie Beratungen

Nach dem „Schrems II“-Urteil erreichten uns vermehrt Beschwerden und Hinweise über unzulässige Datenexporte. Darüber hinaus haben wir das Thema auch proaktiv bearbeitet.

Ein wichtiger Gegenstand unserer Beratungen mit der BVG in Sachen „Jelbi“[3] und „Check-In-Check-Out-App“[4] waren bspw. internationale Datenflüsse und der Einsatz US-verflochtener Dienstleister:innen. Der BVG gelang es nicht darzulegen, wie diesbezügliche Datenverarbeitungen rechtmäßig erfolgen sollen. Denn die einbezogenen Dienstleister:innen müssen zu ihrer Aufgabenerfüllung die anfallenden personenbezogenen Daten im Klartext verarbeiten. Dass in diesem Fall keine technischen Maßnahmen bestehen, die den unzulässigen Zugriff von US-Behörden auf die Daten ausschließen, hatten wir bereits berichtet.[5] Die BVG hatte zwar den Einsatz besonders abgeschotteter Hardware[6] in Betracht

[1] EuGH, Urteil vom 16. Juli 2020 – C-311/18, „Schrems II“
[2] Siehe JB 2020, 1.2
[3] Siehe auch 11.1
[4] Siehe auch 11.2
[5] JB 2020, 1.2
[6] Sog. Nitro Enclaves

gezogen, der grds. eine sinnvolle technische Sicherheitsmaßnahme sein kann. Jedoch kann hierdurch ein Zugriff von Dienstleister:innen und damit eine Zugriffsmöglichkeit der US-Behörden nicht ausgeschlossen werden.

Wir haben uns zudem an einer länderübergreifenden Prüfaktion der deutschen Aufsichtsbehörden zur Umsetzung des „Schrems II"-Urteils beteiligt.[7] Hierfür haben wir rund 900 Berliner Unternehmen hinsichtlich möglicher Datenexporte in Staaten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums (Drittländer) einer automatisierten Vorprüfung unterzogen. Über achtzig Unternehmen haben wir dann auf Basis der Erkenntnisse aus der Vorprüfung um Stellungnahme gebeten, weil wir Hinweise auf unzulässige Datenexporte gefunden hatten. Der von uns dabei verwendete Fragenkatalog orientierte sich an dem länderübergreifend abgestimmten, im Internet veröffentlichten Fragenkatalog[8].

Im Rahmen der von uns geführten Verfahren mussten wir regelmäßig feststellen, dass den Unternehmen überhaupt nicht bewusst war, dass auch reine Support- oder Administrations-Zugriffe oder kurzzeitige Entschlüsselungen[9] rechtfertigungsbedürftige Datenexporte darstellen.

b) Gutachten zur Rechtslage in den USA — Auswirkungen auf Datenverarbeitungen in der EU

Im „Schrems II"-Urteil hat der EuGH die Rechtslage in den USA bereits sehr umfangreich geprüft. Dennoch blieben einige Fragen offen, insbesondere hinsichtlich Unternehmen, die keine klassischen IT-Dienstleister:innen sind. Gemeinsam mit den deutschen Aufsichtsbehörden haben wir ein Rechtsgutachten bei Professor Stephen I. Vladeck, University of Texas at Austin, in Auftrag gegeben. Professor Vladeck ist renommierter Kenner des US-amerikanischen Geheimdienstrechts und hatte im „Schrems II"-Verfahren bereits ein Rechtsgutachten für Facebook erstellt. Einige zentrale Befunde aus seinem Gutachten[10] seien hier herausgegriffen:

- Das nach dem „Schrems II"-Urteil des EuGH nicht mit den europäischen Grundrechten ver-

[7] Siehe auch Pressemitteilung vom 1. Juni 2021; https://www.datenschutz-berlin.de/fileadmin/ user_upload/pdf/pressemitteilungen/2021/20210601-PM-Schrems_II_Pruefung.pdf

[8] Siehe bspw. unter https://datenschutz-hamburg.de/pages/fragebogenaktion/

[9] Wie etwa bei Diensten zur Erkennung und Abwehr von Angriffen auf Webseiten und Content Delivery Networks (CDN)

[10] Stephen I. Vladeck, „Memo on Current State of U.S. Surveillance Law and Authorities", abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/datenexporte

einbare US-Recht betrifft sehr viele Unternehmen. Denn unter den insoweit relevanten Begriff „electronic communication service provider“ fallen nicht nur klassische IT- und Telekommunikationsunternehmen, sondern bspw. auch Banken, Fluggesellschaften, Hotels oder Versanddienstleister:innen. Zudem ist es in manchen Unterkategorien dieses Begriffs nicht einmal erforderlich, dass die Dienste der Öffentlichkeit zur Verfügung gestellt werden, sondern es kann bspw. genügen, dass ein Unternehmen seinen Mitarbeitenden einen E-Mail-Dienst bereitstellt. Der Begriff umfasst auch Anbieter:innen von „remote computing services“, also klassischen Cloud-, Rechen- oder Hosting-Dienstleistungen, und nicht nur herkömmliche Telekommunikationsanbieter:innen.

- Auch wenn ein Unternehmen nur hinsichtlich ganz weniger oder gar nur eines einzelnen Dienstes (etwa E-Mail-Dienst für Mitarbeitende) als „electronic communication service provider“ anzusehen ist, sind die Zugriffsrechte der US-Behörden nicht auf Daten im Zusammenhang mit diesem Dienst beschränkt. Vielmehr „infiziert“ eine auch noch so geringfügige Einordnung als „electronic communication service provider“ sämtliche Daten des Unternehmens, auch wenn dieser Kommunikationsdienst gar nichts mit der eigentlichen unternehmerischen Tätigkeit zu tun hat.

- Nutzt ein selbst nicht als „electronic communication service provider“ anzusehendes Unternehmen Dienste eines „electronic communication service providers“, dann unterliegen die dortigen Daten dem Zugriff der US-Behörden.

- Das nach der Bewertung des EuGH problematische US-Recht[11] greift nicht nur ein, wenn Daten in den USA verarbeitet werden, sondern auch dann, wenn US-Unternehmen oder ihre Tochtergesellschaften Daten außerhalb der USA verarbeiten – etwa in Europa. Das US-Recht ist insoweit extraterritorial anwendbar. US-Unternehmen können sich nicht damit verteidigen, dass die Herausgabe der Daten nach der Datenschutz-Grundverordnung (DS-GVO) unzulässig ist.

- Auch europäische Unternehmen, die in den USA aktiv sind, können dem problematischen US-

[11] Insoweit ist von besonderer Bedeutung Section 702 des US-amerikanischen Foreign Intelligence Surveillance Act of 1978 (FISA), zugleich 50 U.S. Code §§ 1881, 1881a, weil hierüber Unternehmen und Beschäftigte zur Herausgabe von Daten gezwungen werden können.

Recht unterfallen. Dies gilt aber wohl nicht für Muttergesellschaften, die nicht selbst, sondern nur durch ihre Tochtergesellschaften in den USA aktiv sind.

c) Empfehlungen des Europäischen Datenschutzausschusses (EDSA) zu ergänzenden Schutzmaßnahmen bei Datenexporten

Wie bereits im letzten Jahr berichtet,[12] hat der EDSA Empfehlungen erarbeitet, wie Verantwortliche und Auftragsverarbeiter:innen, die personenbezogene Daten in Drittländer übermitteln wollen, vorgehen sollten. Auch an der Überarbeitung dieser Empfehlungen nach öffentlicher Konsultation haben wir uns beteiligt. Die Empfehlungen, die detailliert auf die neuen Standardvertragsklauseln der EU-Kommission[13] abgestimmt sind, liegen nunmehr in finaler Version 2.0 vor.[14]

Die finale Version enthält im Wesentlichen nur Klarstellungen ggü. der zur öffentlichen Konsultation gestellten Version 1.0. Insbesondere hat der EDSA – in Übereinstimmung mit der Rechtsprechung des EuGH – den sog. risikobasierten Ansatz[15] für Datenexporte nochmals ausdrücklich abgelehnt.

Die Version 2.0 der Empfehlungen behandelt auch den Fall, dass die Rechtslage im Drittland unklar ist.[16] In diesem Fall kann sich nach ordnungsgemäßer Prüfung die Situation ergeben, dass keine ergänzenden Schutzmaßnahmen erforderlich sind. Bedingung hierfür ist, dass die/der Datenexporteur:in mittels eines detaillierten Berichts nachweisen kann, dass das Recht des Drittlandes weder so ausgelegt noch in der Praxis so angewandt wird, dass es die jeweiligen Daten und/oder die jeweiligen Empfänger:innen betrifft. Es kommt hier also nicht nur auf die Anwendung in der Praxis an, sondern zusätzlich auch auf die Auslegung des unklaren Rechts. Nur dass problematisches Recht in der Praxis nicht angewandt wird, genügt nicht für das Eingreifen dieser Ausnahmeregelung. Es ist folgerichtig nicht ausreichend, darauf abzustellen, dass das problematische Recht auf kein einziges vergleichbares Unternehmen und kein einziges vergleichbares Datum je ange-

[12] JB 2020, 1.2
[13] Siehe 1.1.d
[14] EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, abrufbar unter https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de
[15] Bei einem risikobasierten Ansatz werden Eintrittswahrscheinlichkeit und drohender Schaden bewertet, um dann ein gewisses Niveau an Risiken zu akzeptieren, ab einer gewissen Risikobewertung weitere Schutzmaßnahmen vorzusehen und zu hohe Risiken nicht zu akzeptieren, sondern die Datenverarbeitung zu unterlassen.
[16] EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Rn. 43.3

wandt wurde. Vielmehr muss diese Nichtanwendung Folge des Umstandes sein, dass das Recht des Drittlandes so ausgelegt wird, dass es nicht auf die in Rede stehenden Unternehmen und Daten anwendbar ist.

Im besonders praxisrelevanten Fall USA ist zu beachten, dass das US-Recht zum Teil nicht den europäischen Grundrechtsstandards genügt. Für eine Berücksichtigung der Praxis ist aber kein Raum, wenn bereits die Rechtslage defizitär ist. Darüber hinaus ermöglicht das US-Recht in vielen praxisrelevanten Fällen nicht, präzise Aussagen zum Vorliegen oder Nichtvorliegen von Zugriffen der Behörden zu machen. In solchen Fällen kann die praktische Erfahrung des Datenimporteurs nicht berücksichtigt werden.[17]

d) Neue Standardvertragsklauseln

Im Juni hat die EU-Kommission neue Standardvertragsklauseln beschlossen. Es gibt nunmehr ein einziges umfassendes Set von Standardvertragsklauseln für Datenexporte in Drittländer.[18] Diese umfassen anders als die alten Standardvertragsklauseln auch die Regelungen zur Auftragsverarbeitung und sind insoweit zwingend, wenn eine Rechtfertigung des Datenexports über die Standardvertragsklauseln erfolgt. Darüber hinaus gibt es Standardvertragsklauseln für Auftragsverarbeitungsverträge innerhalb des EWR,[19] deren Nutzung freigestellt ist. Die neuen Standardvertragsklauseln greifen unter anderem das „Schrems II"-Urteil des EuGH auf und sind detailliert abgestimmt auf die Empfehlungen des EDSA zu ergänzenden Schutzmaßnahmen.[20] Die nach der Rechtsprechung des EuGH erforderlichen Prüfungen und ergänzenden Schutzmaßnahmen sind nun ausdrücklich in den Standardvertragsklauseln geregelt.[21]

In der Praxis ist zu beachten, dass andere Vereinbarungen der Parteien in keinem Fall unmittelbar oder mittelbar im Widerspruch zu den Standardvertrags-

[17] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Rn. 47

[18] Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, C/2021/3972, ABl. L 199 vom 7. Juni 2021, S. 31–61

[19] Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Abs. 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Abs. 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates, C/2021/3701, ABl. L 199 vom 7. Juni 2021, S. 18–30

[20] Siehe 1.1.c

[21] Klausel 14 der Datenexport-Standardvertragsklauseln, Anhang zum Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, C/2021/3972, ABl. L 199 vom 7. Juni 2021, S. 31–61

klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden dürfen.[22] Ein solcher Widerspruch kann bspw. auch dann vorliegen, wenn durch Vergütungsregelungen die effektive Wirkung von Pflichten und Rechten aus den Standardvertragsklauseln gefährdet wird. Derartige zunächst rein wirtschaftliche Vereinbarungen ohne datenschutzrechtlichen Bezug können so indirekt Verstöße gegen das Datenschutzrecht hervorrufen. Hier ist stets eine Einzelfallprüfung erforderlich. Pauschale Vergütungsregelungen für sämtliche Leistungen von Auftragsverarbeiter:innen dürften allerdings unzulässig sein, weil dadurch bspw. auch solche Kontrollen[23] kostenpflichtig würden, die nur deswegen erforderlich sind, weil Auftragsverarbeiter:innen gegen datenschutzrechtliche Verpflichtungen verstoßen haben. Hierdurch könnten Verantwortliche daran gehindert werden, datenschutzrechtlich zwingend erforderliche Kontrollen durchzuführen. Entsprechendes gilt für weitere Unterstützungspflichten.

Übermittlungen personenbezogener Daten in Drittländer ohne von der EU-Kommission attestiertes angemessenes Datenschutzniveau bleiben auch mit den neuen Standardvertragsklauseln eine Herausforderung. Die erforderliche Prüfung der Rechtslage und Praxis in dem betreffenden Drittland beschränkt sich zwar auf den konkreten Datentransfer, muss aber insoweit umfassend sein. Oftmals wird der damit verbundene Aufwand außer Verhältnis zu dem Nutzen des Datenexports stehen. Gerade im Bereich der Nutzung von IT-Dienstleistungen ist der pragmatische Weg daher ein Verzicht auf Datenexporte in nicht als sicher anerkannte Drittländer. Für den Fall USA ist dies meist sogar die einzige rechtskonforme Lösung, da die Rechtslage höchstrichterlich festgestellt unzureichend ist und ergänzende Schutzmaßnahmen nur in wenigen Ausnahmefällen in Betracht kommen. Verantwortliche, die personenbezogene Daten unzulässig in Drittländer übermitteln – sei es direkt oder durch Dienstleister:innen oder deren Subunternehmer:innen – müssen die Datenexporte sofort beenden und übermittelte Daten zurückholen. Verstöße können nicht nur Anordnungen nach sich

[22] Klausel 2 a) der Datenexport-Standardvertragsklauseln, Anhang zum Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, C/2021/3972, ABl. L 199 vom 7. Juni 2021, S. 31–61; Klausel 2a) der Auftragsverarbeitungs-Standardvertragsklauseln, Anhang zum Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Abs. 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Abs. 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates, C/2021/3701, ABl. L 199 vom 7. Juni 2021, S. 18–30

[23] Siehe Art. 28 Abs. 3 UAbs. 1 lit. h DS-GVO

ziehen, die den Geschäftsbetrieb vor erhebliche Probleme stellen können, sondern auch hohe Bußgelder. Darüber hinaus ergeben sich aus der extraterritorialen Anwendbarkeit des US-amerikanischen Überwachungsrechts vergleichbare Probleme, wenn US-Unternehmen, Tochtergesellschaften von US-Unternehmen oder sonstige in den USA tätige Unternehmen IT-Dienstleistungen in Europa anbieten.

1.2 Digitalisierung der Schulen — Fortsetzung

Im vergangenen Jahr haben wir ausführlich über die Defizite im Bereich der Digitalisierung der Schulen berichtet.[24] Auch in diesem Jahr waren wir wieder mit diesem Thema befasst. Trotz einiger Verbesserungen ist das Ziel einer datenschutzgerechten Digitalisierung der Schulen noch weit entfernt.

Mit der Digitalisierungsstrategie liegt ein konkreter Zeitplan seit August 2021 vor.

Bis weit in das Frühjahr hinein wurden die Schüler:innen zu einem überwiegenden Teil ausschließlich im schulisch angeleiteten Lernen zu Hause (saLzH) unterrichtet. Neben den gravierenden Auswirkungen des fehlenden Präsenzunterrichts auf die Entwicklung der Schüler:innen zeigte sich deutlich, dass es auch nach vielen Monaten der Pandemie nicht gelungen war, flächendeckend funktionierende und dem geltenden Recht entsprechende digitale Infrastrukturen bereitzustellen und den Schulen rechtssichere Softwarelösungen zum effektiven Distanzlernen zur Verfügung zu stellen. Wir haben unsere intensiven Beratungen von Schulleitungen, Lehrkräften und Eltern auch in diesem Jahr fortgesetzt. Auch haben wir der Bildungsverwaltung immer wieder unsere Unterstützung angeboten, die jedoch leider nicht immer angenommen worden ist. In der für die Schulen schwierigen Zeit der Pandemie sind wir unserer Aufsichtstätigkeit mit Bedacht nachgegangen und haben auf durchgreifende Maßnahmen weitestgehend verzichtet. Der temporäre Verzicht auf Aufsichtsmaßnahmen gegen den Einsatz nicht datenschutzkonformer Lösungen darf jedoch nicht dazu führen, dass sich dieser verstetigt. Wir haben daher die Erwartung, dass die Schulen, sofern nicht schon geschehen, umgehend einen Wechsel zu datenschutzkonformen Lösungen und Konfigurationen vollziehen.

Die Senatsverwaltung für Bildung, Jugend und Familie kann diesen Aspekt nicht nachvollziehen. Vielmehr ist es so, dass die Stabsstelle auf die Berliner Beauftragten für Datenschutz und Informationsfreiheit zugegangen ist, um u.a. Datenschutzfragen zu unterschiedlichen Projekten zu klären und um sich Rat einzuholen.

Das digitale Angebot, das zentral durch die Senatsverwaltung für Bildung, Jugend und Familie zur Verfügung gestellt wird, wird immer attraktiver, so dass von einem Wechsel der Schulen auszugehen ist.

Wir haben öffentlich sehr deutlich darauf hingewiesen[25], dass die einzelnen Schulen als die nach dem Berliner Schulgesetz (SchulG) datenschutzrechtlich

[24] JB 2020, 1.4

[25] Pressemitteilung vom 22. Januar 2021; siehe https://www.datenschutz-berlin.de/ fileadmin/user_upload/pdf/pressemitteilungen/2021/20210122-PM-Digitaler_Unterricht_ Missstaende_beheben.pdf

Verantwortlichen allein nicht in der Lage sind, für jedes einzusetzende Produkt eine umfassende Prüfung der Einhaltung aller datenschutzrechtlichen Anforderungen und eine Bewertung der Sicherheit der Daten vorzunehmen. Wir sehen die Bildungsverwaltung in der Pflicht, diese Aufgabe zu übernehmen und die Schulen zu unterstützen, um bei diesen für Rechtssicherheit zu sorgen. Die Schulen sind mit den notwendigen Überprüfungen der eingesetzten Werkzeuge überfordert, da es eben gerade nicht nur um die Bewertung der pädagogischen Eignung digitaler Lehrmittel geht, sondern darüber hinaus eine Prüfung komplexer datenschutzrechtlicher Sachverhalte erforderlich ist. Schulleitungen und Lehrkräfte sind hierfür weder ausgebildet, noch verfügen sie über die notwendigen zeitlichen Ressourcen. Es bedarf der Festlegung von Mindeststandards für den Einsatz digitaler Lehr- und Lernmittel und einer Vorauswahl an pädagogisch geeigneten und rechtmäßig einzusetzenden digitalen Diensten und Produkten durch die Bildungsverwaltung. Wir haben darauf gedrängt, eine solche Aufgabe der Bildungsverwaltung auch schulgesetzlich zu verankern, um die notwendige Verbindlichkeit zu erreichen. Sehr erfreulich ist, dass der Gesetzgeber unsere Anregungen aufgenommen und kurz vor Ende der Legislaturperiode wichtige Weichenstellungen für einen datenschutzgerechten digitalen Schulunterricht vorgenommen hat.[26] Nun ist es an der Schulverwaltung, diesen gesetzlichen Anforderungen nachzukommen.

Der Doppelhaushalt 2022/2023 wurde im Sommer verabschiedet. Um dem Erfordernis des Digitalisierungsfortschritts näher zu treten, wurden zusätzliche Stellen geschaffen, welche sich aktuell im Stellenbesetzungsverfahren befinden.
Gerne möchte die Senatsverwaltung für Bildung, Jungend und Familie die eigenverantwortlichen Schulen unterstützen. Das Schulgesetz (SchulG) sieht eine Aufgabenteilung der Aufsichtsbehörde gem. § 105 SchulG und der Schulämter gem. § 109 SchulG vor.

Nach der Änderung des SchulG wird eine Liste geprüfter digitaler Lehr- und Lernmittel durch die Senatsverwaltung für Bildung, Jungend und Familie bereitgestellt, die fortlaufend ergänzt wird.

Zentrale Steuerungselemente wie das Mobile Device Management (MDM) wurden ebenfalls installiert.

1.2.1 Gesetzliche Grundlagen für die Schuldigitalisierung

Wegen fehlender Rechtsgrundlagen im SchulG war der Einsatz digitaler Lehr- und Lernmittel im Unterricht seit Beginn der Pandemie nur möglich, wenn hierfür eine wirksame, d. h. informierte und freiwillige Einwilligung der Eltern bzw. volljährigen Schüler:innen vorlag. Diese an den Schulen geübte Praxis begegnet jedoch erheblichen datenschutzrechtlichen Bedenken. Die Nutzung digitaler Werkzeuge bringt eine ganz neue Qualität der Unterrichtsgestaltung mit sich und ist gleichzeitig mit einer umfangreichen Verarbeitung personenbezogener Daten verbunden. Diese unterscheidet sich in ihrem Umfang ganz erheblich von der im Rahmen des analogen Schulunterrichts stattfindenden Datenverarbeitung und hat erhebliche Auswirkungen auf die Persönlichkeitsrechte der Schüler:innen und Lehrkräfte. Die Schaffung einer gesetzlichen Regelung für die Verarbeitung personenbezogener Daten war daher notwendig. Dies ergibt sich bereits aus der Wesentlichkeitsrecht-

[26] Siehe 1.2.1

sprechung des Bundesverfassungsgerichts.[27] Einwilligungen als Grundlagen für die Datenverarbeitung sind hier nicht geeignet. Angesichts des durch den staatlichen Bildungs- und Erziehungsauftrag[28] geprägten Schulverhältnisses besteht ein Über-/Unterordnungsverhältnis zwischen Schüler:innen und Schulen. Die für die Wirksamkeit einer Einwilligung notwendige Voraussetzung der Freiwilligkeit[29] lässt sich insoweit kaum erfüllen. Wir haben viele Monate darauf gedrängt, dass die notwendigen Änderungen im SchulG vorgenommen werden, um für alle Beteiligten Rechtssicherheit für die Nutzung entsprechender Werkzeuge zu schaffen. Wir haben es daher grds. begrüßt, dass die Bildungsverwaltung im Frühjahr einen Referentenentwurf für eine Anpassung des SchulG vorgelegt hat. Leider wurde uns der Entwurf erst sehr spät im Rahmen der Beteiligung interessierter Fachkreise und Verbände zugeleitet. Zielführender wäre es gewesen, uns bereits bei der Erarbeitung des Entwurfs einzubinden, denn leider begegnete dieser in weiten Teilen ganz erheblicher datenschutzrechtlicher Kritik. Zudem mussten wir feststellen, dass unsere immer wieder unterbreiteten Vorschläge nicht berücksichtigt wurden.

Insbesondere wurde unser Vorschlag, eine Verpflichtung zur verbindlichen Festlegung der für Schulen geeigneten digitalen Lehr- und Lernmittel gesetzlich zu verankern, abgelehnt. Die Bildungsverwaltung scheute den Ressourcenaufwand und äußerte die Sorge, die pädagogische Freiheit könnte durch eine zentrale Festlegung digitaler Medien eingeschränkt werden. Diese Sorge ist jedoch unberechtigt. Eine Bündelung der Kapazitäten in der Bildungsverwaltung führt im Ergebnis gerade zu einer Entlastung der Schulen, die dann ihre Ressourcen in die pädagogische Arbeit stecken können. Aufwendige Mehrfachprüfungen durch die Schulen werden so verhindert.

Da die Bildungsverwaltung nicht bereit war, unsere Vorschläge für die Änderung und Ergänzung des SchulG umzusetzen, haben wir uns entschieden, selbst konkrete Formulierungsvorschläge zu erarbeiten. Uns war es wichtig, dass im SchulG nicht nur eine Befugnis für die Verarbeitung personenbezogener Daten beim Einsatz digitaler Lehr- und Lernmittel einschließlich des von der Bildungsverwaltung zur Verfügung gestellten Lernmanagementsystems bei der Erfüllung schulbezogener Aufgaben geschaffen wird, sondern auch eine Grundlage für die Da-

[27] Siehe JB 2020, 1.4.4
[28] Art. 7 Abs. 1 Grundgesetz (GG)
[29] Siehe EG 43 DS-GVO

tenverarbeitung bei der Nutzung digitaler Kommunikationswerkzeuge, zu denen neben den Videokonferenzen auch datenschutzkonforme Messenger- oder E-Mail-Dienste zählen. Die von der Bildungsverwaltung im Referentenentwurf vorgeschlagene Regelung hätte solche Dienste nicht umfasst. Besonders wichtig war es uns, im SchulG die Festlegung zu treffen, die nähere Ausgestaltung der Datenverarbeitung in einer gesonderten „Digitale-Lernmittel-Verordnung“ zu regeln. Eine solche Verordnung bietet die Chance, jederzeit zügig auf geänderte Gegebenheiten aufgrund neuer Technologien reagieren und die nötigen Anpassungen vornehmen zu können.

Im Rahmen unseres gesetzlichen Auftrages,[30] das Abgeordnetenhaus zu beraten, haben wir unsere Formulierungsvorschläge den Koalitionsfraktionen des Abgeordnetenhauses vorgestellt. Wir begrüßen es sehr, dass unsere Vorschläge daraufhin in das noch im September verabschiedete SchulG aufgenommen worden sind. Berlin hat damit ein modernes SchulG, das die Grundlagen für einen datenschutzgerechten Unterricht schafft.

Besonders erfreulich ist, dass der Gesetzgeber unsere Anregung aufgenommen hat, die Bildungsverwaltung auch gesetzlich zu verpflichten, eine Auswahl für die an Schulen in Betracht kommenden digitalen Lehr- und Lernmittel festzulegen und damit den Schulen die notwendige Hilfestellung bei der Auswahl datenschutzkonformer digitaler Werkzeuge an die Hand zu geben.[31] Die Regelung tritt zu Beginn des Schuljahres 2022/2023 in Kraft.[32] Die Zeit sollte von der Bildungsverwaltung genutzt werden, damit sich die Schulen spätestens zum nächsten Schuljahr darauf verlassen können, geprüfte datenschutzkonforme Werkzeuge nutzen zu können.

1.2.2 Schuldatenverordnung und „Digitale-Lernmittel-Verordnung“

Mit der Verabschiedung des SchulG hat der Gesetzgeber die notwendigen Rechtsgrundlagen geschaffen, um einen digitalen Unterricht zu ermöglichen und in diesem Rahmen die Verarbeitung personenbezogener Daten zu legitimieren. Allerdings kann das Gesetz hierfür nur das Gerüst vorgeben, das in der Praxis mit Leben erfüllt werden muss. Die Bildungsverwaltung steht nun in der Pflicht, die entsprechenden Rechtsverordnungen zu erlassen.

Zunächst ist die völlig veraltete Schuldatenverord- Der Referentenentwurf der geänderten Schulda-

[30] Art. 57 Abs. 1 lit. c DS-GVO, § 11 Abs. 1 Satz 1 Nr. 3 BlnDSG
[31] § 7 Abs. 2a Satz 2 SchulG
[32] § 129 Abs. 13 SchulG

nung aus dem Jahre 1994 zu novellieren. Wir drängen seit 2018 darauf, diese nicht nur kosmetisch zu überarbeiten, sondern sie stattdessen vollständig neu zu strukturieren.[33] Leider hat die Bildungsverwaltung unseren Vorschlag bislang nicht aufgegriffen. Seit unserer letzten umfangreichen Stellungnahme aus dem Februar zum vorliegenden Entwurf und einer Erörterung im Fachausschuss des Abgeordnetenhauses im März[34] wurden wir auch nicht mehr in die Angelegenheit einbezogen.

ten-Verordnung wurde grundlegend neu strukturiert und an das moderne Datenschutzrecht angepasst.

Die Senatsverwaltung für Bildung, Jugend und Familie bezieht die Berliner Beauftragte für Datenschutz und Informationsfreiheit weiterhin auch auf Arbeitsebene in die Erstellung der Schuldatenverordnung mit ein. So wurde etwa der umfassend neu strukturierte Referentenentwurf im Februar 2022 der Berliner Beauftragten für Datenschutz und Informationsfreiheit auf Arbeitsebene zugeleitet. Die in der daraufhin erfolgten Stellungnahme gemachten Anregungen wurden hinsichtlich ihrer Umsetzbarkeit geprüft und sofern rechtlich wie fachlich vertretbar umgesetzt.

Die Schuldatenverordnung enthält in erster Linie Regelungen, die sich auf den Schulalltag und damit eher auf schuladministrative Vorgänge beziehen. Sie regelt den Inhalt und den Umgang mit Schüler:innenunterlagen (Schüler:innenbogen, Schüler:innenpersonalblatt, Schüler:innenakte, Schüler:innenkarteien etc.) sowie Aufbewahrungsfristen etwa in Bezug auf Zeugnisse, Unterlagen des schulpsychologischen Dienstes oder sonderpädagogische Gutachten. Diese Regelungen bedürfen zwar dringend der Aktualisierung, unterliegen jedoch nicht den ständigen Veränderungen durch die Digitalisierung. Deswegen ist es zielführend, neben der Schuldatenverordnung eine „Digitale-Lernmittel-Verordnung“ zu erlassen, die die Vorschriften des SchulG für den Einsatz digitaler Lehr- und Lernmittel sowie digitaler Kommunikationswerkzeuge konkretisiert und die datenschutzrechtlichen Anforderungen definiert.

Da die Digitalisierung der Schulen auch in Zukunft immer wieder die Anpassung der rechtlichen Regelungen an die sich ändernden zukünftigen Technologien erfordern wird, bedarf es zweier getrennter Verordnungen, um zügig auf veränderte Gegebenheiten reagieren zu können, ohne gleich die gesamte Schuldatenverordnung anpassen zu müssen. Wir begrüßen es, dass der Gesetzgeber insoweit unserem Vorschlag gefolgt ist und die Bildungsverwaltung verpflichtet hat, neben der Schuldatenverordnung eine solche „Digitale-Lernmittel-Verordnung“ zu erlassen.[35] In dieser Verordnung sind die datenschutzrechtlichen Anforderungen in rechtlicher und technischer Sicht zu konkretisieren, damit sie im

Ausgewählte Materien, deren Regelung vormals in der Schuldaten-Verordnung beabsichtigt war, wurden – trotz verbleibender rechtlicher Bedenken hinsichtlich der Abgrenzbarkeit – in eine separate „Digitale-Lehr- und Lernmittel-Verordnung“ ausgegliedert. Diese – vormals im Entwurf der Schuldaten-Verordnung befindlichen – Regelungen wurden der Berliner Beauftragten für Datenschutz und Informationsfreiheit im Rahmen der Zusammenarbeit auf Arbeitsebene zur Kenntnis gegeben. Darüber hinaus wird die Berliner Beauftragte für Datenschutz und Informationsfreiheit auch zukünftig weiter einbezogen, etwa im Rahmen der Anhörung beteiligter Fachkreise und

[33] Siehe JB 2019, 5.4

[34] TOP 3 der 38. Sitzung des Ausschusses für Kommunikationstechnologie und Datenschutz (KTDat) am 22. März 2021

[35] § 64 Abs. 11 Satz 2, § 64 c Abs. 3 Satz 2 SchulG

praktischen Schulalltag umgesetzt werden können. Wir erwarten, dass die Bildungsverwaltung uns frühzeitig in die Erarbeitung der „Digitale-Lernmittel-Verordnung“ einbezieht und die notwendige Novellierung der Schuldatenverordnung nunmehr zügig abschließt.

Verbände.

1.2.3 Lernraum Berlin“ — Was hat sich getan?

Wir haben in unserem letzten Jahresbericht[36] ausführlich über das seit 2005 existierende Projekt „Lernraum Berlin“ berichtet. Durch die Corona-Pandemie bekam der „Lernraum Berlin“ als Lernmanagementsystem des Landes Berlin plötzlich eine besondere Bedeutung, da an vielen Schulen der digitale Unterricht hierüber realisiert wurde. Leider zeigten sich in diesem Projekt, in das wir zuvor nicht einbezogen worden waren, diverse Mängel in Bezug auf Datenschutz und Datensicherheit. Wir stehen hierzu nach wie vor im Austausch mit der Bildungsverwaltung. Bezüglich der Datenschutzanforderungen konnten wir einige Fortschritte bewirken. So wurde die vor der Änderung des SchulG für den Einsatz des „Lernraums Berlin“ im Unterrichtskontext notwendige Einwilligungserklärung in Abstimmung mit uns mehrfach überarbeitet und angepasst. Außerdem wurde ab Januar eine datenschutzkonforme Videokonferenzlösung unter Nutzung der Open Source-Software Big Blue Button in den „Lernraum Berlin“ integriert. Der Einsatz des zuvor genutzten Videokonferenzsystems, das von uns bislang als nicht datenschutzgerecht eingeordnet wird,[37] konnte so reduziert werden. Nach einem umfangreichen Schriftwechsel mit der Bildungsverwaltung hat uns diese schließlich zugesichert, die datenschutzrechtlich bedenkliche Videokonferenzlösung mit dem Beginn der Weihnachtsferien vollständig abzuschalten.

In Bezug auf das nun genutzte Videokonferenzsystem wurde uns ein Konzept vorgestellt, mit welchem Lehrkräfte die Möglichkeit haben, Eltern für Elternabende oder Elterngespräche temporäre Kennungen für das Videokonferenzsystem zur Verfügung zu stellen. Diese Möglichkeit begrüßen wir sehr, da so ein Rückgriff auf andere – nicht datenschutzkonforme – Videokonferenzsysteme und die Zweckentfremdung der Schüler:innenzugänge hierfür vermieden werden kann.

Hinsichtlich der von uns bereits im vergangenen Jahr festgestellten Datenschutzmängel der fehlenden Mandantenfähigkeit bzw. fehlender Löschroutinen[38]

Der Lernraum Berlin wird in seiner architektonischen und fachlichen Ausrichtung kontinuierlich und systematisch weiterentwickelt. So wurden im Schuljahr 2021/2022 beispielsweise eine digitale Pinnwand und die Kennwortrücksetzung durch Lehrkräfte eingeführt, die Möglichkeiten zur Kurseinschreibung und die Einladungsfunktion erweitert.

Zur langfristigen Sicherstellung des Betriebs und weiterer Skalierungsmöglichkeiten sowie zur Umsetzung der Datenschutzvorgabe der Mandantentrennung wird die Architektur des Lernmanagementsystems seit Januar 2021 grundlegend überarbeitet. Die Aufteilung des Lernraum Berlin in eine zentral verwaltete Instanz pro Schule (Mandant) wurde mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit und den zuständigen Personalgremien abgestimmt und die notwendigen Infrastrukturen implementiert. Nach Abschluss der Pilotierung werden im Schuljahr 2022/2023 sukzessive alle Schulen auf eine eigene Instanz umgestellt

[36] JB 2020, 1.4.1
[37] Siehe dazu auch 2.2
[38] Siehe JB 2020, 1.4.1

konnten ebenfalls Fortschritte erzielt werden. Es wurden Löschroutinen mit uns abgestimmt und Maßnahmen ergriffen, die die Gesamtsicherheit des Systems deutlich verbessern konnten. Mittlerweile hat uns die zuständige Senatsverwaltung ein Konzept zur Mandantentrennung vorgelegt, welches sehr tragfähig erscheint und die Aufteilung des Lernraums auf jeweils eine Einzelinstanz pro Schule vorsieht. Mit der Umsetzung dieses Konzepts wäre auch dieser schon lange bestehende Mangel endlich abgestellt.

Wir werden die Weiterentwicklung des „Lernraums Berlin“ auch künftig begleiten und stehen der Bildungsverwaltung auch bei weiteren Projekten beratend zur Verfügung.

1.2.4 Lehrkräfte-Unterrichts-Schul-Datenbank

Die Berliner Lehrkräfte-Unterrichts-Schul-Datenbank (BLUSD) ist ein IT-Fachverfahren, das von den Schulen für die Schulverwaltung genutzt wird. Personenbezogene Daten von sämtlichen Schüler:innen, Eltern und Lehrkräften sowie anderen schulischen Mitarbeitenden werden für die durch das SchulG zugewiesenen Aufgaben in diesem Verfahren automatisiert verarbeitet, z. B. zur Organisation des Unterrichts, der Anwesenheitskontrolle oder der Zeugniserstellung. Zugriffsmöglichkeiten auf dieses System sind nur in einem begrenzten Umfang im Wesentlichen durch die Schulleitungen vorgesehen. Grundsätzlich ist der Einsatz der BLUSD nach dem SchulG für alle Schulen verbindlich. Jedoch ist der Prozess, sämtliche Schulen an das System anzuschließen, noch nicht abgeschlossen. Wir begleiten das Projekt schon seit 2016. Nachdem lange Zeit kaum ein Austausch mit den Projektverantwortlichen stattfand, haben wir angesichts der zahlreichen aktuellen Vorhaben bei der Weiterentwicklung der BLUSD seit Anfang dieses Jahres den Austausch mit der Bildungsverwaltung intensiviert. In regelmäßigen konstruktiven Treffen werden anstehende Änderungen nun frühzeitig kommuniziert und erörtert. Hinweise und Anregungen unsererseits wurden aufgenommen und in weiten Teilen auch umgesetzt.

Da offenbar geplant ist, die in der BLUSD verarbeiteten personenbezogenen Daten auch für andere Zwecke, wie z. B. das Schulportal für Berliner Lehrkräfte[39], nutzbar zu machen, ist ein besonderes Augenmerk darauf zu richten, dass dies nur im Rahmen zuvor gesetzlich festgelegter Zwecke erfolgt und mit der Sicherheitsarchitektur der BLUSD vereinbar ist. Ein Beispiel ist die Nutzung der in der BLUSD ent-

Alle geplanten Erweiterungen werden in regelmäßigen Treffen präsentiert und in konstruktiver Form unter Datenschutz- und Datensicherheitsaspekten betrachtet. In einigen Bereichen (Schnittstellen zu anderen Verfahren, wie z. B. EALS, Schulportal, …) ist eine gemeinsame Abstimmung erforderlich, um die jeweils erforderlichen rechtlichen Voraussetzungen zu initiieren.

[39] Siehe https://schulportal.berlin.de

haltenen personenbezogenen Daten für die Bereitstellung von Benutzungszugängen in den von der Bildungsverwaltung zur Verfügung gestellten Lernmanagementsystemen. Um die Nutzung der im IT-Fachverfahren gespeicherten personenbezogenen Daten der Schüler:innen, die einem besonderen Schutz und einer strengen Zweckbindung unterliegen, auch hierfür zu ermöglichen, war es notwendig, das SchulG anzupassen und die Datenverarbeitung explizit gesetzlich zu regeln.[40] Sofern sonstige Erweiterungen oder Änderungen der technischen Realisierung in Planung sind, bedarf es einer engen Begleitung, um die Einhaltung der datenschutzrechtlichen und technischen Vorgaben sicherzustellen. Wir werden daher auch dieses Projekt durch Fortsetzung des konstruktiven Austauschs weiterhin begleiten.

Die datenschutzkonforme Digitalisierung der Schulen bleibt eine besondere Herausforderung. Mit der Anpassung der schulgesetzlichen Regelungen ist ein wichtiger Schritt erfolgt. Es ist jetzt Aufgabe der Bildungsverwaltung, die notwendigen Konkretisierungen auf der Verordnungsebene zu schaffen. Eine besonders wichtige Aufgabe besteht zudem darin, nun die im Gesetz vorgesehene verbindliche - Auswahl datenschutzkonformer digitaler Lehr- und Lernmittel festzulegen und die hierfür erforderliche Fachkompetenz in der Bildungsverwaltung aufzubauen. Dabei ist Eile geboten, damit zu Beginn des neuen Schuljahres 2022/23 tatsächlich eine solche Auflistung für die Schulen zur Verfügung steht. Wir erwarten, dass die Bildungsverwaltung diese Verpflichtung ernst nimmt. Unser in der Vergangenheit wiederholt unterbreitetes Angebot zur Beratung in Datenschutzfragen besteht fort.

Nach der Schulgesetzesänderung wurde eine Bedarfsermittlung an gewünschten Applikationen der Schulen durchgeführt. Dieses ist ein fortwährender Prozess.
Hierfür wurde von der Senatsverwaltung für Bildung, Jugend und Familie ein zentrales Serviceportfoliomanagement installiert. Jede App wird nach festgelegten Kriterien, darunter auch auf datenschutzrechtliche Konformität, geprüft.
Eine Liste an digitalen Lehr- und Lernmitteln ist niemals abschließend, sondern fortlaufend. Applikationswünsche der Schulen gehen regelmäßig im Schulservicezentrum Berlin (SSZB) der Senatsverwaltung für Bildung, Jugend und Familie ein.

1.3 Corona-Impfmanagement des Landes Berlin

1.3.1 Online-Terminbuchung bei Privatunternehmen

Zum Ende des Jahres 2020 sah sich Berlin – wie auch alle übrigen Bundesländer – mit der Aufgabe konfrontiert, möglichst kurzfristig die Schutzimpfungen der Bürger:innen gegen den Erreger SARS-CoV-2 zu organisieren. Mit der technischen Abwicklung der Online-Impfterminvergabe hat die insoweit zuständige Senatsverwaltung für Gesundheit, Pflege und Gleichstellung ein Privatunternehmen betraut. Hiergegen wäre grds. nichts einzuwenden, soweit der Beauftragung des Unternehmens ein entsprechender Auftragsverarbeitungsvertrag zugrunde läge und das Unternehmen die Grenzen, die ihm als Auftragsverarbeiter gesetzt sind, auch einhielte. Gerade Letzteres ist jedoch nicht der Fall. Im Fokus

Zur Sicherstellung des ordnungsgemäßen und insbesondere fristgerechten Starts der Berliner Impfkampagne wurde Ende des Jahres 2020 nach Durchführung eines Vergabeverfahrens ein leistungsstarker privater Anbieter mit der Umsetzung der Impfterminvergabe und Impfdokumentation für das Land Berlin beauftragt. Auf die im Land Berlin vorhandenen Fachverfahren wurde zum damaligen Zeitpunkt nicht zurückgegriffen, weil diese nicht uneingeschränkt den Anforderungen für die Impfkampagne entsprachen. Dies galt gleichfalls für das von der Kassenärztlichen Bundesvereinigung zur Verfügung gestellte Terminbuchungssystem.

[40] Siehe § 64a Abs. 10, § 64c SchulG

unserer Kritik steht hierbei, dass die Bürger:innen im Rahmen des Online-Terminbuchungsprozesses mit der Anlage eines Nutzungskontos auch zwingend ein eigenes Vertragsverhältnis mit dem Privatunternehmen eingehen müssen.

Bei der Nutzung des Impfterminvergabe und Impfdokumentationssystems in einem der Berliner Impfzentren war die Eröffnung eines Nutzerkontos zur Buchung von Impfterminen entgegen der Auffassung der Berliner Beauftragten für Datenschutz und Informationsfreiheit keine zwingende Voraussetzung. Die Eröffnung eines Nutzerkontos wurde aber im Interesse der Sicherstellung einer möglichst hohen Impfquote und damit im Interesse des Infektionsschutzes ermöglicht. Die Bürgerinnen und Bürger hatten davon unabhängig zu jedem Zeitpunkt die Möglichkeit, einen Impftermin telefonisch über die dafür vom Land Berlin zur Verfügung gestellte Impf-Hotline zu vereinbaren. Soweit die Impfwilligen hierbei – auch unter Wahrnehmung ihres informationellen Selbstbestimmungsrechts – von der Möglichkeit Gebrauch gemacht haben, ihr bereits bei dem Privatunternehmen bestehendes oder neu eröffnetes Nutzerkonto zu nutzen, können sie die darin gespeicherten Daten und das Konto jederzeit selbst löschen. Davon unabhängig werden die betreffenden Daten nach Ablauf der gesetzlich vorgeschriebenen Dokumentations- und Aufbewahrungspflicht von 10 Jahren gelöscht. Hierauf wurden die Impfwilligen bereits im Vorfeld der Impfung schriftlich durch das Land Berlin und den Anbieter hingewiesen.

Mit Fortgang der COVID-19-Pandemie und den damit einhergehenden Beschränkungen des öffentlichen und privaten Lebens auf der Grundlage der jeweiligen Corona-Verordnungen hat sich gezeigt, dass mit der Eröffnung eines Nutzerkontos und der dadurch geschaffenen Zugriffsmöglichkeit auf Impfunterlagen für die Bürgerinnen und Bürger zahlreiche Anfragen zur Ausstellung von Ersatz-Impfnachweisen und Impfzertifikaten zeitnah bearbeitet werden konnten. Besonders während den sog. Phasen des Lock-Downs im Herbst und Winter im Jahr 2021 waren die Impfnachweise elementare Voraussetzung für die Teilnahmen am öffentlichen und privaten Leben, weil der Zugang oftmals durch sog. 2G oder 3G-Regelungen beschränkt war.

Für Impfungen gegen SARS-CoV-2, die in den Impfzentren stattfanden und weiterhin stattfinden, müssen die Berliner:innen einen konkreten Termin vereinbaren. Erst im Jahresverlauf wurden in bestimmten Impfzentren auch Impfungen ohne vorherige Terminvereinbarung durchgeführt. Neben der telefonischen Terminbuchung über eine Impfhotline bestand und besteht nach wie vor die Möglichkeit,

einen Impftermin online zu buchen. Für diese Online-Terminbuchung nutzt die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung den Service eines Privatunternehmens. Zwar hat die Kassenärztliche Bundesvereinigung (KBV) zu diesem Zweck ein Online-Terminbuchungssystem bereitgestellt, das von einigen Ländern – u. a. Brandenburg – auch eingesetzt worden ist. Die Nutzung dieses Systems war für die Länder jedoch nicht verpflichtend und wurde von Berlin auch nicht veranlasst. Möchten Berliner:innen online einen Impftermin in einem Impfzentrum buchen, kommen sie daher an der Nutzung des von dem Privatunternehmen betriebenen Systems nicht vorbei.

In ihrer „Datenschutzinformation zur Impfung gegen SARS-CoV-2 (Corona-Impfung) in Impfzentren“ informiert die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung die Berliner:innen darüber, dass sie für die Online-Terminvereinbarung besagtes Unternehmen einsetze und dieses Unternehmen als Auftragsverarbeiter für sie tätig werde. Gegen den Einsatz eines Privatunternehmens als Auftragsverarbeiter ist – wie eingangs erwähnt – grds. nichts einzuwenden.

Ein Auftragsverarbeiter darf die Daten allerdings ausschließlich im Auftrag und auf Weisung des Verantwortlichen verarbeiten. Das ist bei der vorliegenden Einbindung des Unternehmens nicht der Fall. Denn die Terminbuchung über das eingesetzte System setzt das Anlegen eines Nutzungskontos bei dem Privatunternehmen voraus. Dadurch entsteht ein Vertragsverhältnis zwischen dem Unternehmen und den einzelnen Nutzer:innen. Die Datenverarbeitung des Unternehmens im Zusammenhang mit der Erstellung des Nutzungskontos erfolgt also zum Zweck der Durchführung des zwischen ihm und den jeweiligen Nutzer:innen geschlossenen Vertrags. Dadurch verlässt das Unternehmen seine Rolle als Auftragsverarbeiter für die zuständige Senatsverwaltung und wird selbst als datenschutzrechtlich Verantwortlicher tätig.

Daran, dass Personen, die eine Impfung gegen SARS-CoV-2 erhalten möchten, faktisch gezwungen werden, ein Vertragsverhältnis mit einem Privatunternehmen einzugehen, störten sich nicht nur viele Impfwillige, die sich in der Folge mit entsprechenden Nachfragen und Beschwerden an uns wandten. Auch wir hatten die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung und das Unternehmen bereits frühzeitig auf die bestehende Problematik aufmerksam gemacht und darauf hingewiesen, dass die Einbindung des Unternehmens auch daten-

schutzgerecht ausgestaltet werden kann.

Ein datenschutzgerechtes Verfahren setzt u. a. voraus, dass die Nutzungskonten, die die Berliner:innen bei dem Unternehmen angelegt haben, nur im Auftrag und auf Weisung der zuständigen Senatsverwaltung – und eben nicht zu eigenen Zwecken des Unternehmens – angelegt und genutzt werden dürfen. Die zuständige Senatsverwaltung ist deshalb gehalten, ggü. dem Unternehmen die Löschung der Nutzungskonten anzuweisen, sobald diese ihren Zweck erfüllt haben.

Wenn ein Unternehmen als Auftragsverarbeiter Daten für eine Senatsverwaltung verarbeiten soll, darf dies nur im Rahmen der Weisungen seiner Auftraggeberin erfolgen.[41] Stellt eine Verantwortliche Datenschutzverstöße durch ihren Auftragsverarbeiter fest, hat sie ggü. dem Auftragsverarbeiter mit den Mitteln des Vertragsrechts auf ein vertragskonformes Verhalten zu drängen. Dass wir insofern unverzügliche Maßnahmen von ihr erwarten, haben wir der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung mitgeteilt.

Möchten Bürger:innen per Online-Anmeldung einen Impftermin erhalten, bleibt ihnen bisher oft nichts anderes übrig, als – vermittelt durch die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung – Kund:innen eines Privatunternehmens zu werden. Dies kann weder im Interesse der Bürger:innen noch der Verwaltung sein. Es ist für uns unverständlich, dass die zuständige Senatsverwaltung unsere wiederholten Hinweise zur Art und Weise der Einbindung des Unternehmens als Auftragsverarbeiter für die Terminbuchung in den Impfzentren bisher ignoriert hat. Die von uns erwarteten Maßnahmen zur Herstellung eines datenschutzkonformen Zustands wurden bislang nicht getroffen. Wir werden daher weiterhin darauf hinwirken, dass die personenbezogenen Daten der Impfwilligen nur im Rahmen des gesetzlich Erlaubten verarbeitet werden.

1.3.2 Die Sache mit der Zweckbindung

Durch eine Pressemitteilung der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung mussten wir erfahren, dass sich diese mit der Kassenärztlichen Vereinigung (KV) Berlin darauf verständigt hat, dass die KV Berlin Einladungen zur Inanspruchnahme von Schutzimpfungen gegen den Erreger SARS-CoV-2 an rund 400.000 Personen, die aufgrund einer bestehenden chronischen Erkrankung eine priorisierte Impfberechtigung aufweisen, ver-

Die für Gesundheit zuständige Senatsverwaltung war schon in der Anfangsphase der Impfkampagne im Winter 2020/2021 in Kontakt mit Vertreterinnen und Vertretern der Kassenärztlichen Vereinigung Berlin (KV) und der Krankenkassen, um chronisch kranke Personen, die nach der damals geltenden Fassung der Coronavirus-Impfverordnung prioritär impfanspruchsberechtig waren, Impfcodes für die Impfterminbuchung zur Verfü-

[41] Siehe Art. 29 DS-GVO

sendet. Die Einladung sollte „im Auftrag“ der Senatsverwaltung und auf Grundlage der bei der KV Berlin vorliegenden Abrechnungsdaten erfolgen. Diese Vorgehensweise war weder zulässig noch notwendig.

gung zu stellen. Schon zum damaligen Zeitpunkt wurden im Gegensatz zur Rechtsauffassung der Berliner Beauftragten für Datenschutz und Informationsfreiheit erhebliche Zweifel an der datenschutzrechtlichen Zulässigkeit der Verwendung der den Krankenkassen vorliegenden personenbezogenen Daten für den Versand von Impfeinladungen geäußert, da die rechtlichen Grundlagen hierfür nicht vorlägen. Zudem wies der GKV-Spitzenverband u.a. darauf hin, dass den Krankenkassen Abrechnungsdaten erst mit einem Zeitverzug von sechs bis neun Monaten vorliegen, so dass ein relevanter Teil von Personen mit Erkrankungen oder Risikofaktoren keine Information über die Impfberechtigung erhalten würde. Gleiches galt für Kassenwechsler, da der aufnehmenden Krankenkasse für diese Personengruppe zunächst keine Diagnosedaten zur Verfügung stehen. Dies führte dazu, dass zum Schutze des Lebens und der Gesundheit der besonders vulnerablen Personengruppen der chronisch Kranken die für Gesundheit zuständige Senatsverwaltung sehr kurzfristig pragmatische Lösungen zum Versand der Impfeinladungen einschließlich der für die Terminbuchung erforderlichen Impfcodes finden musste, da dem Land Berlin personenbezogene Daten zu chronisch Kranken nicht vorliegen (und auch nicht vorliegen dürfen). Die Behauptung der Berliner Beauftragten für Datenschutz und Informationsfreiheit, die gewählte Vorgehensweise sei „nicht notwendig“ gewesen und eine rechtskonforme Alternative hätte zur Verfügung gestanden, geht damit an der damaligen Realität vorbei.

Die Auffassung der Berliner Beauftragten für Datenschutz und Informationsfreiheit, die KV sei ohne Rechtsgrundlage tätig geworden, wird nicht geteilt. Rechtsgrundlage für die Datenverarbeitung auf Seiten der KV Berlin war Art. 6 Abs. 1 lit. c) i.V.m. Art. 9 Abs. 2 lit. i) DSGVO, § 6 Abs. 2 CoronaImpfV (a.F.) i.V.m. dem Auftrag des Berliner Senats (Erfüllung der übertragenen Verpflichtungen). Die Beauftragung und die anschließend geschlossene Vereinbarung „Zur Umsetzung der Beauftragung zur Auswertung von versichertenbezogenen Daten und dem Versand von Einladungsschreiben“ bildeten die Grundlage für die KV Berlin, die betroffenen Personengruppen zur Impfung einzuladen, die wegen ihrer (Vor)Erkrankung einen Anspruch auf eine Schutzimpfung mit hoher oder erhöhter Priorität hatten. Die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung und die KV haben hierbei den aus § 20i Abs. 3 Satz 11 Nr. 3 SGB V (a.F.) i.V.m. § 6 Abs. 2 und 3 CoronaImpfV a.F. erkennbaren Willen des

Gesetzgebers aufgenommen, dass die obersten Landesgesundheitsbehörden und die Kassenärztlichen Vereinigungen bei den Impfungen gegen das Corona-Virus zusammenwirken konnten. Diese Möglichkeit ergab sich auch aus der Begründung zur Coronavirus-Impfverordnung. Darüber hinaus wurde die KV durch die SenGPG zur Beachtung der einschlägigen Vorgaben der DSGVO und des SGB X verpflichtet. Die KV Berlin selbst hat die datenschutzrechtlichen Fragen intensiv mit einem von ihr beauftragten privaten Beratungsunternehmen aus dem Bereich Datenschutz eruiert. Damit war das Einladungsmanagement aus datenschutzrechtlicher Sicht unter der CoronaImpfV a.F. und entgegen der juristischen Einschätzung der Berliner Datenschutzbehörde zumindest rechtlich vertretbar. Die Behauptung der Berliner Beauftragten für Datenschutz und Informationsfreiheit, Vorgaben des Sozialdatenschutzes seien „einfach ignoriert“ worden, entspricht nicht der Realität und wird ausdrücklich zurückgewiesen.

Seitens der KV Berlin wurden rund 400.000 Schreiben an die damals impfberechtigten Personen verschickt. Der Rechtsaufsicht bei SenWGPG sind diesbezüglich keine aufsichtsrechtlichen Beschwerden von Bürgerinnen und Bürgern gegen dieses Vorgehen und/oder gegen die KV Berlin bekannt. Vielmehr hat die weit überwiegende Anzahl der damals impfberechtigten Personen auf den Versand der Einladungen gewartet, um eine Impftermin in einem der Berliner Corona-Impfzentren buchen zu können. Für Privatversicherte wurde zeitgleich ein anderes Einladungsverfahren unter Nutzung der Impfhotline des Landes Berlin umgesetzt, das gleichermaßen die Impfterminbuchung ermöglichte.

Abschließend sei angemerkt, dass es aus Sicht der Senatsverwaltung für Wissenschaft, Gesundheit, Pflege und Gleichstellung fraglich erscheint, wie eine Maßnahme, die dem Gesundheitsschutz und sicherlich auch der Rettung von Leben diente, in dem vorliegenden Jahresbericht überhaupt als Schwerpunktthema ausgewählt werden konnte. Es wäre wünschenswert gewesen, wenn die Berliner Beauftragte für Datenschutz und Informationsfreiheit - trotz ihrer Zuständigkeit - bei der Abwägung der hier betroffenen Rechtsgüter und der besonders eilbedürftigen Situation hätte feststellen können, dass letzte, datenschutzrechtliche Bedenken hinter dem Gesundheitsschutz der Bevölkerung zurückstehen können.

Die KV stellen in Deutschland u. a. die ambulante

ärztliche Versorgung der gesetzlich Krankenversicherten sicher. Die Vertragsärzt:innen rechnen alle Leistungen, die sie für gesetzlich Versicherte erbringen, quartalsweise mit der jeweils zuständigen KV ab. Diese Abrechnungsdaten enthalten auch Angaben über die ärztlichen Diagnosen. Bei den Daten handelt es sich daher aus gutem Grund um besonders schützenswerte Sozialdaten, deren Verarbeitung durch das Sozialgesetzbuch (SGB)[42] engen Grenzen unterworfen ist.

Grundsätzlich dürfen die KV die Sozialdaten nur für die gesetzlich konkret genannten Aufgaben verarbeiten. Die Ermittlung und Benachrichtigung von Impfberechtigten fällt jedoch nicht in diesen Aufgabenkatalog.

Auch eine sog. „zweckändernde Weiterverarbeitung" der Abrechnungsdaten kam hier nicht in Betracht. Eine solche wäre nur zulässig gewesen, soweit diese durch Rechtsvorschriften des SGB oder nach dem Infektionsschutzgesetz (IfSG) angeordnet oder erlaubt worden wäre.[43] Das war jedoch nicht der Fall. Insbesondere sieht das IfSG keine Verpflichtung der KV Berlin vor, impfberechtigte Personen unter den gesetzlich Krankenversicherten zu identifizieren und zu kontaktieren. Vielmehr ordnet das Gesetz lediglich an, dass die KV Berlin bestimmte Angaben über bereits durchgeführte Schutzimpfungen in pseudonymisierter[44] Form an das Robert-Koch-Institut und an das Paul-Ehrlich-Institut übermitteln muss.[45]

Eine Rechtsgrundlage für das Vorgehen der Gesundheitsverwaltung und der KV Berlin bestand also nicht. Darauf haben wir den zuständigen Staatssekretär hingewiesen. Aber steht der Datenschutz – wie böse Zungen behaupten – damit wieder einmal der Bekämpfung der Corona-Pandemie im Weg? – Keineswegs!

Die chronisch Erkrankten hätten nach den gesetzlichen Vorgaben nämlich sehr wohl auf ihre priorisierte Impfberechtigung hingewiesen werden können. Nur nicht durch die KV, sondern durch die gesetzlichen Krankenkassen und die privaten Krankenversicherungen. Denn für diese sind durch den Bundesgesetzgeber genau zu diesem Zweck Rechtsgrundlagen

[42] Hier insbesondere durch § 285 SGB V
[43] § 285 Abs. 3 Satz 1 SGB V
[44] Pseudonymisieren ist das Ersetzen identifizierender Angaben wie Name, Adresse, Geburtsdatum oder anderer eindeutiger Kennzeichen bzw. Merkmale durch eine andere Bezeichnung (z. B. eine laufende Nummer) derart, dass ein Rückschluss auf die Person ohne Kenntnis der Zuordnungsregel nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.
[45] § 13 Abs. 5 Satz 1 IfSG

geschaffen worden, um die Inanspruchnahme und die Sicherheit der Impfstoffe überwachen zu können.[46] Der Vorteil wäre übrigens gewesen, dass von dieser Variante auch die chronisch erkrankten Personen hätten profitieren können, die privat versichert sind. Denn für diese Personengruppe liegen der KV naturgemäß keine Abrechnungsdaten vor. Privatversicherte, die aufgrund einer bestehenden chronischen Erkrankung eine priorisierte Impfberechtigung aufweisen, waren daher weiterhin darauf angewiesen, sich zunächst ein ärztliches Attest zu besorgen, um einen Impftermin vereinbaren zu können.

An die Verarbeitung von besonders schutzbedürftigen Sozialdaten werden nicht ohne Grund hohe Anforderungen gestellt. Diese Vorgaben dürfen auch in Zeiten einer Pandemie nicht einfach ignoriert werden. Ein gesetzeskonformer Weg hätte zur Verfügung gestanden.

1.4 Datenverarbeitung durch Corona-Teststellen

Mit Einführung der kostenlosen Corona-Antigen-Schnelltests (sog. Bürgertestungen[47]) schossen Corona-Teststellen in großer Zahl aus dem Boden. Zeitweise gab es allein in Berlin weit über 1.000 Teststellen. Mit dem Datenschutz und der Datensicherheit haben es viele Teststellen dabei nicht so genau genommen.

Als Aufsichtsbehörde sind wir zuständig für diejenigen Teststellen, deren Betreiber:innen ihren Sitz in Berlin haben. Bei diesen gab es eine Reihe von Datenpannen und zahlreiche andere datenschutzrechtliche Verstöße.

Viele Teststellen bieten Bürger:innen die Möglichkeit, sich per Internet für einen Testtermin zu registrieren. Die Erhebung der für die Testdurchführung notwendigen personenbezogenen Daten wird so vereinfacht. Zudem ist es auf diese Weise möglich, den Bürger:innen ihr Testergebnis auf elektronischem Wege zu übermitteln, sodass sie nicht vor Ort auf das Ergebnis warten müssen.

Eine Reihe von Teststellen verlangte neben den für die Durchführung des Tests notwendigen Angaben weitere personenbezogene Daten, die für die Durchführung der Bürgertestung nicht erforderlich sind. So machten einige Teststellen die Terminbuchung davon abhängig, dass bspw. die Krankenversicherung oder die Personalausweisnummer angegeben wird.

[46] § 20i Abs. 4 Satz 2 SGB V; § 6 Abs. 7 CoronaImpfV (Stand: 10. März 2021)
[47] Siehe § 4a Coronavirus-Testverordnung (TestV)

Da hierfür jedoch keine Rechtsgrundlage besteht, gaben wir solchen Teststellen auf, diese Abfragen aus ihren Terminbuchungsformularen zu entfernen.

Einige Teststellen übermittelten den getesteten Personen ihre Testergebnisse per E-Mail. Dabei kam es, wie es kommen musste: Einige Teststellen versendeten Testergebnisse an falsche Empfänger:innen. Wir gaben den jeweiligen Teststellen konkrete Hinweise, wie die Informationen datenschutzkonform an die getesteten Personen übermittelt werden können.

Dabei wiesen wir sie auch auf die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)[48] hin. Die Orientierungshilfe stellt insbesondere die bestehenden Anforderungen an die Verschlüsselung der Nachrichten dar. Diese richten sich nach den Risiken für betroffene Personen. Die unbefugte Offenlegung der Information über eine Infektion ist ein solches Risiko. Um dies abzuwenden, ist eine qualifizierte Transportverschlüsselung notwendig, aber allein nicht ausreichend. Wenn die getesteten Bürger:innen, wie es die Regel ist, keine Möglichkeit zum Empfang von Ende-zu-Ende-verschlüsselten E-Mails haben, dann muss die Datei mit dem Testergebnis verschlüsselt werden. Zum Entschlüsseln bekommen die Bürger:innen noch im Testzentrum ein ausreichend langes, zufällig generiertes Passwort.

Des Weiteren nutzten einige Teststellen die E-Mail-Adressen der getesteten Personen, um ihnen Werbung, die nichts mit dem Testen zu tun hatte (bspw. für Sportkurse), zu schicken. Die Voraussetzungen für die zulässige Nutzung der E-Mail-Adressen zu Werbezwecken waren regelmäßig nicht erfüllt.

Schließlich traten bei einer Reihe von Teststellen Datenpannen auf, bei denen unbefugte Dritte Daten über die getesteten Bürger:innen abrufen konnten.

Dies traf oft kein einzelnes Testzentrum, sondern eine ganze Reihe von ihnen. Die notwendige Software und die Server-Infrastruktur wird regelmäßig nicht von den Teststellen selbst programmiert und betrieben, sondern als Dienstleistung von Dritten eingekauft. Datenpannen, die in fehlerhafter Implementierung der Software begründet liegen, betrafen deswegen regelmäßig mehrere Teststellen, oft auch in verschiedenen Bundesländern.

[48] Abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/orientierungshilfen

Von diesen Datenpannen erfuhren wir zum einen aus den Datenpannenmeldungen der Betreiber:innen. Zum anderen teilten uns auch Sicherheitsforscher:innen Datenpannen mit, die ihnen bei einer Prüfung auf Sicherheitslücken aufgefallen waren.

Die größten Probleme lagen bei der Software zur Bereitstellung der Testergebnisse über das Internet. Sie darf einer getesteten Person nur den Abruf ihrer eigenen Testergebnisse und dies auch nur nach Anmeldung mit mindestens dem Nutzernamen und einem Passwort ermöglichen. Versuche, auf andere Testergebnisse zuzugreifen, muss die Software unterbinden. Alternativ kann der getesteten Person noch im Testzentrum ein Internet-Link oder Code zum Abruf des Testergebnisses gegeben werden, sofern Link oder Code so viele zufällige Zeichen (Zahlen und Buchstaben) enthalten, dass es praktisch ausgeschlossen ist, durch einfaches Durchprobieren den Code einer anderen Person zu ermitteln und so deren Testergebnisse zu finden.

Einige von uns geprüfte Testzentren verwandten jedoch Links, die jeweils eine fortlaufende Nummer des durchgeführten Tests enthielten. Einfaches Hoch- bzw. Herunterzählen dieser Nummer lieferte Testergebnisse anderer Personen. In anderen Fällen waren die Abrufcodes leicht zu entschlüsseln. Mit einfachen Programmen, die viele mögliche Codes durchprobierten, konnten Testergebnisse von hunderten bzw. tausenden Personen abgerufen werden.

Mitunter fanden sich versteckt, aber mit Fachwissen leicht auffindbar, auf den Webseiten der Testzentren auch Zugangsdaten zu weiteren eingesetzten Dienstleister:innen, die bspw. den Versand von E-Mails und SMS-Nachrichten übernahmen. Mit diesen Zugangsdaten konnten wiederum Daten eingesehen werden, die Rückschlüsse auf die durchgeführten Tests und Kontaktdaten von getesteten Personen zuließen.

Es gibt eine einfache Maßnahme zur Verringerung des Risikos der widerrechtlichen Verarbeitung der Daten, die durch die Testzentren für die getesteten Personen bereitgestellt werden. Sie besteht darin, diese Daten – wie ohnehin rechtlich geboten – so früh wie möglich zu löschen.

Die Verantwortlichen haben uns die beschriebenen Datenpannen in der Regel innerhalb der vom Gesetz vorgesehen Zeitspanne gemeldet. Wir haben daraufhin, wenn nötig, weitere Ermittlungen zum Sachverhalt vorgenommen und Empfehlungen oder auch

Forderungen bezüglich der zu treffenden technischen und organisatorischen Maßnahmen ausgesprochen. Darüber hinaus haben wir verlangt, dass die von den Datenpannen betroffenen Personen informiert werden.

Daneben haben wir auch Untersuchungen von Amts wegen bei einer größeren Anzahl von Teststellen initiiert. Diese richteten sich darauf, sicherzustellen, dass der Schutz der Daten der Bürger:innen nicht dadurch geschwächt wird, dass die Testzentren Dienstleister:innen außerhalb des Europäischen Wirtschaftsraums in Anspruch nehmen.

Die Softwareanwendungen vieler Teststellen nutzen in erheblichem Umfang Cloud-Dienste für den Betrieb der Webseiten und für die Speicherung der Daten, z. B. der Testergebnisse. Dazu kommen E-Mail- und SMS-Versand-Dienste. Diese Dienste werden häufig von US-amerikanischen Dienstleister:innen betrieben. Oder von Dienstleister:innen, die ihrerseits wiederum US-amerikanische Dienstleister:innen als Unter-Dienstleister:innen einsetzen. Die Webseiten haben zudem häufig Inhalte von fremden Servern eingebunden und damit unzulässig personenbezogene Daten an deren Betreiber:innen offengelegt, oftmals auch hier wieder US-Unternehmen. Dies verursacht Risiken für die betroffenen Personen.[49]

Die meisten Teststellen, die wir kontaktierten, stellten die Verstöße freiwillig ab und wechselten bspw. die Dienstleister:innen für die Buchung der Tests, den Betrieb der Webseite oder den Versand von E-Mails. Zudem entfernten sie unzulässige Drittinhalte von ihren Webseiten. In etlichen Fällen mussten wir dafür zunächst grundlegende Aufklärung betreiben, weil die datenschutzrechtlichen Dimensionen überhaupt nicht erkannt worden waren. Als besonders problematisch erwies sich eine Teststelle, die für die gesamte E-Mail-Kommunikation einen Privatkunden-Account eines US-Dienstleisters nutzte.

Aufgrund der Vielzahl der bei uns zum Thema Teststellen eingegangenen und immer noch eingehenden Anfragen und Beschwerden haben wir auf unserer Webseite Informationen zu besonders häufig gestellten Fragen zur Verfügung gestellt.[50]

Im Zusammenhang mit den Bürgertestungen verarbeiten die Teststellen personenbezogene Daten einer großen Anzahl an Bürger:innen, darunter auch Ge-

[49] Siehe 1.1
[50] https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/teststellen

sundheitsdaten. Die große Anzahl an Beschwerden über Teststellen und an Hinweisen zu Sicherheitsmängeln, die uns erreichten, zeigen zusammen mit der Art und dem Umfang der von uns festgestellten Verstöße, dass das Thema Datenschutz bei einer Vielzahl dieser Unternehmer:innen nicht präsent ist, oder die Teststellen die datenschutzrechtlichen Vorgaben schlichtweg ignorieren. Die Berücksichtigung datenschutzrechtlicher Anforderungen bei der Zulassung der Teststellen und der Verweis auf Angebote zur datenschutzrechtlichen Schulung wäre wünschenswert gewesen. Dadurch hätten viele Datenschutzverstöße vermieden und die Daten der Bürger:innen besser geschützt werden können.

1.5 Anwesenheitsdokumentation und Kontaktnachverfolgung

Zur Pandemiebekämpfung hat der Gesetzgeber angeordnet, dass Veranstalter:innen, Restaurantbetreibende und andere Stellen bzw. Personen über die Anwesenheit von Gästen in ihren Räumen Buch führen müssen. Als elektronisches System für diesen Zweck etablierte sich eine von vielen Bundesländern geförderte Anwendung. Wir kontrollierten die Betreiberin dieser Anwendung, um Sicherheit und Datensparsamkeit durchzusetzen.

Eine wesentliche Methode der Bekämpfung der Corona-Pandemie besteht darin, dass die Gesundheitsämter die Kontakte von infizierten Personen feststellen und diese auffordern, sich abzusondern und testen zu lassen, um Infektionsketten zu unterbrechen. Die infizierten Personen kennen einige der Kontakte aus ihrem persönlichen Umfeld. Andere Personen, denen sie vielleicht bei Veranstaltungen, in der Bar oder in einem Geschäft begegnet sind, oder in deren Nähe sie sich bspw. in einem Restaurant oder einem Fußballstadion aufgehalten haben, sind ihnen nicht bekannt. Daher hat der Gesetzgeber die Veranstalter:innen und Betreiber:innen von Restaurants und vielen anderen Einrichtungen verpflichtet, über ihre Gäste Buch zu führen.

Dies geschah insbesondere bei kleinen Einrichtungen zunächst meistens mit Papierlisten oder Zetteln, in die sich die Gäste eintrugen. Dieses Verfahren warf Probleme auf, wenn Gäste die Namen und Adressen anderer Personen im selben Restaurant einsehen konnten, die Veranstalter:innen die gesammelten Daten für andere Zwecke missbrauchten oder staatliche Stellen unbefugt Einblick in die Listen nehmen wollten. Nicht zuletzt war die zum Teil erforderliche Übermittlung der Anwesenheitsdaten an Gesundheitsämter per Fax, Post oder nach einem Scan per E-Mail aufwendig und unsicher.

Es lag daher nahe, diese Zettelwirtschaft durch ein elektronisches Verfahren abzulösen. Eine Vielzahl von Anbieter:innen drängte auf den Markt. Eines dieser Angebote – eine App und das dahinterstehende System – konnte sich vorrangig durchsetzen. In der Tat sprach einiges für dieses System: Es vereinfachte die Aufnahme der Daten und die Übergabe an die Gesundheitsämter für die Veranstalter:innen drastisch. Gleichzeitig sicherte es die Namen und Adressdaten der Gäste durch Verschlüsselung vor dem Einblick der Veranstalter:innen und unbefugter Dritter.

Aus diesem Grund entschlossen sich dreizehn der sechzehn Bundesländer, dieses System zu fördern und die Anwendung zu empfehlen. Das Land Berlin passte seine SARS-CoV-2- Infektionsschutzmaßnahmenverordnung entsprechend an und reduzierte einige Anforderungen an die Anwesenheitsdokumentation, um den Veranstalter:innen den Einsatz des Systems im Einklang mit den infektionsschutzgesetzlichen Vorschriften zu ermöglichen.

So wuchs aus einer kleinen Anwendung eine Infrastruktur für nahezu die gesamte Bundesrepublik. Nach Angaben der Betreiberin der Anwendung installierten mehr als 35 Millionen Personen die App und nutzten das System. In der Tat wurde es vielerorts für die Bürger:innen eine beschwerliche Option, auf die App zu verzichten.

Sinnvoll wäre es gewesen, diese Infrastruktur in die öffentliche Hand zu überführen. Mit der Corona-Warn-App, die Begegnungen von Menschen anhand von Bluetooth-Signalen ihrer Smartphones feststellt und ihnen die Warnung der Kontakte bei Feststellung einer Infektion erlaubt, war dem Bund eine beispielhafte Lösung gelungen. Doch bei dem hier beschriebenen System blieb der Betrieb in privater Hand.

Gleichzeitig entwickelte sich die Pandemie und der Arbeitsanfall der Gesundheitsämter weiter. Bei hohen Infektionszahlen war es den Gesundheitsämtern kaum noch möglich, Infizierte individuell zu befragen und Kontaktpersonen über die Gefahr einer Infektion und ihre daraus resultierenden Pflichten zu informieren. Berge an Daten sammelten sich bei der Betreiberin des beschriebenen Systems, ohne dass die Gesundheitsämter auf die Daten zugriffen. Eine Reihe von Berliner Gesundheitsämtern hat die Software, die für den Abruf von Daten aus dem System erforderlich ist, nie produktiv verwendet.

Trotz der Hinweise der Datenschutzaufsichtsbehörden, darunter auch unserer Behörde, blieben die gesetzlichen Regelungen bestehen, die von den Veranstalter:innen verlangten, dass sie Name und Kontaktdaten ihrer Gäste registrieren. Die Corona-Warn-App zeichnet Namen und Kontaktdaten ihrer Nutzer:innen für den Zweck der Warnung nicht auf, da diese hierzu nicht benötigt werden. Sie allein zu nutzen, war den Veranstalter:innen jedoch infektionsschutzrechtlich verwehrt. Bei der Fortschreibung der infektionsschutzrechtlichen Regelungen wurde unsere Behörde nicht gehört.

Nachdem zunehmend Kritik an dem System der privaten Betreiberin geäußert wurde, erarbeitete die DSK unter unserer Federführung drei Stellungnahmen zur Kontaktnachverfolgung im Allgemeinen und zu dem betreffenden System im Besonderen. Außerdem sprach sich die DSK deutlich dafür aus, die Chancen der Corona-Warn-App zu nutzen, und hob die Vorteile dieses Verfahrens hervor[51].

Parallel kontrollierten wir als zuständige Aufsichtsbehörde das Verfahren bei der Betreiberin des Systems und führten intensive Gespräche zur Behebung von festgestellten Mängeln.

Ein erster rechtlicher Mangel bestand darin, dass die Betreiberin des Systems in eigener Verantwortung die Daten der Nutzenden aufnahm und im weiteren Verlauf verarbeitete, ohne dafür eine Rechtsgrundlage zu besitzen. Sie stützte sich auf einen Vertrag mit den Nutzenden, der so vage gestaltet war, dass die Betroffenen bei Vertragsabschluss nicht absehen konnten, worauf genau sie sich einließen. Die Betreiberin des Systems behielt sich zudem vor, die Nutzungsbedingungen und damit den Vertrag und darauf gründend ihre Berechtigung zur Datenverarbeitung jederzeit einseitig anzupassen. Eine Wahlmöglichkeit für die Betroffenen, die Datenverarbeitung auf die Übergabe der eingegebenen Daten an die betreffenden Veranstalter:innen zu beschränken, eröffnete sie nicht.

Das entspricht nicht der engen Bindung der Verarbeitung der Daten über die Anwesenheit von Personen bei Veranstaltungen an den infektionsschutzrechtlichen Zweck, die der Gesetzgeber vorgegeben hat. Diese Vorgabe gründet in der Sensitivität dieser Daten, die einen tiefen Einblick in das Sozialleben der Bürger:innen bieten.

[51] Pressemitteilung der DSK vom 30. April 2021; abrufbar unter https://www.datenschutzkonferenz-online.de/pressemitteilungen.html

Aus diesem Charakter der Daten und dem flächendeckenden Einsatz des Verfahrens folgen hohe Anforderungen an seine Sicherheit. Dem wurde es jedenfalls zum Zeitpunkt unserer Prüfung nicht gerecht. Im weiteren Verlauf des Jahres hat die Betreiberin dann jedoch an verschiedenen Punkten die Sicherheitseigenschaften der eingesetzten Systeme und Dienste gestärkt.

Problematisch bleibt jedoch, dass das System hochzentralisiert ist. Es speichert nicht nur die Daten der Bürger:innen. Es kontrolliert zum Prüfzeitpunkt auch weitgehend die Datenverarbeitung der Veranstalter:innen und der Gesundheitsämter. Unbefugten, die sich die Kontrolle über das System verschaffen könnten, würden alle Informationen offenliegen; durch die Möglichkeit der Manipulation der Veranstalter:innen- und Gesundheitsamtssoftware auch die doppelt verschlüsselten Namen und Adressdaten der Bürger:innen.

Zudem ließ sich in vielen Fällen die Identität der betroffenen Personen auch ohne Entschlüsselung ermitteln. Dies liegt daran, dass die App häufig mit dem System der Betreiberin kommuniziert. Die dabei anfallenden Verkehrsdaten erlauben vielfach die Identifizierung von Nutzenden der App. Über die so Identifizierten ist dann auch die Anwesenheit an den Orten bekannt, an denen sie die App genutzt haben. Denn die Orts- und Zeitangaben werden anders als Name und Adressdaten der Nutzenden nicht verschlüsselt gespeichert. Dabei wäre dieses Kommunikationsverhalten der App nicht notwendig: Das System hat einen Betriebsmodus, der mit vergleichsweise geringen Änderungen einen Betrieb ganz ohne Kommunikation der App mit dem System der Betreiberin erlaubt. Dazu weist die nutzende Person einfach mit ihrem Smartphone einen QR-Code vor, also ein quadratisches Punktraster, das ihre Kontaktdaten kodiert aufnimmt. Die Veranstalter:innen lesen dies mit einer eigenen App aus und speichern die kodierten Daten ab. Die Vorlage und Prüfung digitaler Impfzertifikate mit den Apps CovPass und CovPassCheck bzw. der Corona-Warn-App zeigen, dass die Voraussetzungen dafür bei den Veranstalter:innen und ihren Gästen gegeben sind.

Wir konfrontierten die Betreiberin des Systems mit den Mängeln und forderten sie auf, einen Maßnahmenplan vorzulegen und abzuarbeiten, mit dem diese beseitigt werden. Von weiteren Maßnahmen (z. B. einer Untersagung des Betriebs) haben wir bisher u. a. abgesehen, um in der laufenden Pandemiesituation den Veranstalter:innen kein Werkzeug zur Erfüllung ihrer infektionsschutzrechtlichen Verpflichtungen

aus der Hand zu nehmen. Stattdessen wirkten wir weiter auf die Betreiberin ein, um sie zu einem Umbau ihres Systems zu bewegen.

Besser ist jedoch die Nutzung eines dezentral operierenden Systems, wie es mit der Corona-Warn-App gegeben ist. Auch die Gesundheitsämter können mit einem solchen System aufgrund ihrer Expertise die Warnung von gefährdeten Personen steuern und Erkenntnisse über Orte mit hoher Infektionsgefährdung gewinnen. Der Schlüssel, der die Tür zu diesem Weg öffnet, liegt nicht in den Händen von Veranstalter:innen oder den Betreiber:innen von Apps, sondern in der Hand des Gesetzgebers.

Ein flächendeckendes System, das Daten über das Sozialleben einer sehr großen Zahl von Bürger:innen erfasst, ohne dass diesen eine große Wahlfreiheit bei der Nutzung bleibt, gehört in die öffentliche Hand. Es muss von Grund auf kompetent und unter öffentlicher Beobachtung, datensparsam, mit starker Zweckbindung und sicherheitsorientiert gestaltet werden.

2 Digitale Verwaltung

2.1 Stand der Digitalisierungsprojekte

Die Corona-Pandemie hat den Digitalisierungsrückstand der Verwaltung an vielen Stellen offengelegt. Aus Sicht der den Einsatz der Informations- und Kommunikationstechnik in der Verwaltung koordinierenden IKT-Steuerung bei der Senatsverwaltung für Inneres, Digitalisierung und Sport hat die Krise der Digitalisierung aber auch neuen Schwung gegeben. Viele zentrale Vorhaben sollen nun Schlag auf Schlag umgesetzt werden. Wir beraten die IKT-Steuerung dabei intensiv hinsichtlich der vielen noch offenen Fragen.

Nachdem die IKT-Steuerung im vergangenen Jahr den IKT-Basisdienst „Digitaler Antrag“ in den Regelbetrieb überführt hat,[52] stand in diesem Jahr das Projekt „Digitale Akte“ im Fokus. Sie ist ein zentraler Baustein für eine moderne digitale Verwaltung und ermöglicht eine elektronische und medienbruchfreie Aktenführung und -bearbeitung. Entsprechend den Vorgaben des Berliner E-Government-Gesetzes (EGovG Bln) soll dieser IKT-Basisdienst künftig eine digitale Durchführung des Dokumentenmanagements, der Vorgangsbearbeitung sowie der revisionssicheren Langzeitspeicherung sicherstellen und

[52] Siehe JB 2020, 2.1

so die Leistungsfähigkeit der Verwaltung stärken.

Bei der Einführung der „Digitalen Akte“, die an ca. 80.000 Arbeitsplätzen der Verwaltung nutzbar gemacht werden muss, handelt es sich um ein Großprojekt. Wir sind von Beginn der Pilotphase an in das Projekt einbezogen worden und beraten die IKT-Steuerung zu den hiermit verbundenen zum Teil sehr komplexen Datenschutzfragen.

Projekte der Verwaltungsdigitalisierung wie dieses beziehen regelmäßig eine sehr große Zahl von öffentlichen Stellen verschiedener Verwaltungsebenen ein. Auch bei der „Digitalen Akte“ bedarf es zunächst der Klärung, welche Beteiligten für welche Datenverarbeitungsvorgänge verantwortlich sind und welche Rechte der davon betroffenen Personen, z. B. auf Auskunft, Berichtigung oder Löschung, sie sicherzustellen haben. Pauschal anzunehmen, die beteiligten Behörden seien für die Datenverarbeitung gemeinsam verantwortlich,[53] führt zu erheblichen Abgrenzungsschwierigkeiten in der Praxis und lässt sich mit den geltenden Datenschutzvorschriften nicht in Einklang bringen. Problematisch ist dabei regelmäßig die fehlende Rechtsgrundlage für eine Datenverarbeitung seitens der Senatsverwaltung für Inneres, Digitalisierung und Sport, bei der die IKT-Steuerung angesiedelt ist. Wichtig ist zudem, von vornherein Sorge dafür zu tragen, dass die Rollen und Berechtigungen innerhalb der einzelnen Verwaltungen für Zugriffe auf die mit der „Digitalen Akte“ verarbeiteten personenbezogenen Daten in der Weise festgelegt sind, dass die datenschutzrechtlichen Anforderungen eingehalten werden.

Im Rahmen unserer Beratungen haben wir die Projektverantwortlichen im Hinblick auf diese Anforderungen sensibilisiert und stehen weiterhin intensiv im Austausch.

Das EGovG Bln, das die rechtlichen Bedingungen für die Umstellung der Verwaltungsverfahren und -strukturen auf die Nutzung zentraler informations- und kommunikationstechnischer Strukturen schafft, verpflichtet den Senat zu einer Gesetzesevaluation.[54]

Diese erfolgte im Mai dieses Jahres. Dabei stellte sich heraus, dass der Datenschutz nicht als ein gravierendes Hindernis für die Verwaltungsdigitalisierung wahrgenommen wird. So nannten die im Rahmen der Evaluierung befragten Bediensteten den -

[53] i. S. v. Art. 26 Datenschutz-Grundverordnung (DS-GVO)
[54] § 26 EGovG Bln

Datenschutz erst auf Platz 7 von 11 möglichen Hindernissen der Verwaltungsdigitalisierung.[55] Stattdessen wiesen sie vor allem auf fehlende zentral entwickelte IT-Lösungen und Standards, fehlende Budgets sowie fehlende Digitalisierungskompetenzen bei den Beschäftigten hin.[56] Anders als häufig dargestellt, ist der Datenschutz in der Praxis also nicht der große Stolperstein bei der Verwaltungsdigitalisierung.

Mit der Einführung der „Digitalen Akte“ in der Verwaltung stellen sich viele datenschutzrechtliche Herausforderungen. Es ist wichtig, dass die IKT-Steuerung und die beteiligten Verwaltungen die Pilotphase nutzen, um die datenschutzrechtlichen Anforderungen umzusetzen. Wir unterstützen diesen Prozess mit unserer Beratung.

2.2 Einsatz von Videokonferenzsystemen

Auch in diesem Jahr waren Videokonferenzsysteme von besonderer Bedeutung, um die Funktionsfähigkeit der Verwaltung sowie der Wirtschaft in Zeiten der Pandemie aufrechtzuerhalten. Wir haben unsere Unterstützung für Verantwortliche bei der Auswahl datenschutzkonformer Dienste ausgebaut, aber auch Verfahren wegen der Nutzung rechtswidriger Videokonferenzdienste geführt. Während wir bei manchen Anbieter:innen erhebliche datenschutzrechtliche Fortschritte erzielen konnten, mussten wir bei der Nutzung von Videokonferenzsystemen gerade in der Verwaltung oftmals erhebliche Rechtsverstöße feststellen.

Unsere bereits im letzten Jahr erstmalig erschienenen „Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten“ haben wir in diesem Jahr aktualisiert und erweitert.[57] Erfreuliches Ergebnis war, dass wir – nach teilweise sehr umfangreichem Austausch und umfassenden Änderungen bei den Anbieter:innen – nun insgesamt elf Anbieter:innen auf der rechtlichen Ebene durch das bewährte Ampel-System mit „Grün“ bewerten konnten. Diese haben wir anschließend einer technischen Prüfung unterzogen. Auch bei anderen, letztlich nicht mit „Grün“ bewerteten Anbieter:innen konnten wir erhebliche, wenn auch nicht ausreichende Verbesserungen erreichen.

Auf der technischen Ebene sind die Hinweise jetzt

[55] Siehe „Evaluation des Berliner E-Government-Gesetzes“ vom 21. Mai 2021, S. 48 f., Abgeordnetenhaus Berlin, H-18/2765.E; https://www.parlament-berlin.de/adosservice/18/Haupt/vorgang/h18-2765.E-v.pdf
[56] Siehe „Evaluation des Berliner E-Government-Gesetzes“ vom 21. Mai 2021, S. 178, Abgeordnetenhaus Berlin, H-18/2765.E; https://www.parlament-berlin.de/adosservice/18/Haupt/vorgang/h18-2765.E-v.pdf
[57] Siehe https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2021-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_VideokonferenzDienste.pdf

deutlich ausdifferenziert und umfassen verschiedene Anwendungsfälle. Für drei unterschiedliche Szenarien können Unternehmen, Behörden und Vereine auf den ersten Blick erkennen, welche der getesteten Videokonferenzdienste für sie in Betracht kommen: Für jeden Anwendungsfall gibt es eine eigene Ampel. Zu jedem der 23 geprüften Dienste bzw. Dienstegruppen enthält das Papier zudem teils sehr detaillierte Erläuterungen der Mängel und Hinweise zur Konfiguration.

Die Verwaltung haben wir darüber hinaus sehr umfangreich bei der Ausschreibung für Nachfolger:innen der bisherigen zentral beschafften Videokonferenzlösungen unterstützt. Während diese Zusammenarbeit sehr konstruktiv und erfolgreich war, konnten wir in Zusammenarbeit mit der Senatskanzlei und der IKT-Steuerung keine Möglichkeit finden, einen von einigen Senatsverwaltungen und der Senatskanzlei in verschiedenen Formen genutzten Cloud-Dienst rechtskonform einzusetzen. Wir haben die betreffenden Senatsverwaltungen und die Senatskanzlei daraufhin aufgefordert, die Nutzung einzustellen. Dazu waren diese nicht bereit. Die Senatskanzlei als Verhandlungsführerin bot aber technische und organisatorische Änderungen an, um eine übergangsweise tolerierbare Gestaltung zu erreichen. Die diesbezüglichen Gespräche konnten im Berichtszeitraum noch nicht abgeschlossen werden. Dagegen nutzt der „Lernraum Berlin“ nunmehr ein datenschutzkonformes Videokonferenzsystem.[58]

Hinsichtlich des Einsatzes von Videokonferenzsystemen gibt es bisher keine vertiefte Auseinandersetzung der Berliner Beauftragten für Datenschutz und Informationsfreiheit mit den rechtlichen Ansichten der Senatskanzlei. Dennoch wurde lösungsorientiert inzwischen eine On-Premise-Lösung für das Haus angeschafft, die die wesentlichen Beanstandungen im Datenschutz entkräftet. An einer datenschutzkonformen Nutzung der Cloud-Dienste von Webex arbeitet die Senatskanzlei weiterhin.

Es gibt eine Vielzahl rechtskonformer Videokonferenzdienste für die unterschiedlichsten Einsatzzwecke. Die Corona-Pandemie kann nicht den Einsatz rechtswidriger Dienste begründen.

2.3 Umsetzung des Onlinezugangsgesetzes in Bund und Ländern

Bund, Länder und Kommunen stehen bei der Umsetzung des Onlinezugangsgesetzes (OZG) weiter unter Druck.[59] Bis Ende 2022 müssen sie ihre Verwaltungsleistungen über Verwaltungsportale auch online anbieten. Die identifizierten 575 zu digitalisierenden Verwaltungsleistungen sind den einzelnen Bundesländern nach Themenfeldern zugeordnet. Die Digitalisierung erfolgt arbeitsteilig nach dem sog. „Einer-für-Alle-Prinzip“ („EfA-Prinzip“). Das bedeutet, dass jedes Bundesland die Verwaltungsleistungen aus seinem Themenfeld so digitalisiert, dass die entwickelten Lösungen von den anderen Bundesländern übernommen und genutzt werden können.

[58] Siehe 1.2.3
[59] Siehe auch JB 2020, 2.2

Da Datenschutzfragen im Zusammenhang mit der OZG-Umsetzung alle Bundesländer und damit auch sämtliche Datenschutzaufsichtsbehörden betreffen, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) im Herbst 2020 eine Unterarbeitsgruppe damit beauftragt, sich mit den datenschutzrechtlichen Fragen, die sich bei der Entwicklung von Verwaltungsportalen und anderen Fachanwendungen stellen, zu befassen und zu bewerten und gleichzeitig einen Austausch mit dem Bundesministerium des Innern und für Heimat und der Föderalen IT-Kooperation zu führen und koordiniert vorzugehen. Wir beteiligen uns seit Beginn aktiv an dieser Arbeitsgruppe.

Das Land Berlin ist im Rahmen der OZG-Umsetzung gemeinsam mit dem Bundesministerium des Innern und für Heimat und den Ländern Brandenburg, Hamburg und Thüringen für das Themenfeld „Querschnittsleistungen“ verantwortlich. In diesem Bereich wurde zuletzt vor allem die „Basiskomponente Nachweisabruf“ entwickelt. Diese unterstützt eine digitale und medienbruchfreie Nachweiserbringung bei der Beantragung von Verwaltungsleistungen. Sowohl Bürger:innen als auch Unternehmen sollen die Möglichkeit erhalten, den Behörden bestimmte Nachweise, z. B. eine Geburtsurkunde, eine Meldebescheinigung oder ein Führungszeugnis, elektronisch zu erbringen. Mit der „Basiskomponente Nachweisabruf“ soll es möglich sein, durch die Verbindung von Antrags- und Fachverfahren mit den entsprechenden Registern Abrufe über einen zentralen Service zu ermöglichen. Wir haben der IKT-Steuerung bei den sich im Rahmen der Realisierung dieses Projektes stellenden Fragen unsere Unterstützung angeboten.

Ein weiteres, als besonders innovativ präsentiertes Projekt im Rahmen der OZG-Umsetzung ist das „Digitale Schulzeugnis“. Im Rahmen eines Pilotprojekts[60] soll in Berlin die durch Sachsen-Anhalt gemeinsam mit der Bundesdruckerei entwickelte Lösung zur Digitalisierung von Schulzeugnissen eingeführt werden. Mit diesem Projekt soll es den Bildungseinrichtungen ermöglicht werden, fälschungssichere digitale Zeugnisse zu erstellen. Hierfür kommt die Blockchain-Technologie zur Anwendung. Grundlage ist dabei eine öffentliche Blockchain, die ausschließlich von den in der Genossenschaft „govdigital“ verbundenen öffentlichen Rechenzentren betrieben wird. Projektverantwortliche sind neben der Bundesdruckerei in Berlin die Se-

Zur Realisierung der Leistungen gemäß Leistungskatalog zum Onlinezugangsgesetz für den Bereich Bildung besteht eine enge Zusammenarbeit mit dem Land Sachsen-Anhalt.

Die von dem Land Sachsen-Anhalt ursprünglich favorisierte Blockchaintechnologie wurde zwischenzeitlich verworfen und eine Evaluation für mögliche technische Alternativen beauftragt. Das Land Berlin prüft unter den gegebenen Bedingungen derzeit, ob eine „eigene“ Lösung sinnvoll ist. Dies geschieht in dem gemeinsamen Projekt der Senatsverwaltung für Bildung, Jugend und Familie, der Senatsverwaltung für Wirtschaft, Energie und Betriebe und dem ITDZ Berlin.

[60] An diesem Projekt sind neben Berlin die Bundesländer Rheinland-Pfalz und Nordrhein-Westfalen beteiligt.

natsverwaltung für Bildung, Jugend und Familie sowie das IT-Dienstleistungszentrum, die uns bereits frühzeitig in das Projekt eingebunden haben.

Die Senatsverwaltung für Bildung, Jugend und Familie hat im Oktober für das Projekt den Berliner Verwaltungspreis in der Kategorie Innovation erhalten. Dies hat uns erstaunt, denn die rechtlichen Voraussetzungen für den Start des Projektes sind derzeit noch nicht gegeben: Die Ausstellung digitaler Zeugnisse ist nach aktueller Gesetzeslage sowohl schulrechtlich[61] als auch verwaltungsverfahrensrechtlich[62] in Berlin ausgeschlossen, was von der Bildungsverwaltung uns ggü. eingeräumt wurde. Auch fehlt derzeit noch die vollständige technische Dokumentation des Projekts.

Neben der Schaffung der notwendigen Rechtsgrundlagen ist in technischer Hinsicht zu berücksichtigen, dass die in einer Blockchain gespeicherten Daten, unabhängig davon, wer diese betreibt, niemals wieder gelöscht werden können. Es muss also sichergestellt werden, dass die Betroffenen ihr Recht auf Löschung oder Berichtigung ihrer personenbezogenen Daten verwirklichen können. Die Projektplanung sieht dazu vor, die in den Zeugnissen enthaltenen personenbezogenen Daten lediglich als „Hash-Werte“, d. h. als kryptografische Prüfsummen, in der Blockchain zu speichern. Uns ist wichtig, dass die Projektverantwortlichen genau evaluieren, ob sich die Daten zu einem späteren Zeitpunkt nicht einfach durch Ausprobieren erraten lassen und so den jeweiligen Personen wieder zugeordnet werden können. Da sich in der genutzten Blockchain der „govdigital“ alle beteiligten Parteien per definitionem vertrauen, entfallen aufwendige Prüfverfahren bei der Erstellung eines neuen Blocks. Damit wird die Blockchain letztlich aber nur wie eine einfache Datenbank genutzt. Es stellt sich also die Frage, welchen Mehrwert das neue Verfahren in technischer Hinsicht bringt und ob das durchaus unterstützenswerte Ziel, die Schulzeugnisse digital zur Verfügung zu stellen, sich nicht auch mit der in dem Konzept ohnehin vorgesehenen digitalen Signatur erreichen lässt. Wir werden das Projekt weiterhin begleiten und stehen den Projektverantwortlichen beratend zur Seite, erwarten jedoch, dass die notwendigen rechtlichen Voraussetzungen jetzt geschaffen werden.

Die OZG-Umsetzung stellt auch in datenschutzrechtlicher Hinsicht eine besondere Herausforderung

[61] Siehe § 58 Abs. 2 Schulgesetz (SchulG)
[62] Siehe § 2 Abs. 2 Satz 2 Gesetz über das Verfahren der Berliner Verwaltung (VwVfG Bln)

dar. Wir sind überzeugt, dass eine erfolgreiche Verwaltungsdigitalisierung nur gelingen kann, wenn die Bürger:innen von vornherein sicher sein können, dass mit ihren personenbezogenen Daten sorgsam umgegangen wird. Die Schaffung von Transparenz ist von besonderer Bedeutung, um das notwendige Vertrauen bei der Inanspruchnahme digitaler Dienstleistungen zu erreichen.

3 Inneres und Sport

3.1 Polizei übermittelt widerrechtlich Versammlungsdaten

Zwei förmliche Beanstandungen ggü. der Polizei in einem einzigen Prüfverfahren sind ein Novum. Leider sahen wir uns aufgrund der fehlenden Kooperationsbereitschaft der Polizei und einer eklatant rechtswidrigen Datenübermittlung durch die Polizei an das Verwaltungsgericht dazu gezwungen.

Der ersten Beanstandung wurde durch die Übersendung der Klageschrift an die Berliner Beauftragte für Datenschutz und Informationsfreiheit Rechnung getragen.

Anlass unseres Prüfverfahrens war die Meldung einer Datenpanne durch die Polizei, in der diese uns mitteilte, dass sie im Rahmen eines verwaltungsgerichtlichen Verfahrens eine Gefährdungsbewertung zusammen mit den betreffenden Verwaltungsvorgängen an das Verwaltungsgericht in ungeschwärzter Form übersandt hatte.

Was die zweite Beanstandung wegen der Übersendung des Verwaltungsvorgangs in ungeschwärzter Form durch die Polizei an das VG betrifft, ist die Polizei ihrer gesetzlichen Vorlagepflicht gegenüber dem Verwaltungsgericht nach § 99 Abs. 1 S. 1 VwGO nachgekommen. Danach sind Behörden verpflichtet, den Verwaltungsgerichten amtliche Auskünfte zu erteilen und Akten oder Urkunden vorzulegen sowie elektronische Dokumente zu übermitteln. Nach dem Amtsermittlungsgrundsatz (§ 86 Abs. 1 VwGO) muss das Gericht die tatsächlichen Grundlagen für seine Entscheidung selbst ermitteln und seine rechtliche Auffassung unabhängig von der Verwaltung gewinnen und begründen. Darüber, welche Informationen zur Beurteilung des Streitgegenstandes entscheidungserheblich sind, entscheidet allein das Gericht. Der behördliche Verwaltungsvorgang ist deshalb vollständig an das Gericht zu übermitteln. Dazu gehören auch die für die Bearbeitung der Versammlungsanmeldung ggfs. erforderlichen Gefährdungsbewertungen.

Zuvor hatten Medien darüber berichtet, dass die betreffenden Polizeiakten einem Rechtsanwalt im Zuge einer Akteneinsicht beim Verwaltungsgericht vorgelegt worden seien. Der Anwalt hatte im Auftrag seines Mandanten im Zusammenhang mit einer Versammlung geklagt. Bei der Akteneinsicht habe er laut Medienberichten Einblick in Daten der Anmelder:innen von Gegendemonstrationen erhalten.

Zwar ermächtigt § 99 Abs. 1 S. 2 VwGO die Behörde unter den dort genannten Voraussetzungen zur Verweigerung der Vorlage und der Auskunft, verpflichtet sie aber nicht dazu. Es handelt sich mithin um eine komplexe Ermessensentscheidung, die unter Abwägung der im Spannungsfeld stehenden öffentlichen und privaten Interessen vorzunehmen ist. Diesbezüglich ist allerdings keineswegs zwingend anzunehmen, dass im vorliegenden Fall das behördliche Ermessen auf Null reduziert, mithin als einzig rechtlich zulässige

Entscheidung die teilweise Zurückhaltung von Informationen aus dem Verwaltungsvorgang gegenüber dem Gericht verblieben war.

Die Polizei beantwortete infolge unsere Fragen zur Datenpannenmeldung und teilte zudem mit, dass die Meldung lediglich vorsorglich aufgrund der medialen Berichterstattung erfolgt sei, die Datenübermittlung an das Verwaltungsgericht jedoch für zulässig erachtet werde.

Aus den Antworten der Polizei war ersichtlich, dass in der mit den Verwaltungsvorgängen übersandten Gefährdungsbewertung Daten von Personen, die gleichgelagerte Versammlungen und Gegenversammlungen angemeldet hatten bzw. für die Leitung solcher Versammlungen vorgesehen waren, enthalten waren. Neben Vor- und Zunamen betraf dies polizeiliche Erkenntnisse zu diesen Personen. So wurde bspw. ausgeführt, ob und wenn ja, welche allgemeinen strafrechtlichen und staatsschutzrelevanten Erkenntnisse zu den betroffenen Personen vorliegen. Zudem waren in der Gefährdungsbewertung Daten weiterer Personen enthalten, die die Polizei in Verbindung zu den angemeldeten Versammlungen setzte, weil sie bspw. früher ähnliche Versammlungen angemeldet hatten oder als Unterstützer:innen der angemeldeten Versammlungen galten.

Im Übrigen ist anzumerken, dass keine Anhaltspunkte für die Annahme vorliegen, der Kläger könnte die durch Akteneinsicht erlang-ten Daten missbräuchlich genutzt – diese insbesondere unbefugte an Dritte weitergegeben haben.

Abgesehen von der Gefährdungsbewertung enthielten die von der Polizei an das Verwaltungsgericht übersandten Akten u. a. auch die E-Mail der Anmelderin einer inhaltlich nicht im Zusammenhang mit dem Streitgegenstand stehenden Veranstaltung; Name, Adresse, Geburtsdatum, Telefonnummer und E-Mail-Adresse eines Hinweisgebers zur streitgegenständlichen Versammlung sowie Name und E-Mail-Adresse eines Medienvertreters.

Der Sachverhalt wurde allerdings - wie von der Berliner Beauftragten für Datenschutz und Informationsfreiheit ausgeführt - zum Anlass genommen, die Mitarbeitenden der Polizei erneut für eine sehr sorgfältige Einzelfallprüfung zu sensibilisieren, ob schutzwürdige personenbezogene Daten Dritter vor Übersendung von Verwaltungsvorgängen an Gerichte nach § 99 Abs. 1 S. 2 VwGO geschwärzt werden sollten.

Zur abschließenden Beurteilung der Rechtslage baten wir die Polizei daraufhin mehrfach vergeblich um Übersendung der Klageschrift. Die Polizei teilte uns schließlich mit, dass sie unserer Bitte leider nicht nachkommen könne, weil sie nicht Urheberin der erbetenen Klageschrift und daher nicht berechtigt sei, diese zu übermitteln. Ferner sei das Dokument nicht Teil der an das Verwaltungsgericht übersandten Akten.

Hier mussten wir die erste Beanstandung aussprechen:

Die Polizei ist gesetzlich verpflichtet, uns alle Informationen, die für die Erfüllung unserer Aufgaben

erforderlich sind, bereitzustellen.[63] Zudem besteht die Pflicht, mit uns bei der Erfüllung unserer Aufgaben zusammenzuarbeiten.[64] Zu unseren Aufgaben gehört es, die Anwendung der Vorschriften über den Datenschutz zu überwachen und durchzusetzen sowie Untersuchungen über die Anwendung der Vorschriften über den Datenschutz durchzuführen.[65] Die Klageschrift ist zur Erfüllung dieser Aufgaben erforderlich, weil zur rechtlichen Beurteilung der Rechtmäßigkeit der Datenübermittlung die Kenntnis des Streitgegenstands, der sich aus der Klageschrift ergibt, entscheidend ist.

Die gesetzlichen Pflichten der Polizei zur Bereitstellung dieser Informationen sowie zur Zusammenarbeit sind dabei nicht begrenzt durch etwaige fremde Urheberschaften dieser Informationen. Einer solchen Logik folgend wäre es für uns auch in vielen Fällen kaum möglich, die Rechtmäßigkeit einer Datenverarbeitung durch verantwortliche Stellen zu prüfen, weil die dort vorliegenden Informationen in Form von Unterlagen oft eine Urheberschaft außerhalb dieser Stellen haben. Man kommt bei der Prüfung der Rechtmäßigkeit einer Datenverarbeitung also regelmäßig nicht umhin, auch Informationen fremder Urheberschaft zu erhalten. Demgemäß weit hat der Gesetzgeber unsere Befugnisse gefasst.

Dies hat schließlich auch die Polizei eingesehen und uns in Folge unserer Beanstandung eine Kopie der Klageschrift übersandt.

Nun war uns eine rechtliche Bewertung der beschriebenen Datenübermittlung möglich, die zur zweiten Beanstandung führte:

Die Übersendung der Akten durch die Polizei an das Verwaltungsgericht ohne vorherige Schwärzung der im Sachverhalt beschriebenen personenbezogenen Daten war rechtswidrig.[66]

Insbesondere kann eine solche Datenübermittlung nicht auf § 99 Abs. 1 Verwaltungsgerichtsordnung (VwGO) gestützt werden. Nach dieser Norm sind Behörden zwar ggü. dem zuständigen Verwaltungsgericht zur Vorlage von Urkunden oder Akten, zur Übermittlung elektronischer Dokumente und zu Auskünften verpflichtet. Jedoch kann dies verweigert werden, wenn das Bekanntwerden des Inhalts dem Wohl des Bundes oder eines Landes Nachteile

[63] § 13 Abs. 4 Nr. 2 BlnDSG
[64] § 54 BlnDSG
[65] § 11 Abs. 1 Satz 1 Nr. 1, 8 BlnDSG
[66] Verstoß gegen § 32 Abs. 1 Nr. 1 BlnDSG i. V. m. § 99 Abs. 1 Verwaltungsgerichtsordnung (VwGO)

bereiten würde oder wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheim gehalten werden müssen.

Ihrem Wesen nach grds.[67] geheim zu halten sind personenbezogene Daten Dritter, die in zu übermittelnden Unterlagen aus verschiedenen Gründen und in unterschiedlichen Zusammenhängen erwähnt werden.[68] Unstreitig ist jedoch auch, dass im Zusammenhang mit der Berufung auf eine wesensgemäße Geheimhaltungsbedürftigkeit ein strenger Maßstab anzulegen ist, weil hierdurch die richterliche Aufklärungs- und Rechtsfindungstätigkeit eingeschränkt wird.[69] Daher ist eine sorgfältige Abwägung der Geheimhaltungsinteressen mit den im Zusammenhang mit dem Gerichtsverfahren - bestehenden Informationsinteressen unter Würdigung des gesamten Sachverhalts im Einzelfall vorzunehmen.[70]

Im vorliegenden Fall ist bereits äußerst zweifelhaft, ob überhaupt ein gerichtliches Interesse an den von der Polizei übermittelten personenbezogenen Daten von Personen, die gleichgelagerte Versammlungen und Gegenversammlungen angemeldet haben oder hatten bzw. für die Leitung solcher Versammlungen vorgesehen waren, bestand.

Für die Bewertung des Streitgegenstands konnte es zwar von Interesse sein, ob zum selben Zeitpunkt gleichgelagerte Versammlungen und Gegenversammlungen angemeldet wurden und welcher Verlauf dieser Versammlungen aufgrund früherer polizeilicher Erkenntnisse zu erwarten war. Jedoch muss man hierfür in aller Regel nicht wissen, welchen Vor- und Zunamen die Anmeldenden bzw. Leitungen anderer Versammlungen haben und welchen konkreten Personen polizeiliche Erkenntnisse zugeordnet werden. Insoweit genügen regelmäßig anonymisierte Angaben. Vorliegend kommt erschwerend hinzu, dass der Streitgegenstand keinen direkten Bezug zu anderen Versammlungen hatte.

Die gleichen Überlegungen gelten grds. auch für Daten von Personen, die bspw. früher ähnliche Versammlungen angemeldet hatten oder als Unterstützer:innen der angemeldeten Versammlungen galten. Allenfalls könnten insoweit in Einzelfällen personenbezogene Daten im Zusammenhang mit der

[67] D. h. in der Regel, die Ausnahmen zulässt
[68] st. Rspr., vgl. etwa BVerwG, Beschluss vom 19. April 2010 – 20 F 13/09, Rn. 22; BVerwG, Beschluss vom 28. Juli 2015 – 20 F 3.15, Rn. 16 mit jeweils weiteren Nachweisen
[69] Siehe Schoch/Schneider VwGO/Rudisile VwGO § 99, Rn. 18 mwNw
[70] Siehe BVerwG, Beschluss vom 10. Januar 2017 – 20 F 3.16, Rn. 10

streitgegenständlichen Versammlung von Interesse sein. Hinsichtlich der übrigen Daten Dritter war keinerlei Interesse des Verwaltungsgerichts erkennbar.

Selbst wenn davon auszugehen wäre, dass an den im Sachverhalt beschriebenen personenbezogenen Daten von Anmeldenden anderer Versammlungen sowie an den mit diesen Versammlungen in Verbindung stehenden sonstigen Dritten ein abstraktes - gerichtliches Informationsinteresse besteht, überwiegen vorliegend die Interessen der Betroffenen an der Geheimhaltung ihrer personenbezogenen Daten.

Hierbei ist zunächst zu berücksichtigen, dass Personen, die Versammlungen durchführen bzw. leiten wollen, grds. gesetzlich verpflichtet sind, diese vorher bei der Polizei anzumelden. Sie können sich demnach regelmäßig einer Erhebung und Weiterverarbeitung ihrer Daten durch die Polizei nicht entziehen, wenn sie ihr Grundrecht auf Versammlungsfreiheit wahrnehmen wollen. An eine zweckändernde Verarbeitung dieser Daten sind bereits aus diesen Gründen hohe Maßstäbe anzusetzen.

Hinzu kommt, dass für die personenbezogenen Daten, die im Zusammenhang mit Gegendemonstrationen zur streitgegenständlichen Versammlung in den polizeilichen Verwaltungsvorgängen gespeichert sind und von der Polizei an das Verwaltungsgericht übermittelt wurden, die allgemeine Gefahr besteht, dass sie durch Akteneinsichtnahme des Klägers oder der Klägerin oder Dritter an unbefugte Personen gelangen und die Betroffenen hierdurch möglicherweise einer persönlichen Verfolgung ausgesetzt sind. Insoweit sei bspw. auf sog. Feindeslisten verwiesen, in denen Daten missliebiger Personen gesammelt und die zum Teil mit ausdrücklichen oder subtilen Drohungen oder Hinweisen vorwiegend im Internet veröffentlicht werden.

Zu beachten ist auch, dass Angaben zu politischen Meinungen, die sich aus der Anmeldung bzw. Teilnahme an Versammlungen ablesen lassen, zu den Kategorien besonderer personenbezogener Daten zählen und daher besonders schutzwürdig sind.[71] Auch strafrechtliche und staatsschutzrelevante Erkenntnisse können aus Sicht der Betroffenen sehr sensitiv sein, weshalb auch insoweit das Geheimhaltungsinteresse schwer wiegt.

Ferner ist zu berücksichtigen, dass die Betroffenen nicht selbst an der streitgegenständlichen Versamm-

[71] Siehe § 33 i. V. m. § 31 Nr. 14 BlnDSG

lung sowie am diesbezüglichen Gerichtsverfahren beteiligt sind, demnach über die Verarbeitung ihrer Daten in diesem Zusammenhang regelmäßig nicht informiert sind und somit auch nicht ihre Betroffenenrechte wahrnehmen können.

Im Übrigen ist anzumerken, dass es sich um eine zurückliegende Versammlung gehandelt hat. Das Gerichtsverfahren war insofern nicht eilbedürftig. Eine Nachforderung von benötigten personenbezogenen Daten durch das Gericht wäre also zu einem späteren Zeitpunkt problemlos möglich gewesen.

Die Polizei zeigte sich mit der Beanstandung im Hinblick auf die Datenübermittlung an das Verwaltungsgericht nicht einverstanden, teilte jedoch mit, dass der Fall zum Anlass genommen worden sei, die Mitarbeitenden noch einmal zu sensibilisieren, zukünftig verstärkt sehr sorgfältig in jedem Einzelfall zu prüfen, ob schutzbedürftige Daten Dritter vor der Übersendung von Verwaltungsvorgängen an Gerichte geschwärzt werden müssen.

3.2 Auskunftsrechte gegenüber der Polizei ohne Ausweiskopie möglich

Jede Person soll grds. in Erfahrung bringen können, welche Daten die Polizei über sie speichert. Ein solches Auskunftsverfahren sieht das Berliner Datenschutzgesetz (BlnDSG) vor. Im letzten Jahr hat das Verwaltungsgericht über einen Fall entschieden, der dieses Verfahren nun für die Bürger:innen vereinfacht.[72] Die Polizei hat bisher – nach eigenen Angaben zur Betrugsprävention – Auskunftsersuchen nur bearbeitet, wenn die Bürger:innen ihrem Antrag eine Ausweiskopie beigefügt hatten.

Nach der Rechtsprechung des Verwaltungsgerichts darf die Polizei allerdings nur bei Zweifeln an der Identität der betroffenen Person zusätzliche Informationen anfordern.[73] Hierauf haben wir die Polizei hingewiesen und sie dazu aufgefordert, das bisherige Antragsverfahren zu ändern. Dort hat man uns versichert, dass zukünftig nur noch in Zweifelsfällen eine Ausweiskopie nachgefordert werde. Da das Gesetz „begründete Zweifel“ fordert, sollte die Polizei in diesen Fällen zudem in der Lage sein, ihre Bedenken erläutern zu können.

Zur Beschleunigung der Bearbeitung hatte die Polizei vorgesehen, in Zweifelsfällen eine Meldeabfrage über das IT-Verfahren Einwohnerwesen (EWW)

Auf die entsprechende Aufforderung der Berliner Beauftragten für Datenschutz und Informationsfreiheit hin wurden die Arbeitsabläufe im für die Auskunftsantragsbearbeitung zuständigen LKA 512 dahingehend geändert, dass im Rahmen der Anträge nach § 50 ASOG Bln grundsätzlich keine Ausweiskopien der Antragstellenden mehr verlangt werden. Das Übersenden einer Ausweiskopie bleibt allerdings auf freiwilliger Basis möglich; dies wird entsprechend auf der Internetseite der Polizei Berlin kommuniziert.

Lediglich in Fällen ungeklärter Identitäten wird im Einzelfall eine Ausweiskopie von den Antragstellenden nachgefordert, um begründete Zweifel an der Identität auszuräumen.

Meldeabfragen über das IT-Verfahren Einwohnerwesen (EWW) werden seit Juni 2022 vom LKA 512 in Ermangelung einer Rechtsgrundlage nicht mehr vorgenommen.

[72] VG Berlin, Urteil vom 31. August 2020 – VG 1 K 90.19
[73] Siehe § 45 Abs. 4 BlnDSG

durchzuführen. Hierfür besteht jedoch keine Rechtsgrundlage, da das Gesetz nur erlaubt, Informationen bei der betroffenen Person selbst anzufordern[74]. Eine solche Abfrage wäre auch nicht erforderlich. Meldet sich eine betroffene Person unter Angabe ihres Namens und ihrer Wohnanschrift, sollten regelmäßig bereits die bei der Polizei gespeicherten Daten Hinweise auf die Richtigkeit der Angaben enthalten. Eine Eingangsbestätigung zum Antrag kann – bei Angabe der Adresse – zudem auch ohne vorherige Identitätskontrolle versandt werden, da dadurch in der Regel keine sensitiven Daten offenbart werden.

Meldet sich eine betroffene Person ohne Adressdaten, gibt aber andere Kontaktwege an, kann sie ggf. aufgefordert werden, Adressdaten nachzureichen. Sollten begründete Zweifel dokumentiert sein und sollte die betroffene Person trotz Aufforderung keine weiteren Daten zur Verifizierung nachliefern, kann der Antrag natürlich nicht weiterbearbeitet werden.

Um Auskunftsrechte ggü. der Polizei geltend zu machen, muss regelmäßig keine Ausweiskopie vorgelegt werden. Es genügt ein formloses Schreiben. Dabei ist es natürlich nach wie vor zweckmäßig, Angaben zu machen, die das Auffinden der gespeicherten Daten auch ermöglichen. Die Auskunft ist kostenfrei.

3.3 Wie anonym sind die Hinweisportale der Polizei?

Die Einführung eines anonymen Hinweisgebersystems der Steuerverwaltung in Baden-Württemberg hat bundesweit für Diskussionen über das Für und Wider von Meldeportalen öffentlicher Stellen im Internet geführt. Wir haben in diesem Zusammenhang bei der Polizei nachgefragt, wie anonym deren Angebote zur Meldung von möglichen Rechtsverstößen betrieben werden.

Die Polizei Berlin ermöglicht, wie im Jahresbericht dargestellt, über das „Anonyme Hinweisgebersystem“ und das „Berliner Hinweisportal“ bei der Abgabe von Meldungen und Hinweisen vollständig anonym zu bleiben. Bei der Nutzung beider Systeme werden keine IP-Adresse gespeichert, so dass auch im Nachhinein keine Ermittlung des Anschlussinhabenden möglich ist. Diese beiden digitalen Angebote wurden extra dafür geschaffen, um den Bürgerinnen und Bürgern eine vollständige Anonymität anbieten zu können.

Zur Verfügung stehen den Bürger:innen insoweit die „Internetwache“, das „Anonyme Hinweisgebersystem“ und das „Berliner Hinweisportal“.

Die „Internetwache“ ermöglicht, Anzeigen zu erstatten, Hinweise zu geben, aber auch Fragen zu stellen, Versammlungen anzumelden oder Beschwerden einzureichen. Hierfür müssen die Nutzer:innen au-

Die Internetwache der Polizei Berlin ermöglicht, Anzeigen zu erstatten, Hinweise zu geben, Fragen zu stellen, Versammlungen anzumelden oder Beschwerden einzureichen. Hierbei ist es für die

[74] Siehe § 45 Abs. 4 BlnDSG

ßer dem Hinweis, den sie geben wollen, keine personenbezogenen Daten angeben. Jede Eingabe wird von einer bzw. einem Polizist:in weiterbearbeitet, die bzw. der bei Bedarf nachfragen kann, falls freiwillig Kontaktdaten angegeben worden sind. Der Erfassung und Speicherung ihrer IP-Adresse müssen Nutzer:innen durch Setzen eines Häkchens auf der Seite der „Internetwache“ allerdings zustimmen, wenn ihre Eingabe bearbeitet werden soll. Mittels der IP-Adresse kann die Polizei bei begründetem Verdacht auf eine Straftat oder bei bestimmten Gefahren per Gerichtsbeschluss die/den Inhaber:in des Anschlusses ermitteln lassen, über den der Hinweis gegeben wurde, wenn diese Information zur Aufklärung des Sachverhalts erforderlich ist.[75]

Über das „Anonyme Hinweisgebersystem“ möchte die Polizei Hinweise auf Korruption ermöglichen. Hinweisgeber:innen müssen hier grds. keine personenbezogenen Hinweise eingeben, damit der Vorgang bearbeitet wird. Für weitere Nachfragen seitens der Ermittler:innen kann ein eigenes Postfach eingerichtet werden, auf das nur bestimmte Ermittlungspersonen Zugriff haben sollen.

Das „Berliner Hinweisportal“ wird nur zeitweise geschaltet. Die letzten drei Anlässe zum Zeitpunkt unserer Anfrage waren jeweils Zeugenaufrufe zu einem Angriff mit einer abgebrochenen Flasche, zu einem Banküberfall und zu einem Überfall auf einen Geldtransporter.

Bei den letzten beiden Systemen steht für die Polizei die vollständige Anonymisierung der Angebote im Vordergrund. Die Polizei versicherte uns, dass bei Zugriffen auf das „Anonyme Hinweisgebersystem“ und das „Berliner Hinweisportal“ keine IP-Adressen von Nutzer:innen gespeichert werden.

Polizei Berlin wichtig, diese digitalen Verwaltungsleistungen vor Missbrauch zu schützen und im Falle eines begründeten Verdachts auf eine Straftat oder bei bestimmten Gefahren nach Vorliegen eines entsprechenden Gerichtsbeschlusses den Anschlussinhabenden der IP-Adresse ermitteln zu lassen. Nutzende der Internetwache werden transparent darauf hingewiesen, dass ihre IP-Adresse bei der Nutzung des Angebotes gespeichert wird.

3.4 Weitergabe von Daten eines Beschwerdeführers an den von der Beschwerde betroffenen Mitarbeiter

Bei der Bearbeitung einer Beschwerde gegen einen Mitarbeiter der Polizei ist die Beschwerde dem betreffenden Mitarbeiter zusammen mit den personenbezogenen Daten des Beschwerdeführers weitergegeben worden.

Nach der Feststellung des Mangels bei der Beschwerdebearbeitung durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit in dem dargestellten Einzelfall wurden umgehend alle mit der Bearbeitung von Beschwerden betrauten Dienststellen schriftlich über die anzupassende Verfahrensweise informiert. Sie wurden angewiesen, ab sofort bei der Bearbeitung von Beschwerden darauf zu achten, dass den beschwerten Mitarbeiterinnen und Mitarbeitern neben dem Sach-

[75] Siehe § 100j Strafprozessordnung (StPO)

verhalt allenfalls die Anrede sowie Vor- und Nachname der Beschwerde führenden Person übermittelt werden. Darüberhinausgehende Informationen sind zu schwärzen.

Diese Verfahrensänderung wird auch in die neu zu fassende Geschäftsanweisung über die Bearbeitung von Beschwerden aufgenommen.

Bürger:innen können sich jederzeit über das Verhalten von Mitarbeiter:innen öffentlicher Stellen beschweren – das ist über das Petitionsrecht im Grundgesetz (GG) garantiert.[76] Bei Beamt:innen ist gesetzlich vorgesehen, dass sie zu Beschwerden, Behauptungen und Bewertungen, die für sie ungünstig sind oder ihnen nachteilig werden können, vor deren Aufnahme in die Personalakte anzuhören sind.[77] Unabhängig davon kann eine Weitergabe des Beschwerdeinhaltes auch erforderlich sein, wenn so eine Verhaltensänderung oder ein Überdenken der eigenen Position im Sinne der Beschwerdeführer:innen angestoßen werden kann.

Um den Beschäftigten die Wiedererkennung des betroffenen Sachverhaltes zu ermöglichen, kann es zudem zulässig sein, den Namen der Beschwerdeführer:innen kenntlich zu lassen – aber auch hier können besondere Umstände dagegensprechen.

Nicht erforderlich ist jedoch regelmäßig – wie im vorliegenden Fall dennoch geschehen – die Weitergabe von Kontaktdaten, wie Wohnanschrift und Telefonnummer von Beschwerdeführer:innen. Die aktuelle Geschäftsanweisung der Polizei zum Umgang mit Beschwerden sieht insoweit keine Schwärzung personenbezogener Daten vor. Das haben wir bemängelt.

Die Beschwerdestellen der Polizei und das dortige Zentrale Beschwerdemanagement haben umgehend Maßnahmen ergriffen, um Daten von Beschwerdeführer:innen in Zukunft besser zu schützen. Die Polizei hat uns zugesagt, die betreffende Geschäftsanweisung in unserem Sinne zu überarbeiten.

3.5 Mangelnde Identifizierung der antragstellenden Person bei der Online-Beantragung von einfachen Melderegisterauskünften

Aufgrund einer Bürgerbeschwerde haben wir das Online-Verfahren für die Erteilung von einfachen Melderegisterauskünften aus dem Melderegister ge-

[76] Siehe Art. 17 GG
[77] § 86 Landesbeamtengesetz (LBG)

prüft. Ein Bürger hatte festgestellt, dass das Landesamt für Bürger- und Ordnungsangelegenheiten (LABO) aufgrund einer Anfrage zu ihm eine Auskunft aus dem Melderegister erteilt und somit seine personenbezogenen Daten an die anfragende Person übermittelt hatte. Diese Person hatte im Rahmen ihres Antrags auf Auskunft online offensichtlich falsche Personalien angegeben. So gab der Antragsteller bzw. die Antragstellerin als Name „Mickey Mouse" und als Anschrift „12345 Disneyland, Mausstrasse 1, Demokratische Volksrepublik Korea" an.

Grundsätzlich hat der Bundesgesetzgeber im Bundesmeldegesetz (BMG) Grundlagen dafür geschaffen, dass Privatpersonen bzw. private Stellen, wie z. B. Unternehmen, auf Antrag eine Auskunft aus dem Melderegister erhalten können.[78] Demnach dürfen Meldebehörden bspw. eine sog. einfache Melderegisterauskunft zu einer Person erteilen und dabei den Familiennamen, Vornamen, Doktorgrad, die derzeitige Adresse und sofern die Person verstorben ist, diese Tatsache an einen privaten Dritten übermitteln.[79] Die einfachen Melderegisterauskünfte können dabei auch elektronisch bzw. durch einen automatisierten Abruf über das Internet erteilt werden.[80] In Berlin gibt es ein Online-Verfahren zur Beantragung und Erteilung von einfachen Melderegisterauskünften (Online Melderegisterauskunft – OLMERA), das durch das LABO betrieben wird. Über eine Webseite können aus dem aktuellen Datenbestand des Melderegisters Auskünfte beantragt werden.[81]

Auch nicht registrierte Nutzer:innen können über die Online-Anwendung eine Auskunft aus dem Melderegister erhalten. Bislang war dies wie folgt ausgestaltet: Sofern der bzw. die Nutzer:in durch Auswahl des entsprechenden Textfeldes versicherte, dass die erteilte Auskunft nicht zu gewerblichen Zwecken verwendet wird, gelangte er bzw. sie zu einer Eingabemaske, in der Angaben zur eigenen Person eingetragen werden mussten. Dort musste der bzw. die Antragsteller:in verpflichtend folgende Informationen über sich angeben: Name, Vorname, Postleitzahl, Ort, Straße und Hausnummer. Zusätzlich konnte das Land und die E-Mail-Adresse eingegeben werden.

[78] Siehe §§ 44, 45 BMG

[79] Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat die grds. auch ohne Einwilligung der betroffenen Person mögliche Erteilung von Melderegisterauskünften bereits mehrfach kritisiert; Siehe bspw. die Entschließung der DSK vom 8./9. März 2001 zur Novellierung des Melderechtsrahmengesetzes.

[80] Siehe § 49 Abs. 2 BMG

[81] https://olmera.verwalt-berlin.de

Bisher fand dabei allerdings weder eine Identitäts- noch eine Plausibilitätsprüfung im Hinblick auf die angegebenen Daten statt. Es wurde also auch nicht geprüft, ob die anfragende Person ihre Personalien richtig eingegeben hat bzw. ob es sich um fiktive Angaben handelt. Zwar enthält das BMG keine konkrete Regelung zu der Frage, ob und wenn ja wie die, eine Melderegisterauskunft abfragende Person zu identifizieren ist. Aus der Allgemeinen Verwaltungsvorschrift zur Durchführung des Bundesmeldegesetzes (BMGVwV), die Hinweise und Erläuterungen zur Anwendung der einzelnen gesetzlichen Regelungen des BMG enthält, geht jedoch ausdrücklich hervor, dass im Rahmen der automatisierten Melderegisterauskunft eine Identifizierung der anfragenden Person oder Stelle erfolgen muss.[82] Demnach ist die Identifizierung der anfragenden Person oder Stelle erforderlich. Natürliche oder juristische Personen, die bei der das Melderegister führenden Stelle registriert sind, werden durch ihre Zugangskennungen identifiziert. Soweit keine Registrierung vorliegt, sind Anfragende durch die Angabe des Namens, der Anschrift und ggf. des Geburtsdatums zu identifizieren.

Auch vor dem Hintergrund des datenschutzrechtlichen Auskunftsrechts[83] bzw. zur Erfüllung der Auskunftspflichten ggü. betroffenen Personen, deren Daten im Zuge einer einfachen Melderegisterauskunft weitergegeben wurden, muss zwingend eine Identifizierung der abfragenden Person erfolgen. Für eine ordnungsgemäße Auskunftserteilung und zur Ermöglichung von Datenschutzkontrollen werden die Angaben der im Rahmen der automatisierten Melderegisterauskunft anfragenden Person oder Stelle protokolliert.[84]

Nach alldem muss im Rahmen des automatisierten Abrufverfahrens die Identität der anfragenden Person oder Stelle anhand bestimmter Angaben verifiziert werden. Dies bedeutet, dass das Online-Verfahren technisch derart ausgestaltet sein muss, dass die Angaben von nicht registrierten OLMERA-Nutzer:innen kontrolliert und eine automatisierte Melderegisterauskunft jedenfalls dann nicht erteilt wird, wenn die Identität nicht überprüft werden kann. Indem das LABO im Rahmen des Online-Verfahrens OLMERA keine ausreichende Identifizierung der antragstellenden Personen vorgesehen hatte, hat es gegen die Pflicht zur Einhaltung tech-

[82] Siehe 49.0.1 BMGVwV
[83] Nach Art. 15 Datenschutz-Grundverordnung (DS-GVO) i. V. m. § 10 BMG
[84] Siehe § 49 Abs. 6 BMG i. V. m. § 40 BMG

nisch-organisatorischer Maßnahmen[85] verstoßen. Wir haben ggü. dem LABO daher eine Verwarnung ausgesprochen und es dazu aufgefordert, OLMERA entsprechend anzupassen.

Das LABO hat in der Folge bei dem Hersteller die technische Weiterentwicklung der Anwendung OLMERA beauftragt und intern an der technischen Einbindung der neuen Lösung gearbeitet, die inzwischen auch umgesetzt wurde. Seit dem 1. Dezember 2021 muss sich eine Person, die eine Online-Melderegisterauskunft möchte, mittels der elD-Funktion des neuen Personalausweises (nPA), des elektronischen Aufenthaltstitels (eAT) bzw. der elD-Karte für Unionsbürger identifizieren. Hierfür wird der Basisdienst elD verwendet, der durch die Senatsverwaltung für Inneres, Digitalisierung und Sport verantwortet wird.

Das LABO hat auf Anregung der Berliner Beauftragten für Datenschutz und Informationsfreiheit das Verfahren zur automatisierten Erteilung von Melderegisterauskünften unter Einbindung der Innenverwaltung fortentwickelt. Seit 1. September 2021 ist eine automatisierte Melderegisterauskunft nur unter Einsatz des elektronischen Identitätsnachweises (Personalausweis, elektronischer Aufenthaltstitel, eID-Karte) zu erhalten. Aus Sicht des Senats hat sich dieses Verfahren bewährt. Es fördert zugleich die allgemeine Akzeptanz und Verbreitung des elektronischen Identitätsnachweises.

Insbesondere zur Gewährleistung individueller Betroffenenrechte, wie des Rechts auf Erhalt einer datenschutzrechtlichen Auskunft, ist es notwendig, dass Meldebehörden die Empfänger:innen von Melderegisterdaten identifizieren und deren Daten protokollieren. Hierzu muss bei der Erteilung von Melderegisterauskünften über eine Online-Anwendung technisch sichergestellt werden, dass die Angaben zur Identität der antragstellenden Person überprüft werden, bevor diese eine Auskunft aus dem Melderegister erhält.

3.6 Datenverarbeitung bei parlamentarischen Wahlen

Im Zusammenhang mit parlamentarischen Wahlen werden personenbezogene Daten der Wähler:innen durch verschiedene Verantwortliche, z. B. Behörden und Parteien, zu unterschiedlichen Zwecken verarbeitet. Da am 26. September 2021 neben der bundesweit durchgeführten Wahl des Deutschen Bundestags in Berlin auch die Wahlen des Abgeordnetenhauses von Berlin und der Bezirksverordnetenversammlungen sowie ein Volksentscheid stattfanden, haben wir uns bereits im Vorfeld des Wahltags intensiv mit den Datenverarbeitungen beschäftigt und Informationsmaterial für die Öffentlichkeit erstellt.[86] Darüber hinaus sind wir insbesondere in den Wochen vor und nach den Wahlen zahlreichen Beschwerden von Bürger:innen nachgegangen.

Aufgrund einer Anfrage der Landeswahlleiterin, die für die ordnungsgemäße Vorbereitung und Durch-

[85] Gemäß Art. 5 Abs. 1 lit. f DS-GVO i. V. m. Art. 32 Abs. 1 DS-GVO
[86] Siehe hierzu den Ratgeber „Wahlwerbung durch politische Parteien“; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/wahlwerbung

führung aller politischen Wahlen sowie für die Ermittlung und Feststellung des amtlichen Wahlergebnisses verantwortlich ist, haben wir uns bereits Anfang des Jahres mit zwei speziell für Wahlen gestalteten Onlineformularen befasst – der „Onlinebeantragung von Wahlscheinen“ (OLIWA) sowie der „Onlinemeldung von Wahlhelfenden“, die über die Anwendung OLAV erfolgt. Über OLAV können sich Wahlhelfende registrieren und über OLIWA besteht die Möglichkeit für wahlberechtigte Bürger:innen, einen Wahlschein zu beantragen bzw. Briefwahlunterlagen anzufordern.

Bei beiden Onlinediensten werden personenbezogene Daten verarbeitet, da die Nutzer:innen zur Antragstellung bzw. zur Meldung als Wahlhelfer:innen Angaben zur eigenen Person machen müssen, die dann an die jeweils zuständigen öffentlichen Stellen übermittelt werden. Die Datenverarbeitungen können dabei insbesondere auf wahlrechtliche Vorschriften, wie z. B. das Bundeswahlgesetz (BWahlG) und die Bundeswahlordnung (BWO) sowie das Landeswahlgesetz (WahlG) und die Landeswahlordnung (LWO), gestützt werden. Sofern jedoch über die jeweils gesetzlich bestimmten Daten hinaus weitere Daten der betroffenen Personen erhoben werden, muss hierfür zwingend eine Einwilligung eingeholt werden. Hierauf haben wir die Landeswahlleiterin hingewiesen und gefordert, dass die freiwillig anzugebenden Daten in den Onlineanwendungen OLIWA und OLAV deutlich als solche gekennzeichnet werden müssen. Ferner haben wir die Anpassung der dort jeweils hinterlegten Datenschutzerklärung verlangt. In dieser muss u. a. transparent und nachvollziehbar erläutert werden, für welchen Zweck die Daten erhoben werden, und dass die Verarbeitung einwilligungsbasiert erfolgt.[87]

Des Weiteren haben wir uns im Zusammenhang mit den diesjährigen Parlamentswahlen schwerpunktmäßig – aufgrund zahlreicher Beschwerden – mit der Verarbeitung von Daten der wahlberechtigten Bürger:innen zu Zwecken der Wahlwerbung befasst. Hierbei ist zwischen der Übermittlung von Daten aus dem Wählerverzeichnis durch das LABO an Parteien und andere empfangsberechtigte Stellen sowie der weiteren Verarbeitung der Daten durch diese Empfänger:innen zu unterscheiden.

Das BMG erlaubt den Meldebehörden, dass sie politischen Parteien, Wählergruppen und anderen Träger:innen von Wahlvorschlägen in den sechs Mona-

[87] Dies folgt aus den Transparenz- und Informationspflichten nach Art. 12, 13 DS-GVO.

ten vor einer Parlamentswahl Auskunft aus dem Melderegister erteilen dürfen.[88] Die Träger:innen einer Volksinitiative und eines Volks- und Bürgerbegehrens dürfen ebenfalls Daten abfragen. Die Auskünfte aus dem Melderegister dürfen ausschließlich zum Zweck der Wahlwerbung verwendet werden.[89] Die durch die Melderegisterauskunft gewonnenen Daten müssen zudem spätestens einen Monat nach dem Tag der Wahl bzw. der Abstimmung wieder gelöscht bzw. vernichtet werden.[90] Die Auskunftserteilung muss im Einzelfall unterbleiben, wenn für eine bestimmte wahlberechtigte Person eine Übermittlungssperre aufgrund eines Widerspruchs, ein bedingter Sperrvermerk[91] oder eine Auskunftssperre[92] im Melderegister eingetragen ist.

Das Melderecht schreibt auch vor, dass die Auskünfte nur über einzelne Altersgruppen erteilt werden dürfen. Nicht erlaubt ist daher eine Übermittlung der Daten sämtlicher Wahlberechtigter. Die Beschränkung auf Altersgruppen deckt sich häufig auch mit den Vorstellungen der Parteien, bspw. Erst- oder Jungwähler:innen oder Senior:innen gezielt mit Themen der jeweiligen Altersgruppe ansprechen zu können. Da bei der Zusammenstellung der Personengruppen, über die Auskunft erteilt werden soll, gesetzlich allein auf das Alter abgestellt werden darf, ist ein anderes Auswahl- bzw. Suchkriterium, wie z. B. die Religionszugehörigkeit oder das Geschlecht, nicht zulässig.

Viele Parteien haben vor den Wahlen von diesem besonderen Fall der Melderegisterauskunft Gebrauch gemacht und das LABO um die Übermittlung der Daten von bestimmten Gruppen der Wahlberechtigten gebeten. Bei der Überprüfung der diesbezüglichen Eingaben konnten wir bislang keinen datenschutzrechtlichen Verstoß des LABO feststellen. Die Datenübermittlungen erfolgten gemäß den gesetzlichen Vorgaben.

Allerdings haben wir in einigen Fällen festgestellt, dass Parteien bei der weiteren Verarbeitung der abgefragten Daten zu Wahlwerbezwecken gegen datenschutzrechtliche Vorschriften verstoßen haben.

Wenn Parteien Wahlwerbeschreiben an die erhaltenen Adressen verschicken, müssen sie gleichzeitig den Empfänger:innen bestimmte Informationen über

[88] § 50 Abs. 1 Satz 1 BMG
[89] § 50 Abs. 1 Satz 3 BMG
[90] § 50 Abs. 1 Satz 3 BMG
[91] Siehe § 52 BMG
[92] Siehe § 51 BMG

die Datenverarbeitung zur Verfügung stellen. Unter anderem muss für die Empfänger:innen leicht erkennbar sein, wer für die Datenverarbeitung verantwortlich ist und wie sie die/den Verantwortliche:n erreichen können. Die Parteien müssen auch darüber informieren, aus welcher Quelle die Adressdaten stammen und wann sie wieder gelöscht werden. Wenn die Daten bei der Verarbeitung an Dienstleister:innen offengelegt werden, müssen die Parteien auch dies unter Angabe der Empfänger:innen transparent machen.[93] Diese Angaben waren nicht in allen Wahlwerbeschreiben enthalten, die uns von Beschwerdeführer:innen zur Prüfung vorgelegt wurden.

In einem Fall war nicht einmal eindeutig erkennbar, wer für die Datenverarbeitung verantwortlich war. Die Partei hatte die Wahlwerbeschreiben so aussehen lassen, als handele es sich um persönliche Wahlempfehlungen von öffentlich bekannten Privatpersonen. Für viele Empfänger:innen war dabei der Eindruck entstanden, die Partei hätte ihre Daten an die vermeintlichen Absender:innen der Schreiben weitergegeben, was unzulässig wäre. Dieser Verdacht hat sich im Laufe unserer Ermittlungen jedoch nicht bestätigt. Vielmehr hat die Partei in Absprache mit den vermeintlichen Absender:innen die Briefe gestaltet und selbst bzw. mithilfe eines Dienstleisters versandt.

Parteien können sich zur Versendung von Wahlwerbeschreiben professioneller Dienstleister:innen bedienen, wenn sie mit diesen einen wirksamen Auftragsverarbeitungsvertrag abschließen.[94] Wichtig ist dabei, dass die bzw. der Dienstleister:in die ihr/ihm übermittelten personenbezogenen Daten ausschließlich im Auftrag und auf Weisung ihres/seines Auftraggebers bzw. seiner Auftraggeberin verarbeiten darf und nach Durchführung des Auftrags wieder löschen muss. Damit bleiben die Parteien selbst für die Verarbeitung der Daten verantwortlich. Die Dienstleister:innen dürfen die Daten keinesfalls zu eigenen Zwecken verwenden oder mit den Daten von anderen Auftraggeber:innen zusammenführen.

Auch hier mussten wir feststellen, dass nicht alle Parteien entsprechende Vereinbarungen mit ihren Dienstleister:innen abgeschlossen hatten, bevor sie die Adressdaten an diese weitergegeben haben. Bislang liegen uns jedoch keine Hinweise darauf vor, dass Dienstleister:innen Adressdaten, die sie von

[93] Die Auflistung aller Informationen, die die Parteien zur Verfügung stellen müssen, findet sich in Art. 14 Abs. 1 und 2 DS-GVO.
[94] Siehe Art. 28 Abs. 3 DS-GVO

Parteien erhalten haben, tatsächlich nicht wieder gelöscht und/oder zu anderen Zwecken verwendet haben.

Auch wenn im Zusammenhang mit der Vorbereitung und Durchführung von Parlamentswahlen bestimmte Datenverarbeitungen durch Behörden und Parteien aufgrund besonderer gesetzlicher Regelungen erlaubt sind, müssen die Verantwortlichen streng darauf achten, den Umfang der verarbeiteten Daten und den Zweck der Verarbeitungen entsprechend den Regelungen zu beschränken. Hinsichtlich der Transparenzpflichten finden die allgemeinen Vorschriften der Datenschutz-Grundverordnung (DS-GVO) auch in diesen Fällen Anwendung.

Das LABO fügt Auskünften im Vorfeld von Wahlen oder Abstimmungen künftig einen Hinweis an die Datenempfängerinnen und - empfänger auf die Zweckbindung gemäß § 50 Absatz 1 Satz 3 in Verbindung mit Satz 1 Bundesmeldegesetz bei, wonach die Daten nur für die Werbung bei einer Wahl oder Abstimmung verwendet werden dürfen und für die Adressatinnen und Adressaten der Werbung nach Maßstab eines objektivierten Empfängerhorizonts erkennbar sein muss, dass es sich um Werbung von Parteien, Wählergruppen oder anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen oder Abstimmungen handelt.

Zudem wird darauf hingewiesen, dass die Daten spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten sind.

3.7 Veröffentlichung von Fotos und anderen Daten auf der Webseite von Sportvereinen

Für viele Sportvereine ist ein eigener Internetauftritt eine wichtige Möglichkeit, das Vereinsleben darzustellen und für die jeweilige(n) Sportart(en) sowie eine Vereinsmitgliedschaft zu werben. Es wenden sich jedoch immer wieder betroffene Personen an uns und beschweren sich über die Veröffentlichung ihrer personenbezogenen Daten auf der Webseite eines Sportvereins. Bei der Prüfung dieser Eingaben stellen wir regelmäßig fest, dass in den Vereinen nach wie vor Unklarheiten bestehen, ob und welche Daten auf die vereinseigenen Webseiten gestellt werden dürfen.

Diesen Beitrag hat der Senat zum Anlass genommen, den Landessportbund Berlin (LSB Berlin) im Zuge der kollegialen Zusammenarbeit zu kontaktieren.

Als Dachverband der Fachverbände des Amateursports, der bezirklichen Sportarbeitsgemeinschaften und sonstiger Sportinstitutionen in Berlin übernimmt der LSB Berlin auch Aufgaben der fachlichen Beratung für seine Mitgliedsvereine.

Die Veröffentlichung von personenbezogenen Daten im Internet ist eine Datenübermittlung an einen unbegrenzten Personenkreis, da Webseiten grds. weltweit aufgerufen werden können. Hieraus ergeben sich für die Betroffenen Risiken, denn die so veröffentlichten Informationen können von jedermann recherchiert und bspw. auch zu Werbezwecken sowie zur Profilbildung ausgewertet werden. Eine besondere Gefahr ergibt sich zudem daraus, dass die Daten auch in Staaten abgerufen werden können, in denen die DS-GVO oder vergleichbare Bestimmungen nicht gelten.

Da auf der Internetseite des LSB Berlin zum Thema „Datenschutz im Verein“ bereits umfangreiche Informationen bereitgestellt werden, wurde angeregt, diese um die Hinweise aus dem Jahresbericht zu ergänzen.

Eine Möglichkeit einer rechtmäßigen Veröffentlichung ist es, sich von den betroffenen Personen (Vereinsmitglieder, Dritte) eine Einwilligung geben

zu lassen. Dabei müssen die gesetzlichen Voraussetzungen einer wirksamen Einwilligung beachtet werden.[95] Insbesondere muss die Einwilligung der betroffenen Person auf ihrer freien Entscheidung beruhen. Die Person muss hierfür zuvor ausreichend und verständlich darüber informiert werden, welche Daten der Verein zu welchem Zweck verarbeiten will. Zu beachten ist ferner, dass die Einwilligung jederzeit für die Zukunft frei widerrufbar ist. Auch hierüber sollte die betroffene Person informiert werden. Eine besondere Form der Einwilligung ist in der DS-GVO nicht vorgesehen, sodass die Einwilligung sowohl schriftlich als auch elektronisch, mündlich oder konkludent erfolgen kann. Aufgrund der Nachweispflicht[96] sollte der Verein jedoch Einwilligungen schriftlich einholen oder die Abgabe von Einwilligungen anderweitig dokumentieren.

Die Veröffentlichung personenbezogener Daten kann auch ohne eine Einwilligung der betroffenen Person erfolgen, wenn hierfür eine andere Rechtsgrundlage besteht. In Betracht kommt hier zum einen Art. 6 Abs. 1 Satz 1 lit. b DS-GVO, wenn die Datenverarbeitung zur Erreichung des Vereinszwecks bzw. des Mitgliedschaftsverhältnisses, insbesondere zur Verwaltung und Betreuung der Mitglieder erforderlich ist. Zum anderen ist eine Veröffentlichung der Daten auf der Grundlage von Art. 6 Abs. 1 Satz 1 lit. f DS-GVO möglich, sofern der Verein oder ein Dritter daran ein berechtigtes Interesse hat, und sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Dies muss der Verein in jedem Einzelfall jedoch sorgfältig prüfen.

So dürfen bspw. Daten von Funktionsträger:innen eines Vereins, wie der Name, die ausgeübte Funktion und die vereinsbezogene Erreichbarkeit (Telefonnummer/E-Mail-Adresse), regelmäßig auch ohne ausdrückliche Einwilligung auf der Webseite veröffentlicht werden, da das Interesse des Vereins an einer umfassenden und vollständigen Außendarstellung bzw. an der Ermöglichung der Kontaktaufnahme ggü. dem Interesse des Einzelnen grds. überwiegt. Für die Veröffentlichung der privaten Anschrift oder weiterer privater Kontaktdaten ist jedoch eine Einwilligung des Funktionsträgers bzw. der Funktionsträgerin erforderlich. Ferner dürfen auch sportartbezogene Informationen, wie z. B. Spielergebnisse und -berichte, Mannschaftsaufstellungen sowie persönliche Leistungen ohne Einwilligung der Betroffenen auf der Homepage veröffent-

[95] Siehe u. a. Art. 6 Abs. 1 Satz 1 lit. a, Art. 4 Nr. 11, Art. 7 und Art. 8 DS-GVO
[96] Siehe Art. 7 Abs. 1 DS-GVO

licht werden, wenn keine schutzwürdigen Interessen der betroffenen Personen entgegenstehen und sie zuvor ausreichend darüber informiert worden sind[97]. Zudem muss sichergestellt sein, dass die Daten nach einem angemessenen Zeitraum gelöscht werden. Bei der Bemessung der zulässigen Dauer der Veröffentlichung ist vor allem die Bedeutung des Ereignisses, auf das sich die Veröffentlichung bezieht, zu berücksichtigen, da sich hieraus das Informationsinteresse der Öffentlichkeit ableitet. Bei der Abwägung der Interessen des Vereins bzw. der Öffentlichkeit mit dem Interesse der betroffenen Person ist in erster Linie ausschlaggebend, ob es sich um eine öffentliche Veranstaltung des Vereins oder eines Verbands handelt und die Namen und die Ergebnisse üblicherweise ebenfalls öffentlich bekannt gegeben werden. Ist dies der Fall, so spricht dies grds. dafür, dass eine Veröffentlichung der Daten erfolgen kann.

Bei der Veröffentlichung von Fotos und anderen personenbezogenen Daten auf Webseiten von Sportvereinen ist Vorsicht geboten. Die Verantwortlichen müssen sorgfältig prüfen, ob eine ausdrückliche Einwilligung eingeholt werden muss, oder ob die Veröffentlichung in sonstiger Weise auf eine Rechtsgrundlage gestützt werden kann. In jedem Fall dürfen nur für den jeweiligen Zweck erforderliche Daten im Internet veröffentlicht werden.

Der LSB Berlin hat zugesagt, die Hinweise und Erläuterungen zu diesem Thema zu prüfen und dies zum Anlass zu nehmen, in einer der nächsten Ausgaben der Mitgliederzeitschrift „Sport in Berlin“ einen Artikel aufzunehmen. Zudem will der LSB Berlin Schulungen zu diesem Thema anbieten.

4 Justiz und Rechtsanwaltschaft

4.1 Funkzellenabfragen-Transparenz-System endlich im Einsatz

Zur Aufklärung besonders schwerer Straftaten ist es unter bestimmten Voraussetzungen zulässig, sog. Funkzellenabfragen durchzuführen.[98] Hierbei können Strafverfolgungsbehörden von Telekommunikationsanbieter:innen Auskunft über die Verbindungsdaten sämtlicher Mobilfunktelefonate, die in einer vorgegebenen Zeit in einem bestimmten Gebiet geführt worden sind, verlangen. Die Betroffenen erfahren hiervon oft nichts.

Funkzellenabfragen greifen in das verfassungsrechtlich geschützte Fernmeldegeheimnis[99] ein und betreffen sehr viele Personen, die keinen Anlass für die Durchführung solcher Maßnahmen gegeben haben.

[97] Siehe Art. 13 DS-GVO
[98] Siehe § 100g Abs. 3 Strafprozessordnung (StPO)
[99] Siehe Art. 10 Grundgesetz (GG)

Wir haben daher im Jahr 2012 die Praxis der Funkzellenabfragen durch Strafverfolgungsbehörden geprüft und dabei diverse Mängel festgestellt.[100] Vielfach unterblieb bspw. die gesetzlich vorgeschriebene Benachrichtigung von Betroffenen, sodass diese keine Rechtsschutzmöglichkeiten wahrnehmen konnten.

Das Abgeordnetenhaus forderte damals den Senat aufgrund unserer Prüfungsergebnisse u. a. auf, eine allgemein zugängliche Information der Öffentlichkeit über Zeit und Ort einer Funkzellenabfrage zu gewährleisten.[101] Daraufhin hat die Senatsverwaltung für Justiz ein entsprechendes Projekt gestartet, das wir rechtlich und technisch eng begleitet und unterstützt haben.

Das in dem Projekt entwickelte Funkzellenabfragen-Transparenz-System (FTS) steht nunmehr allen interessierten Bürgerinnen und Bürgern zur Verfügung.[102] Nach aktuellem Stand entspricht das System den datenschutzrechtlichen Anforderungen und ist ein großer Gewinn für die Betroffenenrechte.

4.2 Recht auf Auskunft aus der Prüfungsakte in der Jurist:innenausbildung

Das Gemeinsame Juristische Prüfungsamt der Länder Berlin und Brandenburg (GJPA) ermöglicht im Rahmen der juristischen Staatsprüfungen die Einsichtnahme in die handgeschriebenen Aufsichtsarbeiten und die Bewertungsbögen der Prüfer:innen vor Ort. Darauf musste in Zeiten der Pandemie freilich oft verzichtet werden. Kopien der Prüfungsakte können allerdings nur gegen Kostenerstattung angefordert werden.Der genaue Inhalt der selbstverfassten Klausuren ist insbesondere wichtig für Kandidat:innen, die ihre Bewertung nachvollziehen möchten oder eine Prüfung nicht bestanden haben. Die Ergebnisse der Examina haben für viele Kandidat:innen Auswirkungen auf das gesamte spätere Berufsleben.

Die Datenschutz-Grundverordnung (DS-GVO) sieht vor, dass Stellen, die personenbezogene Daten verarbeiten, über diese kostenfrei Auskunft erteilen und kostenfreie Kopien der verarbeiteten Daten zur Verfügung stellen müssen.[103] Als Recht der Europäischen Union geht diese Bestimmung anderslautenden Regelungen in den Mitgliedsstaaten grds. vor, denn anderenfalls bestünde die Gefahr, dass Unions-

Das GJPA verfolgte die Entwicklung der Rechtsprechung zur Anwendbarkeit des Art. 15 DS-GVO auf die juristischen Staatsprüfungen und zum Umfang des Auskunftsrechts stets genau. So stand das GJPA in ständigem Kontakt zum die Revision im Verfahren BVerwG 6 C 10.21 führenden LJPA Nordrhein-Westfalen, zudem sind zwei Mitarbeiter zur Beobachtung der mündlichen

[100] Siehe JB 2012, 2.1
[101] Siehe JB 2013, 5.4
[102] https://fts.berlin.de/
[103] Art. 15 Abs. 3 DS-GVO

recht in den Mitgliedsstaaten ungleich oder überhaupt nicht angewendet wird, was wiederum dem Zweck der Europäischen Einigung zuwiderlaufen würde.[104]

Verhandlung vor dem Senat am 30. November 2022 entsandt worden.

Das GJPA beruft sich hinsichtlich des von ihm praktizierten Auskunftsverfahrens auf eine Vorschrift des Berliner Juristenausbildungsgesetzes (JAG),[105] die die Anwendung der DS-GVO ausschließen soll und hält auch sonst die DS-GVO nicht für anwendbar.

Die Rechtslage zur Anwendbarkeit des Art. 15 DS-GVO auf die juristischen Staatsprüfungen und zum Umfang des Auskunftsrechts war trotz der Entscheidung des EuGH in der Rechtssache „Nowak“ (Urteil vom 20. Dezember 2017, C-434/16, juris) auch nicht eindeutig. Dies zeigt sich schon daran, dass die Vorinstanzen wegen grundsätzlicher Bedeutung der Rechtssache die Berufung bzw. die Revision zuließen.

Da das Ergebnis der Prüfung jedoch u. a. auch darüber entscheidet, ob die Kandidat:innen ihren späteren Beruf auch in anderen Mitgliedsstaaten der Union ausüben können, fällt die Verarbeitung personenbezogener Daten schon aus diesem Grund unter Unionsrecht. Auch hat der Europäische Gerichtshof (EuGH) bereits entschieden, dass Prüfungsantworten und -bewertungen selbst dann als personenbezogene Daten gelten, wenn die Unterlagen unter einer Kennziffer verarbeitet werden.[106]

Noch in der mündlichen Verhandlung beantragte der Vertreter des Bundesinteresses beim Bundesverwaltungsgericht zudem letztlich ohne Erfolg, das Verfahren auszusetzen und dem EuGH Fragen zur Reichweite des Art. 15 DS-GVO vorzulegen.

Warum die kostenfreie Übersendung von Kopien das GJPA bei der Durchführung von Prüfungen beeinträchtigt, konnte uns das Prüfungsamt nicht überzeugend darlegen. Die Auskunft über verarbeitete Daten gehört zu den Aufgaben von Behörden im Kontakt mit Bürger:innen. Die ordnungsgemäße Durchführung obliegt der jeweils verantwortlichen Stelle. Die Berücksichtigung fiskalischer Interessen muss bei einer Aufgabenerfüllung im Rahmen der Grundrechte regelmäßig zurücktreten.

Ausgehend hiervon war die Verwaltungspraxis des GJPA, Kand. keine unentgeltlichen Kopien ihrer Aufsichtsarbeiten nebst den Prüfergutachten zur Verfügung zu stellen, vor der höchstrichterlichen Entscheidung des Bundesverwaltungsgerichts vom 30. November 2022 jedenfalls gut begründet.

Wir haben das GJPA daher zunächst in einem Einzelfall verwarnt, weitere aufsichtsrechtliche Schritte behalten wir uns für die Zukunft vor.

Nach dem Urteil des Bundesverwaltungsgerichts hat das GJPA entschieden, seine Verwaltungspraxis hieran auszurichten. Eine streitige Entscheidung darüber, ob § 23 Abs. 3 JAG dem Anspruch auf Erhalt unentgeltlicher Kopien der Aufsichtsarbeiten nebst den Prüfergutachten entgegensteht, soll nicht herbeigeführt werden. Den Kand. werden daher nunmehr auf einen entsprechenden Antrag hin unentgeltlich Kopien ihrer Aufsichtsarbeiten nebst den Prüfergutachten zur Verfügung gestellt.

[104] Der sog. Anwendungsvorrang, der dem effet-utile-Grundsatz entspringt, ist ständige Rechtsprechung des Europäischen Gerichtshofs (EuGH).
[105] § 23 JAG
[106] EuGH, Urteil vom 20. Dezember 2017 – C-434/16, „Nowak“

Kandidat:innen juristischer Prüfungen haben gemäß Art. 15 DS-GVO Ansprüche auf kostenfreie Auskunft aus ihren Prüfungsunterlagen sowie kostenfreie Kopien. Dies wurde inzwischen auch gerichtlich entschieden.[107]

Vor dem Verwaltungsgericht Berlin sind Stand 30. Dezember 2022 zwei Verfahren anhängig, in denen es ausschließlich um die Problematik „Anspruch auf Erhalt einer unentgeltlichen Kopie der Aufsichtsarbeiten nebst Prüfergutachten gestützt auf Art. 15 DS-GVO“ geht. Seitens des GJPA ist hier nach der höchstrichterlichen Entscheidung des Bundesverwaltungsgerichts alles dafür in die Wege geleitet worden, damit sich diese Verfahren unstreitig erledigen.

4.3 Umsetzung der JI-Richtlinie im Justizvollzug

Mit über dreijähriger Verspätung[108] hat der Berliner Gesetzgeber nunmehr die sog. JI-Richtlinie[109] im Datenschutzrecht des Justizvollzugs, der Sozialen Dienste der Justiz und der Führungsaufsichtsstelle beim Landgericht umgesetzt.[110] Die Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung, die den entsprechenden Gesetzesentwurf vorbereitet hat, hat uns frühzeitig hieran beteiligt und Gelegenheit zur Stellungnahme gegeben.

Dabei konnten wir u. a. erreichen, dass bei einer Entscheidung über die Aufschiebung, Einschränkung oder Unterlassung einer Benachrichtigung der betroffenen Person über eine Verarbeitung ihrer Daten gemäß der Vorgabe der JI-Richtlinie[111] in jedem Einzelfall den Grundrechten und den berechtigten Interessen dieser Person Rechnung getragen werden muss.[112]

Auch die Regelung von Fallkonferenzen des Justizvollzugs mit Sicherheitsbehörden[113], die insbesondere im Hinblick auf die Erforderlichkeit der dort praktizierten Datenverarbeitung immer problematisch sind, wurde aufgrund unserer Stellungnahme nachgebessert. Zum einen wurde sie im Hinblick auf die Datenverarbeitungsbefugnisse des Justizvollzugs konkretisiert, zum anderen wird nun in der Geset-

[107] OVG Nordrhein-Westfalen, Urteil vom 8. Juni 2021 – 16 A 1582/20; noch nicht rechtskräftig
[108] Der Gesetzgeber hätte dieser Pflicht gemäß Art. 63 Abs. 1 Satz 1 JI-Richtlinie eigentlich bis zum 6. Mai 2018 nachkommen müssen.
[109] Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-Richtlinie)
[110] Siehe Abghs.-Drs. 18/4032
[111] Siehe Art. 13 Abs. 3 JI-Richtlinie
[112] Siehe § 30 Abs. 3 JI-Richtlinie
[113] Siehe § 48 Justizvollzugsdatenschutzgesetz (JVollzDSG)

zesbegründung explizit darauf hingewiesen, dass die Befugnisse der anderen Teilnehmenden von Fallkonferenzen zur Datenverarbeitung an den Justizvollzug aus deren jeweiligem Fachrecht folgen muss.

Nicht berücksichtigt wurde hingegen unsere Kritik an § 4 Abs. 2 des novellierten Justizvollzugsdatenschutzgesetzes (JVollzDSG). Danach sollen alle Justizvollzugsanstalten, die Jugendstrafanstalt, die Jugendarrestanstalt, die Auskunftsstelle des Justizvollzugs, das Krankenhaus des Justizvollzugs, die Zentrale IT-Stelle der Justizvollzugsanstalten und die Sozialen Dienste der Justiz zusammen eine einheitliche Verantwortliche bilden. Dies widerspricht Wortlaut und Intention des Berliner Datenschutzgesetzes (BlnDSG)[114] sowie der zugrundeliegenden JI-Richtlinie[115]. Danach bestimmt sich die Verantwortlichkeit nach der Entscheidungshoheit über Zweck und Mittel einer Datenverarbeitung. Diese Bestimmung ist darin begründet, dass jeder öffentlichen Stelle eigene Aufgaben- und Zuständigkeitsbereiche zukommen, die zu unterschiedlichen Datenverarbeitungsbefugnissen führen.

Der Senat geht davon aus, dass hier ein Missverständnis zum Inhalt der Regelungen des § 4 Absatz 1 Nr. 1 des Justizvollzugsdatenschutzgesetzes Berlin (JVollzDSG Bln) und des § 4 Absatz 2 JVollzDSG Bln vorliegt. Die Regelungen bestimmen gerade nicht den Justizvollzug und die Sozialen Dienste der Justiz als einheitliche Verantwortliche im Sinne des § 31 Nummer 7 des Berliner Datenschutzgesetzes (BlnDSG). Vielmehr unterscheidet § 4 JVollzDSG Bln ausdrücklich zwischen dem datenschutzrechtlich verantwortlichen Justizvollzug in § 4 Absatz 1 Nr. 1 JVollzDSG Bln einerseits und den Sozialen Diensten der Justiz in § 4 Absatz 2 JVollzDSG Bln andererseits.

Richtig ist allerdings, dass die in § 4 Absatz 1 Nr. 1 JVollzDSG Bln aufgezählten Behörden – also die Justizvollzugsanstalten, die Jugendstrafanstalt und die Jugendarrestanstalt Berlin – sowie deren Untereinheiten und Abteilungen – insbesondere die Einrichtung zum Vollzug der Sicherungsverwahrung, die Einweisungsabteilung, die Auskunftsstelle des Justizvollzugs, das Justizvollzugskrankenhaus und die Zentrale IT-Stelle der Justizvollzugsanstalten und der Sozialen Dienste der Justiz, soweit letztere für den Justizvollzug tätig ist – zusammen einen (einzigen) Verantwortlichen im Sinne des § 31 Nummer 7 BlnDSG bilden.

Die von der Berliner Beauftragten für Datenschutz und Informationsfreiheit hiergegen vorgebrachte Kritik war bereits im Gesetzgebungsverfahren berücksichtigt und in der Gesetzesbegründung zu § 4 Absatz 1 Satz 2 JVollzDSG Bln ausführlich gewürdigt worden (siehe Abgh.-Drs. 18/4032, S. 55 f.). Demnach liegt der einheitlichen datenschutzrechtlichen Betrachtung des Justizvollzugs zugrunde, dass die verschiedenen Justizvollzugsanstalten des Landes Berlin und deren Untereinheiten eine organisatorische Einheit darstellen, die in arbeitsteiligem Zusammenwirken dieselben vollzuglichen Aufgaben und Zwecke verfolgen und sich auf vielfältige Weise in ihrer Arbeit gegenseitig ergänzen. Daher ist diese Betrachtung

[114] Siehe § 31 Nr. 7 BlnDSG
[115] Siehe Art. 3 Nr. 8 JI-Richtlinie

des Justizvollzugs – wozu wie bereits ausgeführt nicht die Sozialen Dienste der Justiz zählen – im Interesse einer sachgerechten Betreuung der betroffenen Personen in verschiedenen Anstalten geboten, um die komplexe Behördenstruktur datenschutzrechtlich adäquat abzubilden. Den berechtigten Interessen der betroffenen Personen trägt zudem die Verhältnismäßigkeitsklausel des § 12 Absatz 1 JVollzDSG Bln angemessen Rechnung.

Aufgabe einer Justizvollzugsanstalt ist es bspw. die Gefangenen zu befähigen, künftig in sozialer Verantwortung ein Leben ohne Straftaten zu führen sowie die Allgemeinheit vor weiteren Straftaten zu schützen.[116] Der Vollzug des Jugendarrestes soll wiederum das Ehrgefühl des Jugendlichen wecken und ihm eindringlich zum Bewusstsein bringen, dass er für das von ihm begangene Unrecht einzustehen hat.[117] Die Sozialen Dienste sind hingegen für Aufgaben der Bewährungshilfe, der Gerichtshilfe und der Führungsaufsicht zuständig und das Krankenhaus des Justizvollzugs naturgemäß einzig und allein für die ärztliche Patient:innenbehandlung. Die genannten Stellen mögen zwar organisatorisch verbunden sein, verarbeiten Daten jedoch im Rahmen verschiedener Aufgaben und zu unterschiedlichen Zwecken.

Besonders problematisch ist in diesem Zusammenhang, dass alle vorgenannten Stellen zusammen mit dem Krankenhaus des Justizvollzugs als eine einheitliche Stelle gelten sollen. Der Schutz der besonderen Kategorien personenbezogener Daten[118], die bei dieser Stelle vornehmlich verarbeitet werden, kann so nicht hinreichend gewährleistet werden.

Soweit Daten zwischen den genannten Stellen ausgetauscht werden sollen, bedarf es hierfür konkreter gesetzlicher Übermittlungsbefugnisse, die sich an den jeweiligen Aufgaben der beteiligten Stellen bemessen. Ein Verzicht auf die eindeutige Normierung solcher Datenübermittlungsbefugnisse aus Gründen der Vermeidung unnötiger Bürokratiekosten, wie es in der Gesetzesbegründung heißt, führt in der Praxis zu Unklarheiten bei der Zulässigkeit des Datenaustausches zwischen diesen Stellen und einem damit verbundenen hohen Risiko einer unzulässigen Datenverarbeitung.

[116] § 2 Berliner Strafvollzugsgesetz (StVollzG)
[117] § 90 Abs. 1 Jugendgerichtsgesetz (JGG)
[118] Siehe § 31 Nr. 14 BlnDSG

Ein weiterer Kritikpunkt betrifft die Normierung zur Verarbeitung biometrischer Daten. Bereits im vormalig geltenden JVollzDSG wurde erstmals die Erfassung biometrischer Merkmale des Gesichts, der Augen, der Hände, der Stimme oder der Unterschrift bei Gefangenen zu erkennungsdienstlichen Zwecken ermöglicht. Wir hatten diese Regelung schon im damaligen Gesetzgebungsverfahren wegen Nichterforderlichkeit und Unverhältnismäßigkeit angesichts des damit einhergehenden erheblichen Eingriffs in die Persönlichkeitsrechte der Betroffenen kritisiert.[119]

Nun ist es zumindest nicht mehr möglich, die Stimme als biometrisches Merkmal zu verarbeiten.[120] Die übrigen biometrischen Merkmale sollen jedoch weiterhin zu vollzuglichen Zwecken verarbeitet werden können.

Nach unserer Kenntnis werden bis heute keine biometrischen Merkmale im Justizvollzug verarbeitet, sodass bereits die Praxisrelevanz dieser Regelung zweifelhaft ist. Offensichtlich ist es dem Justizvollzug bislang auch mit den sonstigen erkennungsdienstlichen Maßnahmen sehr gut möglich, die Identität von Gefangenen zu prüfen, um bspw. Verwechslungen zu vermeiden.

Berlin war im Jahr 2011 mit der Schaffung eines sehr ambitionierten eigenen Justizvollzugsdatenschutzgesetzes bundesweit Vorreiter. Dieses Gesetz wurde nun endlich anhand der neuen europarechtlichen Vorgaben überarbeitet, bedauerlicherweise allerdings nicht in allen erforderlichen Punkten.

4.4 Gerichtsvollzieher: Das „sprechende“ Geschäftszeichen

Die Gerichtsvollzieher:innen nehmen im Gefüge der Gerichtsbarkeit eine wichtige Stellung ein. Grundsätzlich sind sie die Einzigen, die Vollstreckungsmaßnahmen im Wege der Zwangsvollstreckung durchführen dürfen. Auch gilt die Zustellung durch Gerichtsvollzieher:innen als einer der sichersten Wege, um beweisen zu können, welches Schreiben die/der Empfänger:in erhalten hat. Da auch Dritte von einer Zustellung Kenntnis erlangen können, ist es besonders wichtig, dass auf sensitive Daten von betroffenen Bürger:innen, die oft gegen ihren Willen Beteiligte in den genannten Verfahren sind, gut achtgegeben wird.

[119] Siehe JB 2011, 2.2.3
[120] Siehe § 19 Abs. 1 Nr. 5 JVollzDSG

In einem Fall, auf den wir durch die Beschwerde eines Betroffenen aufmerksam wurden, war eine Gerichtsvollzieherin mit einer Zustellung beauftragt worden und hatte als Geschäftszeichen nicht nur die übliche abstrakte Zahlenkombination vergeben, sondern das Geschäftszeichen übernommen, unter dem der Auftraggeber das Verfahren führte. Dieses Geschäftszeichen ließ jedoch auf den Inhalt des verschlossenen Briefes schließen, der dem Betroffenen zuzustellen war.

Während es grds. erforderlich sein kann, zuzustellende Schriftstücke – auch auf den Postumschlägen oder im Sichtfenster – gesondert zu kennzeichnen, um Verwechslungen zu vermeiden, war es für die Tätigkeit der Gerichtsvollzieherin nicht erforderlich, ein solches „sprechendes" Geschäftszeichen des Auftraggebers zu übernehmen. Ein eigenes, kodiertes Geschäftszeichen hätte völlig ausgereicht. Denn soweit das Kennzeichen aus sich heraus Rückschlüsse auf den konkreten Inhalt des Schriftstückes zulässt oder der Inhalt des Schriftstückes bei verschlossenem Umschlag erkennbar ist, liegt ein Verstoß gegen die DS-GVO vor.[121] Eine solche Datenverarbeitung ist für die Aufgabenwahrnehmung nicht erforderlich. Wir haben dieses Vorgehen der Gerichtsvollzieherin mit einer Verwarnung gerügt.

Gerichtsvollzieher:innen dürfen bei Zustellungen keine „sprechenden" Geschäftszeichen verwenden.

Der Senat teilt die Auffassung der Berliner Beauftragten für Datenschutz und Informationsfreiheit, dass in dem geschilderten Fall ein Verstoß gegen die DS-GVO vorliegt. Er hat daher den Präsidenten des Kammergerichts als zuständige Oberbehörde gebeten, alle Gerichtsvollzieherinnen und Gerichtsvollzieher seines Geschäftsbereichs über die jeweiligen Präsidentinnen und Präsidenten der Amtsgerichte über die Beanstandung zu informieren und auf diese Weise zu sensibilisieren.

4.5 Beschränkung des Rechts auf Auskunft gegenüber der Rechtsanwaltschaft

Uns erreichen immer wieder Beschwerden von Bürger:innen, die bei einem Rechtsanwalt bzw. einer Rechtsanwältin die Erteilung einer datenschutzrechtlichen Auskunft beantragt haben. Als Verantwortliche unterliegen Rechtsanwält:innen grds. den Regelungen der DS-GVO und müssen daher auch geeignete Maßnahmen ergreifen, um den betroffenen Personen die jeweiligen Informationen und Mitteilungen zu übermitteln.[122] Das Recht der betroffenen Personen auf Auskunft kann ggü. der Rechtsanwaltschaft jedoch unter Umständen beschränkt sein.

[121] Siehe Art. 6 Abs. 1 Satz 1 lit. e DS-GVO i. V. m. § 132 Abs. 1 BGB
[122] Siehe Art. 12 DS-GVO

Dies hängt mit deren Stellung als sog. Berufsgeheimnisträger:innen bzw. mit der anwaltlichen Verschwiegenheitsverpflichtung zusammen.[123]

Um den Verschwiegenheitspflichten und dem Mandatsgeheimnis Rechnung zu tragen, enthält die DS-GVO Ausnahmetatbestände, die Berufsgeheimnisträger:innen bei der Erfüllung von bestimmten datenschutzrechtlichen Pflichten privilegieren.[124] Darüber hinaus ist der nationale Gesetzgeber befugt, auf Grundlage von sog. Öffnungsklauseln Regelungen zur Einschränkung von Informations- und Benachrichtigungspflichten der Berufsgeheimnisträger:innen zu erlassen, um den Schutz von vertraulichen Daten zu sichern.[125] Der Bundesgesetzgeber hat hiervon im Rahmen der Neufassung des Bundesdatenschutzgesetzes (BDSG) Gebrauch gemacht.[126] So besteht das Recht auf Auskunft der betroffenen Person nach Art. 15 DS-GVO nicht, „soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.“[127] Der grds. umfassende Auskunftsanspruch wird somit hinsichtlich zwingend geheimhaltungsbedürftiger Informationen beschränkt und den Geheimhaltungspflichten ausnahmsweise Vorrang eingeräumt.[128]

Der Wortlaut der entsprechenden Regelung spricht jedoch dafür, dass das Auskunftsrecht einer betroffenen Person ggü. einem Rechtsanwalt bzw. einer Rechtsanwältin nicht generell ausgeschlossen ist, sondern dass der bzw. die Berufsgeheimnisträger:in im Einzelfall prüfen muss, ob bzw. inwieweit durch eine Auskunft Informationen herausgegeben würden, die geheimhaltungsbedürftig sind. In der Praxis zeigt sich, dass insbesondere gegnerische Parteien eines prozessualen oder außerprozessualen Rechtsstreits einen Auskunftsanspruch nach Art. 15 DS-GVO bei Kanzleien geltend machen. In diesen Fällen ist die Interessenabwägung bzw. Identifizierung und Abgrenzung von geheimhaltungsbedürftigen Informationen regelmäßig schwierig. Zu bedenken ist, dass Gegenstand einer Auskunft an die betroffene Person dann regelmäßig Daten sind, die der bzw. die Berufsgeheimnisträger:in in eben dieser

[123] Siehe § 203 Abs. 1 Nr. 3 Strafgesetzbuch (StGB), § 43a Abs. 2 Satz 1 Bundesrechtsanwaltsordnung (BRAO) i. V. m. § 2 Abs. 1 Satz 1 Berufsordnung für Rechtsanwälte (BORA)
[124] Siehe Art. 14 Abs. 5 lit. b und d DS-GVO
[125] Siehe Art. 23 Abs. 1 lit. i DS-GVO und Art. 90 Abs. 1 DS-GVO
[126] Siehe §§ 29, 32 bis 35 BDSG
[127] § 29 Abs. 1 Satz 2 BDSG
[128] Jandt in Roßnagel, Das neue Datenschutzrecht § 8 Rn. 318

Eigenschaft (vor allem von dem bzw. der eigenen Mandant:in) erhalten hat.

Rechtsanwält:innen dürfen Auskunftsanträge nach Art. 15 DS-GVO nicht pauschal ablehnen, sondern müssen im Einzelfall prüfen, ob und inwieweit das Auskunftsrecht der antragstellenden Person aufgrund des Mandatsgeheimnisses bzw. der anwaltlichen Verschwiegenheitsverpflichtung ausgeschlossen ist. Über die Gründe für einen (teilweisen) Ausschluss des Auskunftsrechts bzw. die Gründe für eine Weigerung der Auskunftserteilung muss die betroffene Person unterrichtet werden.[129]

5 Jugend, Bildung, Wissenschaft und Forschung

5.1 Ausführungsvorschriften für die Jugendhilfe — Datenschutz von vornherein mitgedacht

Die Senatsverwaltung für Bildung, Jugend und Familie hat in diesem Jahr Gemeinsame Ausführungsvorschriften zur Zusammenarbeit von Schulen und bezirklichen Jugendämtern im Kinderschutz (AV JugSchul Kinderschutz)[130] erlassen. Gleichzeitig hat sie zur verbindlichen Umsetzung dieser Ausführungsvorschriften einen „Handlungsleitfaden Kinderschutz“ zur Zusammenarbeit zwischen Schulen und bezirklichem Jugendamt veröffentlicht.[131] Wir haben die Senatsverwaltung bei der Erarbeitung der Vorschriften und des Handlungsleitfadens beraten.

Die ressortübergreifende Zusammenarbeit zwischen bezirklichen Jugendämtern und anderen Stellen wirft gerade im Bereich des Kinderschutzes im praktischen Alltag immer wieder erhebliche Datenschutzfragen auf.[132] Ausführungsvorschriften dienen dem Zweck, die gesetzlichen Regelungen und Aufgabenzuweisungen zu konkretisieren und damit die praktische Umsetzung zu erleichtern. Hierbei ist es wichtig, den Fachkräften in den Jugendämtern und den Lehrkräften in den Schulen möglichst konkrete Handlungsanleitungen für die Praxis zur Verfügung zu stellen.

Während das Verfahren für den Umgang mit Kindeswohlgefährdungen bei den Jugendämtern durch

[129] Siehe Art. 12 Abs. 4 DS-GVO
[130] Siehe https://www.berlin.de/sen/jugend/recht/rechtsvorschriften/av_kinderschutzjugschul.pdf
[131] Siehe https://www.berlin.de/sen/jugend/familie-und-kinder/kinderschutz/fachinfo/handlungsleitfaden_kinderschutz_schul_jug.pdf
[132] Siehe zur Zusammenarbeit zwischen Jugend-, Gesundheits- und Sozialämtern im Kinderschutz JB 2015, 6.2; JB 2016, 5.1; JB 2017, 6.1

die Gemeinsamen Ausführungsvorschriften über die Durchführung von Maßnahmen zum Kinderschutz im Land Berlin (AV Kinderschutz JugGes)[133], über die wir in der Vergangenheit mehrfach berichtet haben,[134] detailliert geregelt wird, fehlten bislang entsprechende Regelungen für den Umgang mit Kindeswohlgefährdungen für die Schulen.

Mit den nun erlassenen Ausführungsvorschriften wird im Fall eines in der Schule bekannt gewordenen Verdachts einer Kindeswohlgefährdung ein berlineinheitliches Verfahren vorgegeben, das von den Schulen einzuhalten ist und ggf. eine Information des zuständigen Jugendamtes erfordert. Da es sich bei Kinderschutzfällen immer um höchst sensitive Sachverhalte handelt, muss auf der einen Seite ein besonderes Augenmerk auf die Einhaltung der Datenschutzvorgaben gerichtet werden, um den Schutz der betroffenen Kinder und Jugendlichen zu gewährleisten. Auf der anderen Seite ist es notwendig, auch den Lehrkräften durch klare Vorgaben die vielfach vorliegende Rechtsunsicherheit hinsichtlich des Umgangs mit diesen sensitiven Informationen zu nehmen. Den Lehrkräften muss Handlungssicherheit gegeben werden, welche Daten sie verarbeiten und ggf. an das Jugendamt weitergeben dürfen, damit der Verdacht einer Kindeswohlgefährdung aufgeklärt und eine Gefährdung des Wohls von Kindern und Jugendlichen wirksam abgewendet werden kann. Die zuständige Senatsverwaltung hat hierfür einheitliche Dokumentations- und Mitteilungsbögen entwickelt, die von den Schulen verbindlich zu verwenden sind.

Da die im Zusammenhang mit dem Verdacht einer Kindeswohlgefährdung in den Schulen anfallenden Unterlagen datenschutzgerecht aufbewahrt und vernichtet werden müssen, wenn sie nicht mehr erforderlich sind, war auch dies in den Ausführungsvorschriften zu berücksichtigen. Unsere Vorschläge zur Konkretisierung der Vorschriften in diesem Punkt hat die zuständige Senatsverwaltung aufgegriffen. Wir halten es jedoch für zielführend, bei der ohnehin anstehenden Überarbeitung der Schuldatenverordnung[135] auch konkretisierende Regelungen zum Umgang mit den im Zusammenhang mit Verdachtsfällen von Kindeswohlgefährdungen entstehenden Unterlagen zu schaffen.

Die Senatsverwaltung für Bildung, Jugend und Familie hat uns rechtzeitig um Durchsicht der Unterla-

[133] Siehe https://www.berlin.de/sen/jugend/recht/mdb-sen-jugend-rechtsvorschriften-av_kinderschutz.pdf
[134] JB 2015, 6.2; JB 2016, 5.1; JB 2017, 6.1
[135] Siehe 1.2.2

gen und entsprechende Beratung gebeten. Unsere Hinweise zu den Ausführungsvorschriften und dem Handlungsleitfaden nebst Dokumentations- und Mitteilungsbogen wurden übernommen. Die fehlenden Vorgaben zum Umgang mit Verdachtsfällen von Kindeswohlgefährdungen sollten in der Schuldatenverordnung, deren Überarbeitung ohnehin ansteht, entsprechend ergänzt werden.

5.2 Unverschlüsselter Versand von Zeugniskopien

Die Schulen waren zu Beginn der Winterferien weiterhin von pandemiebedingten Schulschließungen betroffen. Die Halbjahreszeugnisse sollten deshalb nicht – wie gewohnt – vor, sondern erst nach den Winterferien an die Schüler:innen ausgegeben werden. Die Mitteilung der Bildungsverwaltung, Schüler:innen und Erziehungsberechtigten könne auf Wunsch eine Kopie des Zeugnisses auch per E-Mail übermittelt werden, führte bei einzelnen Schulleitungen angesichts der vertraulichen Inhalte zu - datenschutzrechtlicher Unsicherheit.

Datenschutzrechtlich liegt es auf der Hand, dass der unverschlüsselte Versand von Zeugniskopien, die u. a. Noten, Fehlzeiten und Angaben zum Sozialverhalten enthalten, problematisch ist. Die Bildungsverwaltung sah sich offenbar veranlasst, die Schulen in einem weiteren Schreiben darauf hinzuweisen, dass die Übermittlung vorzugsweise Ende-zu-Ende-verschlüsselt und passwortgeschützt erfolgen sollte, führte jedoch dann weiter aus: „Wenn die betroffene Person ausdrücklich um Übermittlung gebeten hat, obwohl diese Voraussetzungen nicht gegeben sind, ist auch das zulässig.“ Gleichzeitig unterbreitete sie einen Textvorschlag für eine Einwilligung in den unverschlüsselten Versand per E-Mail.

Abgesehen davon, dass der Textvorschlag als solcher nicht die datenschutzrechtlichen Anforderungen an eine wirksame Einwilligung erfüllt, hat es uns doch sehr verwundert, dass die Bildungsverwaltung als Rechtsgrundlage für die Einwilligung § 36 des Berliner Datenschutzgesetzes (BlnDSG) benannt hat. Dies ist eine Vorschrift, die allein für die Datenverarbeitung durch Strafverfolgungs- und Strafvollstreckungsbehörden, d. h. insbesondere Polizei, Staatsanwaltschaft und Gerichte, anwendbar ist, jedoch keinesfalls für Schulen. Deren Datenverarbeitung richtet sich allein nach der Datenschutz-Grundverordnung (DS-GVO).

Da die Einhaltung angemessener technischer und organisatorischer Maßnahmen von den Verantwort-

lichen sicherzustellen ist, sehen wir für eine Übermittlung von Schulzeugnissen auf der Grundlage von Einwilligungen keinen Raum. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) hat zu dieser Thematik jüngst einen Beschluss gefasst, nach dem die von Verantwortlichen vorzuhaltenden technischen und organisatorischen Maßnahmen auf objektiven Rechtspflichten beruhen, die nicht zur Disposition der Beteiligten stehen.[136] Ein Verzicht auf entsprechende Maßnahmen auf Basis einer Einwilligung wird nicht für zulässig erachtet. Angewendet auf das zwischen Schüler:innen und Schulen bestehende Über-/Unterordnungsverhältnis kommen Einwilligungen im Schulkontext ohnehin kaum in Betracht.[137]

In der Sache wäre in der Situation – wie im Übrigen von der Bildungsverwaltung auch selbst ausgeführt – eine postalische Übermittlung datenschutzrechtlich vorzugswürdig gewesen. Zwar ist der Versand von Zeugnissen im Wege einer Ende-zu-Ende-Verschlüsselung datenschutzrechtlich nicht zu beanstanden, jedoch sind die wenigsten Schulen derzeit in der Lage, ihre E-Mails entsprechend verschlüsselt zu versenden, geschweige denn haben die meisten Eltern die Möglichkeit zum Empfang Ende-zu-Ende verschlüsselter E-Mails geschaffen.

Wir halten es für notwendig, dass den Schulleitungen und Lehrkräften Lösungen angeboten werden, die diese in die Lage versetzen, sich rechtssicher verhalten zu können. Die Schaffung einer Möglichkeit zur datenschutzkonformen Kommunikation zwischen Lehrkräften, Eltern und Schüler:innen halten wir für überfällig. Wir stehen den Schulen und auch der Bildungsverwaltung dabei gern beratend zur Seite.

5.3 Corona-Selbsttests an Schulen

Im April führte der Senat verpflichtende Selbsttestungen auf eine Infektion mit dem Coronavirus SARS-CoV-2 für die Schüler:innen unter Aufsicht des pädagogischen Personals an allen Schulen ein. Wir erhielten eine Vielzahl von Anfragen und Beschwerden besorgter Eltern, aber auch Lehrkräfte zu diesem Thema. Neben Sorgen über gesundheitliche Gefährdungen wurden Befürchtungen geäußert, die Selbsttests könnten zu einer Verletzung von Persönlichkeitsrechten und Stigmatisierung positiv getesteter Schüler:innen führen.

[136] Siehe https://www.datenschutzkonferenz-online.de/media/dskb/20211124_ TOP_7_Beschluss_ Verzicht_ auf_TOMs.pdf
[137] Siehe EG 43 DS-GVO

Schulen verarbeiten im Fall des Auftretens eines positiven Testergebnisses Gesundheitsdaten der betroffenen Schüler:innen. Diese sensitiven Daten unterliegen einem besonderen Schutz und dürfen nur verarbeitet werden, wenn eine entsprechende Rechtsgrundlage vorliegt. Eine solche enthält das Schulgesetz (SchulG). Es erlaubt den Schulen die Verarbeitung von Gesundheitsdaten, wenn diese erforderlich ist für die Erfüllung der im SchulG geregelten schulbezogenen Aufgaben.[138] Zudem hat die Bildungsverwaltung für die Durchführung der Testungen an den Schulen mit der Schul-Hygiene-Covid-19-Verordnung[139] eine Vorschrift geschaffen, die ausdrücklich auch die Verarbeitung der Testergebnisse durch die Schulen erlaubt. Datenschutzrechtliche Bedenken gegen die Verarbeitung der Gesundheitsdaten durch die Schulen bestehen insoweit nicht.

Wir haben allerdings durchaus das Problem erkannt, dass es bei der Durchführung der Testung aller anwesenden Schüler:innen im Klassenraum kaum vermeidbar ist, dass Gesundheitsdaten positiv getesteter Schüler:innen auch den übrigen Anwesenden zur Kenntnis gelangen. Um einen größtmöglichen Schutz der Gesundheitsdaten sicherzustellen, wäre sicher ein Verfahren vorzugswürdig gewesen, mit dem organisatorisch gewährleistet werden kann, dass die Gesundheitsdaten Dritten ggü. nicht offengelegt werden, wie es z. B. bei einer Einzeltestung der Fall wäre. Allerdings ließe sich ein solches Verfahren für alle Schüler:innen praktisch nicht durchsetzen. Im Falle eines positiven Testergebnisses kann die Kenntnis der Information im Übrigen auch für mögliche Kontaktpersonen erforderlich sein, um die notwendigen Maßnahmen ergreifen zu können, z. B. die Anordnung einer Quarantäne.

Wir haben in der Beantwortung der Anfragen und Beschwerden darauf hingewiesen, dass es sich um eine komplexe Situation handelt, die die Schulen vor erhebliche Herausforderungen stellt. Gleichzeitig haben wir festgestellt, dass die Entscheidung darüber, welches Verfahren der Durchführung von Selbsttests in einer Abwägung der unterschiedlichen betroffenen Rechtsgüter die geringsten Grundrechtseingriffe mit sich bringt, nicht allein datenschutzrechtlich bewertet werden kann. Nach einer anfänglichen Flut von Beschwerden zu der Thematik ver-

[138] § 64 Abs. 1 und 2 SchulG

[139] Zum Zeitpunkt der Einführung der Testpflicht galt § 5 Schul-Hygiene-Covid-19-Verordnung (SchulHygCov-19-VO). Eine entsprechende Rechtsgrundlage findet sich aktuell in § 3 Zweite Schul-Hygiene-Covid-19-Verordnung (2. SchulHygCoV-19-VO).

ringerte sich deren Anzahl nach einigen Wochen erheblich. Wir schließen daraus, dass die Schulen einen Weg gefunden haben, einen Ausgleich zwischen den betroffenen Rechtsgütern herzustellen, um die Verletzung von Persönlichkeitsrechten zu vermeiden.

5.4 Digitale Erpressung: Was gegen Ransomware getan werden muss

Wir erhalten regelmäßig Meldungen über Datenpannen, die von Ransomware verursacht wurden. Professionelle Kriminelle infiltrieren die Informationstechnik von Unternehmen und Behörden, um Geld zu erpressen. Wir beraten betroffene Stellen und legen bei technischen Kontrollen besonderen Wert auf vorbeugende Maßnahmen.

Die Technische Universität Berlin, das Kammergericht, die Stadt Bitterfeld, der Landkreis Ludwigslust-Parchim aber auch viele kleine und mittlere Unternehmen verbindet eine Gemeinsamkeit. Alle wurden Opfer von Angriffen mit sog. Ransomware – Schadprogrammen, deren Zweck es ist, von den Betroffenen Geld zu erpressen. Solche Angriffe werden inzwischen in erster Linie von organisierten Kriminellen durchgeführt und so ähnelt sich oft auch deren Vorgehen.

War ein Angriff erst einmal erfolgreich und hat die IT-Systeme kompromittiert, so dauert es mitunter Monate, bis die angegriffene Stelle wieder ihre volle Arbeitsfähigkeit hergestellt hat. Insbesondere bei komplexen, unübersichtlichen Systemlandschaften, wie sie z. B. an den Hochschulen vorherrschen, ist es alles andere als trivial, sicherzustellen, dass die Schadprogramme von allen wieder in Betrieb genommenen Geräten entfernt wurde. Anderenfalls kann es zu einer Wiederholung des Angriffs kommen.

Ransomware ist kein neues Problem. In den letzten Jahren hat aber eine deutliche Professionalisierung der Angreifer:innen stattgefunden. Wurden zu Anfang wahllos IT-Systeme weitgehend automatisiert verschlüsselt, um relativ kleine Beträge zu erpressen, ist das Vorgehen inzwischen meist ein anderes. Kriminelle Gruppen gehen arbeitsteilig vor und spezialisieren sich auf unterschiedliche Phasen eines Angriffs. Die dabei eingesetzte Software wird häufig von anderen Kriminellen als „Software-as-a-Service“ eingekauft. Anstatt wie früher ein infiziertes System möglichst schnell automatisiert zu verschlüsseln, ist das aktuell angewandte Vorgehen meist ein vorsichtiges, manuell begleitetes Erkunden

eines Netzwerks, in welchem sich ein infiziertes System befindet. Bevor die eigentliche Erpressung beginnt, versuchen die Angreifer:innen sich auf möglichst viele Systeme im Netzwerk auszubreiten. Um den Druck auf die Opfer zu erhöhen, wird oft versucht, Backups zu zerstören oder zu kompromittieren. Außerdem – und hier liegt die besondere Brisanz für den Datenschutz – werden inzwischen auch in vielen Fällen Daten durch die Angreifer:innen heruntergeladen. Denn unter diesen Daten sind häufig auch Daten von Kund:innen. Die Kriminellen drohen mit der Veröffentlichung der Daten und nicht selten gelangen diese im Zuge des Angriffs tatsächlich an die Öffentlichkeit.

Die Ursachen für einen erfolgreichen Angriff sind in vielen Fällen ähnlich. Nach erfolgreicher Erstinfektion eines Systems, welche oft in Form eines infizierten E-Mail-Anhangs oder eines Links auf Schadsoftware beginnt, verbinden sich Angreifer:innen mit diesem System und nutzen es als eine Art Sprungbrett zu weiteren im Netzwerk erreichbaren Systemen. Auch wenn die meisten Softwarehersteller Sicherheitsupdates bereitstellen, werden diese oftmals nicht oder nicht rechtzeitig auf den Systemen installiert. Die Gründe hierfür sind vielfältig und reichen von unzureichendem Patch-Management[140] seitens der IT-Verantwortlichen bis hin zum wissentlichen Einsatz von alter, unsicherer Software, z. B., weil eine kritische Anwendung nicht darauf vorbereitet wurde, mit einer neueren Version des Betriebssystems oder anderer grundlegender Software zusammenzuarbeiten. Aufgrund der Vernetzung der Systeme untereinander genügt dabei manchmal ein einziges unsicheres System, um Angreifer:innen die Tür zum gesamten Netzwerk der Verantwortlichen zu öffnen.

Äußerst problematisch ist außerdem, dass viele IT-Systeme im Auslieferungszustand zunächst unsicher konfiguriert sind und erst einmal durch kompetentes Personal in einen Zustand gebracht werden müssen, in welchem es möglich ist, diese sicher zu betreiben.

Vielfach suchen die Verantwortlichen ihr Heil in einer möglichst umfassenden Überwachung und Protokollierung der Aktivitäten der IT-Systeme. In der Tat sind Überwachungssysteme verfügbar, die bestimmte Angriffsmuster erkennen und vor ihnen - warnen können. So soll ein Angriff frühzeitig er-

[140] Patch-Management beschreibt den Prozess, installierte Software zu aktualisieren und z. B. mit Sicherheitsupdates zu versorgen.

kannt und zumindest seine Auswirkungen begrenzt werden. Doch zum einen kann sich die Wirksamkeit der Systeme als niedriger erweisen als beworben, da die Angreifer:innen Umgehungsstrategien entwickeln. Und zum anderen steht eine unüberlegte Überwachung in einem Spannungsverhältnis zum Datenschutz. Sie ist nur dann zulässig, wenn sie datensparsam konfiguriert ist, wenn sichergestellt ist, dass die Nutzer:innen der Systeme informiert sind, dass und in welchem Umfang die Systeme überwacht werden, und wenn die Protokolldaten ausschließlich für die Gewährleistung der Sicherheit der IT-Systeme und nicht für die Kontrolle der Leistung und des Verhaltens der Beschäftigten genutzt werden. Leider beobachten wir regelmäßig, dass Daten prophylaktisch gesammelt werden, ohne dass ein Plan aufgestellt wurde, wie und unter welchen Bedingungen sie ausgewertet werden sollen. Zu jedem Protokoll, das personenbezogene Daten enthält, gehört auch eine Vorgabe zu seiner datenschutzgerechten Auswertung.

Eine weitere wirksame Maßnahme, welche den Schaden im Falle eines erfolgreichen Angriffs begrenzen kann, ist eine Aufteilung der IT-Systeme der Verantwortlichen auf verschiedene Teilnetze. Diese Teilnetze werden dann so voneinander getrennt, dass nur noch der unbedingt nötige Datenverkehr zwischen ihnen fließen und überwacht werden kann. Durch eine solche Trennung lässt sich im günstigen Fall auch ein erfolgreicher Angriff auf einen kleinen Teilbereich der IT beschränken.

Unternehmen und öffentliche Stellen müssen in die Sicherheit ihrer IT-Systeme investieren. Insbesondere muss sichergestellt werden, dass die eingesetzte Software immer auf dem neusten Stand ist und bekannte Sicherheitslücken beseitigt werden. Gleichzeitig sollten Softwarehersteller dafür Sorge tragen, dass ihre Produkte bereits in ihrer Grundkonfiguration möglichst sicher betrieben werden können. Wo dies nicht der Fall ist, sind die Verantwortlichen in der Pflicht, eine sichere Konfiguration herzustellen. Dazu kann auch zählen, dass große Organisationen ihre IT-Systeme in kleinere Einheiten aufteilen, sodass im Falle eines erfolgreichen Angriffs zumindest das Schadenspotenzial reduziert ist.
Vor dem Hintergrund, dass die Angreifer:innen dazu übergehen, Daten herunterzuladen und zu einem späteren Zeitpunkt zu verkaufen, ist es aus Sicht des Datenschutzes noch einmal wichtiger geworden, wirksame Maßnahmen zu ergreifen, da es nun nicht mehr nur um die Verfügbarkeit von Daten, sondern auch um die Gewährleistung ihrer Vertraulichkeit geht.

6 Gesundheit und Pflege

6.1 Kontaktnachverfolgung in Gesundheitsämtern

Zur effizienten Betreuung von Personen, die mit SARS-CoV-2 infiziert sind, und zur Nachverfolgung ihrer Kontakte soll in den Gesundheitsämtern die Software SORMAS[141] zum Einsatz kommen. Wir haben die Senatsverwaltung für Gesundheit, Pflege und Gleichstellung (SenGPG) bei der Einführung beraten. Gleichzeitig gaben wir zusammen mit Aufsichtsbehörden anderer Länder und des Bundes in einer Arbeitsgruppe Hinweise an die Entwickler:innen und Betreiber:innen des Systems.

Die SARS-CoV-2-Pandemie hat die Gesundheitsämter einem besonderen Druck ausgesetzt. Um den großen Umfang der Infektionsmeldungen zu bewältigen und die Kontaktpersonen von Infizierten zu informieren, sahen sich die Gesundheitsämter gezwungen, ihre Prozesse zu optimieren. Technische Lösungen sollen dabei den Umgang mit der großen Zahl an Infektionsmeldungen vereinfachen und vereinheitlichen.

Wird eine Infektion durch ein Labor bestätigt, erhält das zuständige Gesundheitsamt über das Deutsche Elektronische Melde- und Informationssystem für den Infektionsschutz (DEMIS) eine Mitteilung und kontaktiert die betroffenen Personen. Diese werden über die Umstände der Infektion und nach den Kontakten der letzten Tage befragt, um weitere möglicherweise bereits infizierte Kontaktpersonen warnen zu können. Darüber hinaus kann das Gesundheitsamt anordnen, dass die Kontaktpersonen sich testen lassen oder sogar in Quarantäne gehen müssen.

Dabei verarbeiten die Gesundheitsämter, wie bei vielen anderen meldepflichtigen Infektionskrankheiten auch, Gesundheitsdaten in großem Umfang und übermitteln im Rahmen ihres gesetzlichen Auftrags täglich Infektionszahlen an das Robert-Koch-Institut (RKI).

Für diese Arbeit steht den Gesundheitsämtern die Software SORMAS zur Fallbearbeitung und Kontaktnachverfolgung zur Verfügung.[142] Hierbei handelt es sich um eine quelloffene Software, die ursprünglich zur Bewältigung früherer Epidemien, wie

[141] Surveillance, Outbreak Response Management and Analysis System

[142] Neben SORMAS setzen einige Gesundheitsämter weitere Systeme ein; siehe dazu 1.5

bspw. Ebola in Afrika entwickelt wurde. Einige Gesundheitsämter setzen diese Software bereits ein. Wir haben SenGPG bei der flächendeckenden Einführung von SORMAS intensiv beraten.

Ergänzend haben wir uns darum bemüht, auf die Entwicklung des Softwareprodukts Einfluss zu nehmen. Zusammen mit anderen Aufsichtsbehörden standen wir dafür im Austausch mit dem Helmholtz-Zentrum für Infektionsforschung (HZI), das die Entwicklung der Software im Auftrag des Bundesministeriums für Gesundheit (BMG) koordiniert. Im Ergebnis der Entwicklung soll für die Gesundheitsämter bundesweit eine Version von SORMAS durch eine Institution des Bundes bereitgestellt werden.

Diese zentral betriebene Version mit Namen SORMAS X wurde bereits im Jahr 2020 in Betrieb genommen und in einigen Bundesländern, nicht jedoch in Berlin, im Pilotbetrieb eingesetzt. Entgegen seiner Zusagen war der Projektentwickler HZI im Laufe dieses Jahres nicht in der Lage, die erheblichen Defizite der Software zu beseitigen, auf die die Aufsichtsbehörden hingewiesen hatten. Fristen wurden nicht eingehalten und Dokumente nicht wie gefordert vorgelegt. Es blieb unklar, ob selbst angekündigte Maßnahmen umgesetzt wurden.

Wesentliche Kritikpunkte betrafen den Umfang der mit der Software zu verarbeitenden Daten; die nicht nachvollziehbaren Festlegungen und mangelnden Funktionalitäten zur Löschung von Daten, die für die weitere Arbeit der Gesundheitsämter nicht mehr benötigt werden; die Regelung der Berechtigungen für Gesundheitsämter und ihre Beschäftigten, mit den Daten zu arbeiten; die mangelnde Absicherung von Schnittstellen des Systems nach außen und die Ausgestaltung der Funktionen für den Austausch von Daten zwischen den verschiedenen an der Bearbeitung eines Falls beteiligten Ämtern.

Wir haben uns aufgrund der mangelnden Kooperationsbereitschaft des HZI dazu entschlossen, uns aus dem Beratungsprozess zurückzuziehen. Der zuständigen Senatsverwaltung können wir eine Beteiligung der Berliner Gesundheitsämter an SORMAS X derzeit nicht empfehlen. Die durch einige Gesundheitsämter bereits jetzt eingesetzte und von ihnen selbst betriebene Version der Anwendung ist von dieser Einschätzung nicht betroffen.

Die digitale Fallbearbeitung und Kontaktnachverfolgung in den Gesundheitsämtern steckt noch in den Kinderschuhen. Die Gesundheitsämter benöti-

gen Lösungen, die ihnen eine effiziente Arbeit und – ohne zusätzliche Investitionen an Kraft und Ressourcen – den Schutz der betroffenen Bürger:innen vor Risiken und einer überbordenden Verarbeitung ihrer Daten ermöglichen.

6.2 Digitale Impfzertifikate: Fälschung verhindern, sicher prüfen

Wir gingen Hinweisen auf Möglichkeiten nach, Impfzertifikate und Testnachweise zu fälschen, die Bürger:innen zum Nachweis der Einhaltung der 2G- bzw. 3G-Regeln benötigen, die zur Bekämpfung der Sars-CoV-2-Pandemie eingeführt wurden.

Aufgrund einer Reihe von Anfragen haben wir auch den Einsatz der CovPass-Check-App zur Prüfung digitaler COVID-Zertifikate untersucht und festgestellt, dass keine Gefahr droht.

Um in der Sars-CoV-2-Pandemie weitere Infektionen zu vermeiden, wurde beschlossen, dass nur Personen, die eine vollständige Impfung, ihre Genesung nach einer Infektion oder einen kürzlich erfolgten negativen Test auf Infektion nachweisen können (2G- bzw. 3G-Regeln), zu bestimmten Veranstaltungen zugelassen oder in bestimmte Einrichtungen eingelassen werden. Der Nachweis erfolgt über elektronisch erzeugte Dokumente, die mit einem sog. QR-Code (einem quadratischen Punkteraster) maschinenlesbar gemacht werden.

Die Vorteile, die mit einem der genannten Nachweise verbunden sind, erzeugen einen Anreiz, diese für Personen zu fälschen, die die Voraussetzungen für ihren legitimen Erwerb nicht besitzen.

Wir erhielten Hinweise auf Datenpannen sowohl bei Testzentren[143], als auch bei dem Betreiber eines Portals für die Impfzertifikatsvergabe. Die Ausstellung von Impfzertifikaten über dieses Portal, das für die Nutzung durch Apotheken vorgesehen war, musste über mehrere Wochen ausgesetzt werden, nachdem es Sicherheitsforscher:innen gelungen war, unbefugt ein Benutzerkonto für eine fiktive Apotheke zu registrieren und darüber beliebige Impfzertifikate auszustellen.

Wir gingen der Datenpanne bei dem Portal für die Impfzertifikatsvergabe nach und stellten sicher, dass der Betreiber des Portals aus der Panne ausreichende Lehren zieht. Der Fall zeigte erneut, wie wichtig es ist, ausreichend zuverlässige Vorgehensweisen zu

[143] Siehe 1.4

etablieren, mit denen die Identität von Beteiligten eines Verfahrens – hier der Apotheken – festgestellt und sichergestellt wird, dass diese befugt sind, die von ihnen beanspruchte Rolle in dem Verfahren einzunehmen. Hierauf haben die Aufsichtsbehörden wiederholt in verschiedenen Kontexten hingewiesen.

Keinen Grund zur Sorge bietet jedoch der Einsatz der CovPassCheck-App zur Überprüfung von digitalen Impf- und Genesenenzertifikaten. Restaurants, Geschäfte und andere Einrichtungen sind gesetzlich verpflichtet, die durchlaufene Impfung oder Genesung von Besucher:innen anhand ihrer o. g. Zertifikate zu überprüfen. Hierfür hat das RKI die CovPassCheck-App herausgegeben.

Eine Reihe von Beschwerdeführer:innen haben sich an uns gewendet, da sie den Missbrauch der in ihren digitalen Zertifikaten enthaltenen Daten durch Veranstalter:innen in Folge der Nutzung der CovPass-Check-App befürchteten. Wir konnten ihnen bestätigen, dass die App den Veranstalter:innen nur den Status des jeweiligen Zertifikats sowie Name, Vorname und Geburtsdatum der/des Zertifikatsinhaber:in anzeigt. Letzteres ist erforderlich, um den Veranstalter:innen zu ermöglichen, anhand eines Ausweisdokuments der betroffenen Person die Inhaberschaft des Zertifikats zu überprüfen. Die App speichert bei der Prüfung des Zertifikats mithilfe eines Scans die Daten nur flüchtig. Bereits beim nächsten Scan werden die Daten automatisch gelöscht.

Natürlich gilt diese Einschätzung nur für die CovPassCheck-App. Sollten Veranstalter:innen eine andere App dazu verwenden, bspw. ein Foto von einem vorgewiesenen Zertifikat zu erstellen, verbliebe ihnen eine Kopie aller in dem Zertifikat enthaltenen Daten. Wir raten daher dazu, sich mit der CovPassCheck-App vertraut zu machen und die Veranstalter:innen darum zu bitten, das Display des Smartphones, mit dem die Kontrolle des digitalen Zertifikats durchgeführt wird, zunächst denjenigen zuzuwenden, die kontrolliert werden, und erst danach selbst einzusehen. Hinweise auf konkretes Fehlverhalten von Veranstalter:innen nehmen wir zur Prüfung entgegen.

Wer IT-Systeme zur Verarbeitung von personenbezogenen Daten für den Gebrauch durch eine Vielzahl von Beteiligten bereitstellt, muss für deren sichere Identifizierung sorgen, damit nur diejenigen sie nutzen können, die dazu berechtigt sind. Wenn

Verantwortliche Dokumente der Bürger:innen einsehen dürfen, dann heißt dies nicht, dass sie zur Fertigung einer Kopie berechtigt sind.

6.3 Höchstfristen sind keine zwingenden Speicherpflichten

Eine Bürgerin hatte sich bei uns darüber beschwert, dass die Kassenärztliche Vereinigung (KV) Berlin auf ihr Auskunfts- und Löschungsersuchen nicht reagiert habe. Die Begründung der KV hat uns nicht gänzlich überzeugt.

Auf unsere Nachfrage hat die KV ausgeführt, dass es im Zusammenhang mit der Versendung von Impfeinladungsschreiben im Frühjahr[144] zu einer erhöhten und das Normalmaß übersteigenden Vielzahl von Auskunftsanfragen gekommen sei. Zudem setze die KV zur Erfüllung ihrer Aufgaben zahlreiche Systeme ein, aus denen die angefragten Informationen zusammengetragen werden müssten. Dies habe sich in dem genannten Zeitraum aufgrund der Fülle der Anfragen als überaus zeitintensiv herausgestellt, weshalb sie diesen, wie im vorliegenden Fall, nicht sofort habe nachkommen können. Den Antrag auf Löschung hat die KV sogar komplett abgelehnt. Hierzu hat uns die KV mitgeteilt, dass sie der Aufforderung der Beschwerdeführerin nicht habe nachkommen können, da sie durch eine Regelung im Sozialgesetzbuch (SGB) zur Aufbewahrung verpflichtet sei.[145]

Dass dem Auskunftsersuchen der Beschwerdeführerin aufgrund der dargestellten Überlastung nicht innerhalb der gesetzlichen Frist von einem Monat entsprochen werden konnte, verwundert nicht und war für uns nachvollziehbar. Gleichwohl hätte die Beschwerdeführerin nach den Vorgaben der Datenschutz-Grundverordnung (DS-GVO)[146] zumindest über die Fristverlängerung und die Gründe für die Verzögerung informiert werden müssen. Aus datenschutzrechtlicher Perspektive interessanter war hingegen die Begründung der KV, warum sie sich an der Löschung der Sozialdaten der Beschwerdeführerin gehindert sah.

Richtig ist, dass die von der KV herangezogene Vorschrift im SGB vorsieht, dass bestimmte, im Gesetz näher bezeichnete Sozialdaten von den KV „spätestens nach zehn Jahren“ zu löschen sind. Hierbei handelt es sich jedoch nicht um eine Aufbewahrungspflicht, die der Löschung vor Ablauf

[144] Siehe 1.3.2
[145] Siehe § 304 SGB V
[146] Siehe Art. 12 Abs. 3 DS-GVO

dieses Zeitraums grds. entgegensteht. Vielmehr soll mit der Regelung gewährleistet werden, dass Sozialdaten nicht länger als zur Aufgabenerfüllung unbedingt notwendig gespeichert werden, wenn spezielle Vorschriften nicht eine längere Aufbewahrungsfrist vorsehen. Darauf deutet auch der Wortlaut („spätestens“) hin. Es werden mit der Regelung daher keine Aufbewahrungspflichten statuiert, die einer Löschung entgegenstehen, sondern Höchstfristen der Speicherung festgelegt. Eine Löschung vor Ablauf dieser Frist wäre also rechtlich durchaus möglich, wenn die weitere Verarbeitung der Daten zur Aufgabenerfüllung der Verantwortlichen nicht mehr erforderlich ist.

Ob diese Voraussetzungen im Ausgangsfall auch tatsächlich erfüllt waren, konnten wir auf Grundlage der uns zur Verfügung stehenden Informationen nicht beurteilen. Zudem ist es zunächst Sache der KV, zu prüfen, welche Daten der Beschwerdeführerin zur Erfüllung ihrer Aufgaben auch tatsächlich erforderlich sind. Wir haben die KV daher auf unsere Rechtsauffassung hingewiesen und gebeten, das Löschungsgesuch der Beschwerdeführerin auf Grundlage unserer Ausführungen erneut zu prüfen.

Zwischen Höchstfristen und zwingenden Speicherpflichten besteht ein entscheidender Unterschied. Insbesondere können Löschersuchen von betroffenen Personen nicht mit einem pauschalen Hinweis auf gesetzlich festgelegte Höchstspeicherfristen abgelehnt werden.

6.4 Löschung eines Eintrags über eine nicht bestätigte Kindeswohlgefährdung

In einer bei einem Gesundheitsamt geführten Akte ist der Eintrag, dass sich der Verdacht einer Kindeswohlgefährdung nicht bestätigt hat, spätestens nach Ablauf eines Jahres zu löschen.

Die für den öffentlichen Gesundheitsdienst geltenden Rechtsvorschriften sehen vor, dass personenbezogene Daten, sofern andere Rechtsvorschriften keine Aufbewahrungsfristen festlegen, zu löschen oder zu anonymisieren sind, sobald sie für den Zweck, zu dem sie verarbeitet wurden, nicht mehr benötigt werden, spätestens jedoch zwei Jahre nach Abschluss des die Datenverarbeitung auslösenden Vorgangs. [147]

Die Information, dass sich der Verdacht einer Kindeswohlgefährdung nicht bestätigt hat, wird bereits

[147] § 4d Abs. 1 Gesundheitsdienst-Gesetz (GDG)

nach Ablauf eines Jahres nicht mehr benötigt. Das ergibt sich aus einem Vergleich mit den für das Jugendamt geltenden Vorschriften[148]. Danach sind die Unterlagen spätestens ein Jahr nach der abschließenden Entscheidung zu vernichten und gespeicherte Daten zu löschen, sofern die verantwortliche Stelle im Rahmen einer Gefährdungseinschätzung zu dem Ergebnis gelangt, dass eine Kindeswohlgefährdung nicht vorliegt.

Daraus ergibt sich zwar nur, dass die betroffenen Daten nach spätestens einem Jahr für das Jugendamt unter den genannten Voraussetzungen nicht mehr erforderlich sind. Dasselbe muss aber auch für das Gesundheitsamt gelten. Denn es erschließt sich nicht, warum dieselben Daten für das Gesundheitsamt weiterhin erforderlich sein sollten, wenn sie für das Jugendamt nicht mehr benötigt werden. Auf unsere entsprechende Aufforderung hat das betroffene Gesundheitsamt den Eintrag aus der Akte gelöscht.

Sensitive Angaben zu einem nicht bestätigten Verdacht des Vorliegens einer Kindeswohlgefährdung dürfen nur solange aufbewahrt werden, wie es unbedingt erforderlich ist. Hier sollten Jugend- und Gesundheitsämter die gleichen Fristen anwenden.

6.5 Terminverwaltung in Arztpraxen — Was ist zu beachten?

Auch in diesem Jahr erhielten wir wieder zahlreiche Anfragen und Beschwerden von Bürger:innen aus dem gesamten Bundesgebiet zur Datenverarbeitung durch ein Unternehmen, das von Arztpraxen häufig zur Terminverwaltung eingesetzt wird. Zunehmend wandten sich auch Arztpraxen, Medizinische Versorgungszentren und Krankenhäuser an uns und baten um Hinweise, was sie bei der Inanspruchnahme von Anbieter:innen von Terminverwaltungssoftware beachten müssen.

Viele Praxen sind dazu übergegangen, ihre Terminverwaltung auf darauf spezialisierte Terminverwaltungsunternehmen auszulagern. Für die Praxen sind solche Unternehmen attraktiv, weil diese ihnen versprechen, die Auslastung bei reduzierter Wartezeit für die Patient:innen zu verbessern. Außerdem locken sie mit Zusatzfunktionen wie Terminerinnerungen für die Patient:innen.

[148] Gemeinsame Ausführungsvorschriften über die Durchführung von Maßnahmen zum Kinderschutz im Land Berlin (AV Kinderschutz JugGes), Abschnitt 7.3.3

Die so vertriebenen Lösungen kommen zum Einsatz, wenn Patient:innen selbst über eine dafür eingerichtete Internetseite von Terminverwaltungsunternehmen einen Termin in der Praxis buchen[149] oder wenn Patient:innen telefonisch oder in der Arztpraxis einen Termin vereinbaren und dieser Termin durch das Praxispersonal in das Online-Kalendersystem eines Terminverwaltungsunternehmens eingetragen wird. Im letzteren Fall erfahren die Patient:innen von der Verarbeitung ihrer Daten durch das Terminverwaltungsunternehmen oftmals erst dadurch, dass sie kurz vor dem Termin eine E-Mail oder SMS mit einer Terminerinnerung von dem Unternehmen erhalten.[150] Nicht nur Patient:innen, sondern auch Arztpraxen haben uns gefragt, ob die Patient:innen in den Einsatz von Terminverwaltungsunternehmen einwilligen müssen.

Eine Einwilligung der Patient:innen ist dann nicht erforderlich, wenn Terminverwaltungsunternehmen sog. Auftragsverarbeiter:innen der Arztpraxen sind. Auftragsverarbeiter:innen handeln auf Weisung der Arztpraxen. Die Datenverarbeitung durch Terminverwaltungsunternehmen ist dann insoweit – wie auch bei der Inanspruchnahme sonstiger IT-Dienstleistungsfirmen – vollständig den Arztpraxen, die diesen Dienst nutzen, zuzurechnen. Die Arztpraxen müssen die Patient:innen allerdings in ihrer Datenschutzinformation über den Einsatz von Auftragsverarbeiter:innen informieren.

Anders sieht es aus, wenn Arztpraxen ihre Patient:innen per E-Mail oder SMS an vereinbarte Arzttermine erinnern möchten. Denn Arztpraxen dürfen Patient:innen eine Terminerinnerung nur dann übermitteln oder durch Auftragsverarbeiter:innen übermitteln lassen, wenn die Patient:innen ggü. der Arztpraxis ausdrücklich darin eingewilligt haben, dass ihre Telefonnummern oder E-Mail-Adressen für die Terminerinnerung genutzt werden dürfen.[151] Arztpraxen sollten insoweit ihre Verfahrensweise überprüfen und ggf. anpassen.

Der Zweck der Speicherung der Termindaten entfällt, sobald der Termin vergangen ist. Da die Praxen die Termine inhaltlich in den Patient:innenakten dokumentieren, ist eine zusätzliche Speicherung in den Systemen der Terminverwaltungsunternehmen nach Ablauf des Termins unzulässig. Die somit nach Ablauf des Termins erforderliche zeitnahe Löschung der Daten aus dem Online-Kalendersystem sollte be-

[149] Siehe 6.6
[150] Siehe JB 2019, 6.3
[151] Siehe JB 2019, 6.3

reits im Auftragsverarbeitungsvertrag festgelegt werden.

Die Ärzt:innen müssen sicherstellen, dass die Sicherheit der Verarbeitung durch ihre Auftragsverarbeiter:innen gewährleistet ist, da sie selbst für die Verarbeitung der Daten verantwortlich bleiben. Da die Bewertung des Sicherheitsniveaus von Terminverwaltungsunternehmen eine komplexe Fragestellung ist, empfiehlt es sich für die meisten Arztpraxen, dazu externe Beratung einzuholen, zumindest aber auf gängige Datenschutz- oder Informationssicherheitszertifizierungen der Unternehmen zu achten. Außerdem müssen sie sicherstellen, dass sie die Unternehmen im Auftragsverarbeitungsvertrag zur Geheimhaltung verpflichten, um die ihnen als Berufsgeheimnisträger:innen obliegende gesetzliche Schweigepflicht zu erfüllen.

Auch für den Fall, dass Teile der Datenverarbeitung durch Auftragsverarbeiter:innen außerhalb Deutschlands, insbesondere außerhalb des Geltungsbereichs der DS-GVO stattfinden sollen, ist es geboten, diesbezüglich datenschutzrechtlichen Rat einzuholen.

Häufig besteht Unsicherheit sowohl bei Patient:innen als auch bei Ärzt:innen, was datenschutzrechtlich zu beachten ist, wenn Terminverwaltungsunternehmen eingesetzt werden. Häufig wiederkehrende Fragen haben wir in einer Informationssammlung beantwortet, die auf unserer Webseite abgerufen werden kann.[152]

6.6 Mit Klick zum Termin — Terminvergabeportale und ihr Umgang mit den Daten der Patient:innen

Für Patient:innen ist es komfortabel, selbst über ein Online-Terminvergabeportal Termine mit Arztpraxen zu vereinbaren. Bereits bei der Suche nach einem Termin kann es allerdings dazu kommen, dass höchstpersönliche Informationen wie die gesuchten Fachärzt:innen oder Behandlungsmethoden oder sogar Symptome eingegeben werden. Aufgrund von zwei Hinweisen prüften wir bei einem Anbieter, ob diese Daten unzulässig an Dritte übermittelt werden, und ob der Anbieter seinen Löschverpflichtungen nach Schließung eines Kontos nachkommt.

Sofern Terminverwaltungsunternehmen Webseiten betreiben, über die Patient:innen selbst Termine bei Arztpraxen buchen können, müssen sie sicherstellen, dass die von den Patient:innen eingegebenen

[152] https://www.datenschutz-berlin.de/infothek-und-service/themen-a-bis-z/terminverwaltung-von-arztterminen

(Gesundheits-)Daten vertraulich behandelt werden. Die Verarbeitung von besonderen Kategorien personenbezogener Daten i. S. d. Art. 9 DS-GVO, zu denen auch Gesundheitsdaten zählen, erfordert besondere Sorgfalt. Überwacht das Unternehmen zur Gewährleistung der Sicherheit der von ihm angebotenen Dienste die Interaktionen der Patient:innen mit seiner Internetseite, dürfen dabei keine für diesen Zweck nicht erforderlichen Daten erfasst werden. Besonders problematisch ist die Übermittlung sensitiver Daten wie z. B. die Übermittlung von Symptomen an Unternehmen in Staaten mit einem unzureichenden Datenschutzniveau.

Ein solches Vorgehen wurde uns dieses Jahr durch Sicherheitsforscher:innen bei einer App eines Terminverwaltungsanbieters gemeldet, bei dem wir bereits in der Vergangenheit dasselbe Vorgehen im Kontext seiner Internetseite moniert hatten. Durch die Sicherheitsforscher:innen wurde festgestellt, dass Daten u. a. an ein US-amerikanisches Unternehmen und damit in einen unsicheren Drittstaat übermittelt wurden.

Haben Patient:innen bei einem Terminverwaltungsunternehmen ein Nutzungskonto eingerichtet, um selbst Termine bei Arztpraxen online suchen zu können, besteht ein Vertragsverhältnis zwischen den Patient:innen und dem Terminverwaltungsunternehmen. Wird dieses Vertragsverhältnis gekündigt, entfällt der Zweck, für den das Terminverwaltungsunternehmen die personenbezogenen Daten der Patient:innen gespeichert hat. Mit dem Entfallen des Zwecks geht in aller Regel die Pflicht der/des Verantwortlichen zur unverzüglichen Datenlöschung[153] einher. Ausgenommen sind lediglich Daten, für die eine gesetzliche Aufbewahrungspflicht besteht. Die Löschung müssen die Verantwortlichen selbst vornehmen. Sie können ihr nicht dadurch nachkommen, dass sie den Patient:innen – wie es tatsächlich in einem Fall vorgekommen ist – die Löschung ihrer Daten selbst aufgeben.

Wir haben den betreffenden Anbieter in beiden Fällen um Stellungnahme gebeten und ihn aufgefordert, die vorgefundenen Mängel zu beheben.

Eine Übermittlung von unverschlüsselten Gesundheitsdaten durch Terminverwaltungsunternehmen an Dritte in unsicheren Drittstaaten im Zuge der Terminsuche oder -buchung durch die Patient:innen ist unzulässig, auch wenn sie zu Zwecken der Nut-

[153] Siehe Art. 17 DS-GVO

zungsanalyse erfolgt. Außerdem müssen sich die Patient:innen darauf verlassen können, dass nach einer Vertragskündigung ihre personenbezogenen Daten ohne weiteres Zutun von ihrer Seite gelöscht werden.

6.7 Leicht zu erbeutende Patient:innenakten

Von Amts wegen prüften wir bei einem Krankenhaus die Umsetzung einiger Standardmaßnahmen für die Gewährleistung der Sicherheit der von ihm verarbeiteten Patient:innendaten.

In Kliniken werden heutzutage große Mengen sensitiver Gesundheitsdaten von Patient:innen in digitaler Form verarbeitet. Sowohl Laborgeräte, mit denen physiologische Werte digital erfasst werden, als auch Tablet-Computer am Bett der Patient:innen gehören zum Klinikalltag. Dies hat selbstverständlich viele Vorteile, da die für die Behandlung oft dringend erforderlichen Gesundheitsdaten zeitnah zur Verfügung stehen, und Ärztinnen und Ärzte die Behandlungsdokumentation bspw. aus dem Homeoffice fortführen können. Der letztgenannte Aspekt gewann in der Pandemie zusätzliche Bedeutung.

Daten sind in digitalisierter Form andererseits neuen Risiken ausgesetzt. So versuchen Angreifer:innen immer wieder, von außen in die IT-Systeme der Krankenhäuser einzudringen, um Daten zu erlangen oder durch Verschlüsselung für die Benutzung - unbrauchbar zu machen und so ihre Opfer zu erpressen. Um sich dagegen zu wehren, sind solide Sicherheitsvorkehrungen nötig, die das Eindringen von Angreifer:innen erschweren und erfolgreiche Angriffe auf kleine Teile der Informationstechnik - beschränken.

Wir prüften, ob in dem betreffenden Krankenhaus vier grundlegende Vorkehrungen getroffen wurden: Die zuverlässige Authentifizierung von Beschäftigten bei ihrem Zugriff auf die Kliniksysteme aus dem Homeoffice, den Einsatz von zentral administrierten Dienstgeräten für diesen Zugriff, die Aufteilung der Informationstechnik in voneinander sicherheitstechnisch getrennte Bereiche je nach Schutzbedarf und Zwecken der Datenverarbeitung und die unverzügliche Behebung von entdeckten Schwachstellen in IT-Systemen.

Leider ergab unsere Prüfung wesentliche Defizite in allen vier Bereichen. In der Summe hätten Angreifer:innen mit wohlbekannten und relativ einfachen Angriffsmethoden weitreichenden Zugriff auf die IT-Systeme der Klinik und damit auch Einblick in

nahezu alle Akten aktuell behandelter und ehemaliger Patient:innen erlangen können.

Eine zuverlässige Authentifizierung der Beschäftigten bei ihrem Zugriff auf die Kliniksysteme aus dem Homeoffice setzt zweierlei voraus:

Erstens müssen die Berechtigten ihre Identität unzweifelhaft nachweisen, bevor sie die Passwörter und andere Informationen erhalten, die sie für die Anmeldung bei den Systemen benötigen. Dies gilt sowohl, bei der ersten Zuweisung eines Kontos, als auch bei der Wiederherstellung des Zugangs, wenn z. B. Passwörter vergessen wurden.

Zweitens darf es für Dritte nicht möglich sein, an diese Informationen zu gelangen. Weder durch das Mitschneiden des Netzwerkverkehrs noch durch Phishing – also durch die Vorspiegelung einer legitimen Webseite des Krankenhauses, auf die Beschäftigte durch gefälschte E-Mail-Nachrichten oder Eingriffe in den Netzwerkverkehr geleitet werden, um Passwörter abgreifen zu können –, noch durch Zugriff auf Speicherorte, an denen die für die Einwahl notwendigen Informationen gespeichert sind.

Etablierte Technologien wie Virtual-Private-Networks (VPNs) und Multi-Faktor-Authentifizierung (MFA/2FA) helfen, dies sicherzustellen. Passwörter und andere geheim zu haltende, für die Anmeldung ggf. notwendige Informationen (wie z. B. geheime Schlüssel) müssen von den Speicherorten, an denen sie bereitgestellt wurden, gelöscht werden, sobald die Berechtigten sie erhalten haben. Schließlich ist es nötig, wirklich alle von außerhalb des Krankenhauses zugänglichen Schnittstellen von IT-Systemen auf Risiken zu überprüfen.

Mit dem Einsatz von zentral administrierten Dienstgeräten für den externen Zugriff auf die Kliniksysteme wird sichergestellt, dass dieser Zugriff von einer sicheren Grundlage aus erfolgt. Kommen dagegen Privatgeräte zum Einsatz, ist die Sicherheit der mit ihnen verarbeiteten Daten stark gefährdet. Bemächtigen sich Angreifer:innen eines dieser regelmäßig nur schwach geschützten Systeme, können sie auf alle Daten zugreifen, zu denen auch die Eigentümerin oder der Eigentümer des Geräts Zugriff hat. Waren zu Beginn der Pandemie einige Verantwortliche noch überfordert, ihre Beschäftigten mit Dienstgeräten zu versorgen, so kann es zwei Jahre nach ihrem Beginn keine Entschuldigung mehr für dieses Versäumnis geben.

Die unverzügliche Behebung von entdeckten Schwachstellen gehört zu den elementarsten Anforderungen an einen sicheren Betrieb von Informationstechnik. In dem von uns geprüften Fall waren die Versäumnisse auf diesem Gebiet der IT-Leitung bekannt und wurden über lange Zeit toleriert. Selbst einige sicherheitskritische Systeme wurden mit Software betrieben, die von dem Hersteller nicht mehr gepflegt wird.

In Krankenhäusern sind eng vernetzte IT-Systeme verbreitet, die miteinander verzahnte Dienste anbieten. Softwareaktualisierungen müssen stets auf ihre Auswirkungen in diesen komplexen Systemen geprüft werden. Daher ist es nicht einfach, zu gewährleisten, dass sie hinreichend zeitnah eingepflegt werden. Dies benötigt vorausschauende Planung, die Zusammenarbeit mit den Softwarehersteller:innen, deren zügige Unterstützung vertraglich gesichert werden muss, und einen wohldurchdachten Prozess für den Test aktualisierter Software auf unerwünschte Effekte. Doch es gilt auch hier: Die Komplexität der Aufgabe ist keine Entschuldigung für langanhaltende Defizite.

Auf unsere Aufforderung hin hat das betreffende Krankenhaus begonnen, die Defizite sukzessive zu beseitigen. Der Prozess dauerte zu Redaktionsschluss noch an.

Die Digitalisierung im Gesundheitssystem bietet eine Vielzahl von Chancen, die die Behandlung von Patient:innen erheblich erleichtern und effizienter gestalten können. Durch sie entsteht aber gleichzeitig eine große Zahl neuer Gefahren für die Daten der Patient:innen. Die Verantwortlichen müssen daher der Gewährleistung der Sicherheit ausreichend Aufmerksamkeit und Ressourcen widmen. Methoden nach dem Stand der Technik sind systematisch anzuwenden, die Wirksamkeit der Maßnahmen regelmäßig zu überprüfen – auch aus der Warte externer Angreifer:innen – und gefundene Mängel konsequent und zeitnah auszuräumen.

7. Integration, Soziales und Arbeit

7.1 Beschwerdestelle für geflüchtete Menschen

Über die Einrichtung einer unabhängigen Beschwerdestelle für Geflüchtete durch die Senatsverwaltung für Integration, Arbeit und Soziales (SenIAS) haben wir schon mehrfach berichtet.[154] Die

[154] JB 2019, 7.1 und JB 2020, 6.1

Stelle soll geflüchteten Menschen niederschwellig die Möglichkeit bieten, sich über Missstände und Probleme im Zusammenhang mit ihrer Unterbringung beschweren zu können. Ihnen soll damit die Hürde genommen werden, sich an eine staatliche Stelle wenden zu müssen. Im Rahmen unserer Beratungen haben wir immer wieder darauf hingewiesen, dass es notwendig ist, die Aufgaben dieser Stelle gesetzlich zu verankern, um Rechtssicherheit für die Betroffenen zu schaffen.

Eine solche gesetzliche Grundlage für die Tätigkeit der unabhängigen Beschwerdestelle ist nunmehr geschaffen worden.[155] Die für einen Übergangszeitraum mit unserer Unterstützung entwickelte Lösung, die Tätigkeit der Beschwerdestelle auf der Grundlage von Einwilligungen zu legitimieren, konnte damit abgelöst werden. Wir haben diesen Prozess intensiv begleitet. Dabei haben wir SenIAS dahingehend sensibilisiert, dass im Bereich der Unterbringung wohnungsloser Menschen unterschiedliche Bundes- und Landesgesetze berührt sind. Zu nennen sind z. B. das Asylgesetz (AsylG), das Asylbewerberleistungsgesetz (AsylbLG) oder das Allgemeine Sicherheits- und Ordnungsgesetz Berlin (ASOG Bln).

Den Ausführungen im Bericht zu datenschutzrechtlichen Aspekten im Zusammenhang mit der Errichtung der Berliner unabhängigen Beschwerdestelle (BuBS) und dem einschlägigen Gesetzgebungsverfahren mit dem Ziel, die BuBS im Landesrecht zu verankern, kann vollumfänglich zugestimmt werden.

Da sich insoweit auch die Verarbeitung personenbezogener Daten nach den jeweils wahrgenommenen gesetzlichen Aufgaben bemisst, war es wichtig, hiervon die Aufgaben der Beschwerdestelle abzugrenzen. Dies ist mit der neuen gesetzlichen Regelung erfolgt. Gleichzeitig wird dort klargestellt, dass eine Verarbeitung personenbezogener Daten der geflüchteten Menschen durch die unabhängige Beschwerdestelle immer eine schriftliche Einwilligung der Beschwerdeführer:innen voraussetzt.[156]

Die frühzeitige Beteiligung der Berliner Beauftragten für Datenschutz und Informationsfreiheit sowohl bei den vorbereitenden Maßnahmen zur Errichtung der BuBS als auch bei der Erarbeitung einer Rechtsgrundlage war ein zentrales Anliegen der Senatsverwaltung für Integration, Arbeit und Soziales, um die ausgewiesene datenschutzrechtliche Expertise dieser Behörde bestmöglich zu nutzen und die Vereinbarkeit mit dem innerstaatlichen und europäischen Datenschutzrecht zu gewährleisten. Die bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit mit diesem Vorhaben betrauten Mitarbeitenden haben die Senatsverwaltung für Integration, Arbeit und Soziales während dieser Prozesse kontinuierlich mit Anregungen und vertiefenden Informationen unterstützt und somit wesentlich zum Erfolg der BuBS beigetragen.

Wir begrüßen es, dass SenIAS unseren Vorschlag aufgegriffen und die Aufgaben der unabhängigen Beschwerdestelle nun gesetzlich definiert hat. Mit der unabhängigen Beschwerdestelle kann ein wichtiger Beitrag geleistet werden, damit geflüchtete Menschen niederschwellig Missstände im Zusammenhang mit ihrer Unterbringung geltend machen

Die Senatsverwaltung für Integration, Arbeit und Soziales teilt vorbehaltlos die Notwendigkeit, den Schutz personenbezogener Daten bei der Bearbeitung von Beschwerdevorgängen durch die BuBS konsequent zu wahren. Daher werden insbesondere auch etwaige Anpassungen im Ergebnis der bisher gewonnenen Praxiserfahrungen, etwa

[155] Unterbringungsbeschwerdegesetz (UBeschwG)
[156] § 2 Satz 1 UBeschwG

können. Gerade bei Projekten wie diesen ist allerdings ein besonderes Augenmerk auf den Schutz der personenbezogenen Daten der Menschen zu richten. Verletzungen der Persönlichkeitsrechte wären hier mit einem besonders schweren Vertrauensverlust verbunden. Wir gehen davon aus, dass die besonderen Anforderungen des Datenschutzes bei der Beschwerdebearbeitung gewährleistet werden.

hinsichtlich der Gestaltung von Vordrucken, weiterhin mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit abgestimmt und somit die konstruktive Zusammenarbeit mit dieser Dienststelle fortgeführt.

7.2 Unterbringung Wohnungsloser „per Knopfdruck“

Mit dem ambitionierten Projekt „Gesamtstädtische Steuerung der Unterbringung“ (GStU), über das wir im vergangenen Jahr bereits berichtet haben,[157] plant SenIAS, die bedarfsgerechte Zuweisung von Unterbringungsplätzen für Wohnungslose bezirksübergreifend mithilfe eines zentralen IT-Verfahrens vorzunehmen. Dabei soll gleichzeitig die Kapazitätsplanung und Belegungssteuerung „per Knopfdruck“ unterstützt werden. Da hier auch sensitive Daten, z. B. Daten über die Gesundheit oder die sexuelle Orientierung, von ganz unterschiedlichen Personengruppen wie etwa Asylbewerber:innen oder Wohnungslosen zentral verarbeitet werden sollen, ist es besonders wichtig, die datenschutzrechtlichen Anforderungen von vornherein zu betrachten.

Die im Jahresbericht zu datenschutzrechtlichen Aspekten im Zusammenhang mit der Pilotierung des IT-Fachverfahrens zur Umsetzung der „Gesamtstädtischen Steuerung der Unterbringung“ (GStU) getätigten Aussagen sind aus der Sicht der Senatsverwaltung für Integration, Arbeit und Soziales zutreffend dargestellt.

Als zentraler Baustein des im September von SenIAS vorgestellten „Berliner Masterplans“[158] dient das GStU-Projekt auch dem Ziel, die Wohnungslosigkeit in Berlin bis 2030 insgesamt zu überwinden.

Die frühzeitige Beteiligung der Berliner Beauftragten für Datenschutz und Informationsfreiheit bei den vorbereitenden Maßnahmen zur Pilotierung des Fachverfahrens war ein zentrales Anliegen der Senatsverwaltung für Integration, Arbeit und Soziales, um die ausgewiesene datenschutzrechtliche Expertise dieser Behörde bestmöglich zu nutzen und die Vereinbarkeit mit dem innerstaatlichen und europäischen Datenschutzrecht zu gewährleisten. Die bei der Berliner Beauftragten für Datenschutz und Informationsfreiheit mit diesem Vorhaben betrauten Dienstkräfte haben das GStU-Projektteam während dieser Prozesse kontinuierlich mit Anregungen und vertiefenden Informationen unterstützt und somit wesentlich zur Entwicklung des Fachverfahrens beigetragen.

SenIAS hat zum Ende des Jahres die Pilotphase der GStU gestartet, deren Vorbereitung wir in intensiven Beratungen unterstützt haben. Im Rahmen des Pilotprojekts konnte ein datenschutzrechtlicher Rahmen für die Nutzung des IT-Fachverfahrens für die Vergabe von Unterbringungsplätzen in vier bezirklichen Unterkünften und einer Aufnahmeeinrichtung

Die Senatsverwaltung für Integration, Arbeit und Soziales teilt vorbehaltlos die Notwendigkeit, den Schutz personenbezogener Daten bei der Unterbringung geflüchteter sowie wohnungsloser Personen konsequent zu wahren. Die Anregungen und Hinweise der Berliner Beauftragten für Datenschutz und Informationsfreiheit wurden bei der

[157] JB 2020, 6.2

[158] Siehe „Berliner Masterplan zur Überwindung von Wohnungs- und Obdachlosigkeit bis zum Jahr 2030“, unter: https://www.berlin.de/sen/ias/_assets/aktuelles/2021_09-02-masterplan2030.pdf

des Landesamtes für Flüchtlingsangelegenheiten (LAF) entwickelt werden. Angesichts der unterschiedlichen gesetzlichen Aufgaben, die von den beteiligten Behörden nach unterschiedlichen Rechtsvorschriften wahrgenommen werden, war es wichtig, die jeweilige Verantwortlichkeit für die Datenverarbeitung und die jeweiligen gesetzlichen Befugnisse festzulegen. Für die Nutzung des IT-Fachverfahrens war es notwendig, die Zugriffsrechte zu definieren. Schließlich haben wir darauf hingewirkt, dass die notwendigen Auftragsverarbeitungsvereinbarungen zwischen den beteiligten Akteuren abgeschlossen wurden.

SenIAS plant für die Zukunft die Weiterentwicklung des Projektes durch Schaffung einer „Zentralen Serviceeinheit GStU“. Vertrags- und Unterkunftsmanagement sowie Abrechnung und Qualitätssicherung sollen dort zentral verortet werden. Da sich die Unterbringung der verschiedenen Personengruppen jedoch nach unterschiedlichen gesetzlichen Regelungen richtet, die teilweise im Bundes- und teilweise im Landesrecht verortet sind, müssen die für die Verarbeitung personenbezogener Daten geltenden Vorschriften genau geprüft werden. Ob sich die Einrichtung einer solchen zentralen Stelle angesichts der unterschiedlichen gesetzlichen Rahmenbedingungen rechtlich abbilden lässt, bedarf genauer Betrachtung.

Überarbeitung der notwendigen Dokumente, wie etwa der Datenschutzfolgeabschätzung und der Vereinbarungen zur Auftragsverarbeitung vollumfänglich umgesetzt. Die gemeinsame Überprüfung der Erforderlichkeit der Verarbeitung von Daten bestimmter Datenkategorien führte dazu, dass insgesamt weniger Daten der untergebrachten Personen mittels Fachverfahren verarbeitet werden müssen. Dies führte zu einer wesentlichen Stärkung der informationellen Grundrechte der betroffenen Personen.

Die Überwindung der Wohnungslosigkeit ist eine wichtige sozialstaatliche Herausforderung. Dabei darf jedoch nicht außer Acht gelassen werden, dass die Aufgabe der Unterbringung der verschiedenen Personengruppen in unterschiedlichen Gesetzen verortet ist. Dies bedeutet, dass sich auch die datenschutzrechtlichen Anforderungen voneinander unterscheiden. Für eine Weiterentwicklung des Projektes GStU über den Pilotbetrieb hinaus sind in einem ersten Schritt die rechtlichen Rahmenbedingungen auszuloten. Wir werden uns weiterhin beratend an dem Projekt beteiligen.

Die im Jahresbericht dargestellte Problematik mit der Anwendung bestehender Rechtsgrundlagen zur Datenverarbeitung nimmt die Senatsverwaltung für Integration, Arbeit und Soziales zum Anlass, bei der nun anstehenden gesetzlichen Umsetzung der GStU entsprechende landesrechtliche Ermächtigungstatbestände zur Datenverarbeitung im Kontext der Unterbringung zu schaffen, um allen untergebrachten Personen, unabhängig vom Rechtsstatus, die gleichen Schutzstandards zu gewährleisten. Damit diese Regelungen möglichst grundrechtsschonend ausgestaltet werden, wird die Senatsverwaltung für Integration, Arbeit und Soziales im Vorfeld des Gesetzgebungsverfahrens den weiteren Austausch mit der Berliner Beauftragten für Datenschutz und Informationsfreiheit suchen und die konstruktive Zusammenarbeit mit ihr fortführen.

8 Beschäftigtendatenschutz

8.1 Eine Liste mit Informationen über alle Beschäftigten in der Probezeit

Ein Unternehmen hat eine größere Zahl an Servicekräften eingestellt. Kurz vor dem Ende der Probezeit hat die Geschäftsführung die Vorgesetzte der Servicekräfte angewiesen, eine Liste mit Informationen zu den Beschäftigten zu erstellen, um intern begründen zu können, welche Beschäftigten in der Probezeit gekündigt werden sollen. Einige Informationen auf der Liste standen in keinem zulässigen Zusammenhang mit deren Zweck.

In der Liste wurden neben einigen Stammdaten knappe Einschätzungen über die Beschäftigten und teilweise Empfehlungen für Kündigungen in der Probezeit festgehalten. Gut ein Drittel der Beschäftigten wurde als „kritisch“ oder „sehr kritisch“ bewertet. Für knapp ein Fünftel der Beschäftigten wurde die Empfehlung ausgesprochen, sie in der Probezeit zu kündigen. In einer mit „Begründung“ betitelten Tabellenspalte wurden teilweise Arbeitsmotivation, Krankentage, soziale oder politische Einstellungen, mögliches Interesse an einem – noch nicht bestehenden – Betriebsrat und häufig außerbetriebliche Gründe, die einer flexiblen Einteilung in die Arbeitsschichten entgegenstehen würden, aufgelistet. Solche Gründe konnten andere Tätigkeiten, ein Studium oder ein Hobby sein. Bei zwei Personen wurde auch notiert, dass regelmäßige Psychotherapietermine der gewünschten Flexibilität entgegenstehen würden.

Das Unternehmen hat auf unsere Anfrage hin erklärt, dass die Liste dem Zweck dienen sollte, Leistungen von Beschäftigten objektivierbar zu beurteilen. Auf dieser Grundlage sollte entschieden werden, ob das Arbeitsverhältnis fortgeführt wird. Die Liste wurde von der Vorgesetzten der Servicekräfte per E-Mail an die Geschäftsführung und die Personalabteilung versandt.
Unternehmen dürfen intern Überlegungen anstellen, ob sie Beschäftigte innerhalb der Probezeit kündigen. Da hier Entscheidungen zu mehreren Beschäftigten getroffen werden sollten, spricht nichts gegen eine tabellarische Aufstellung.

Teilweise äußerst problematisch war jedoch der Inhalt der Liste, denn es dürfen natürlich nur solche personenbezogenen Daten herangezogen werden, die keinem Verarbeitungsverbot unterliegen. Die Informationen müssen in einem zulässigen Zusammenhang mit dem Arbeitsverhältnis stehen.

So wurde in der Liste häufig angeführt, dass die Personen für die Dienstplanung nicht flexibel genug seien, ergänzt mit der Begründung, weshalb sie zu bestimmten Zeiten nicht arbeiten können. Dabei muss es einem bzw. einer Arbeitgeber:in für seine bzw. ihre Entscheidung über die Fortführung eines Arbeitsverhältnisses regelmäßig genügen, dass die beschäftigte Person zu bestimmten Zeiten nicht verfügbar ist. Auf dieser Grundlage kann entschieden werden, ob die angegebene verfügbare Zeit ausreicht, um das Arbeitsverhältnis fortzusetzen. Dies gilt in gesteigertem Maße für Informationen, wie „besucht eine Psychotherapie“. Hierbei handelt es sich um ein Gesundheitsdatum, das einem Verarbeitungsverbot unterliegt und für dessen Verarbeitung der Beschäftigtendatenschutz hier keine Ausnahme vorsieht.[159]

Bei insgesamt fünf Beschäftigten war ein Interesse am Betriebsrat oder eine andere Form von Einsatz für kollektive Beschäftigteninteressen notiert. Diese Informationen stehen in keinerlei Zusammenhang mit dem von dem Unternehmen vorgeblich verfolgten Zweck, eine Leistungsbeurteilung der Beschäftigten durchzuführen. Denn Interesse an einem Betriebsrat mag mancher bzw. manchem Arbeitgeber:in ein Dorn im Auge sein, eine Aussage zu der Leistung der Beschäftigten ist diese Information nicht. Auf Nachfrage hat das Unternehmen mitgeteilt, dass diese Anmerkungen auch gemacht wurden, um die Gründung eines Betriebsrates zu unterstützen. Nachweise, die diese Behauptung stützen, konnte das Unternehmen nicht erbringen. Ganz im Gegenteil: Vier der betroffenen Beschäftigten wurden in der Probezeit gekündigt, mit der fünften Person wurde ein Aufhebungsvertrag geschlossen.

Viele der in der Liste aufgeführten Informationen haben die Beschäftigten ihrer Vorgesetzten selbst mitgeteilt. Etwa, wenn sie in E-Mails um eine bestimmte Einteilung in den Dienstplan gebeten und dies begründet haben. Insofern ließ sich eine zunächst geäußerte Vermutung, dass Beschäftigte ausspioniert worden sind, nicht nachweisen. Allerdings dürfen auch auf diesem Wege mitgeteilte Informationen von Arbeitgeber:innen nicht zu den genannten Zwecken weiterverarbeitet werden.

Da eine leitende Angestellte auf Anweisung der Geschäftsführung die unzulässige Datenverarbeitung durchgeführt hat und bei der Datenverarbeitung

[159] Siehe Art. 9 Abs. 1 DS-GVO, § 26 Abs. 3 BDSG

schwerwiegende Folgen in Form von Kündigungen für die Betroffenen drohten, haben wir das Verfahren an unsere Sanktionsstelle zur Prüfung abgegeben, ob ein Bußgeldverfahren eingeleitet werden soll.

Arbeitgebende dürfen Überlegungen anstellen, inwiefern Beschäftigte weiterbeschäftigt werden sollen und insofern auch personenbezogene Daten verarbeiten. Die so verarbeiteten Daten müssen aber für diesen Zweck überhaupt geeignet sein, was heißt, dass sie in einem unmittelbaren Zusammenhang mit dem Arbeitsverhältnis stehen müssen.

8.2 Müssen juristische Referendar:innen dem Kammergericht ihren Gesundheitszustand mitteilen?

Bevor juristische Referendar:innen von dem Kammergericht in den sog. Vorbereitungsdienst aufgenommen werden, müssen sie eine Erklärung zu ihrem Gesundheitszustand abgeben. In dieser sollten sie angeben, ob sie an einer physischen oder -psychischen Erkrankung leiden, wegen der sie sich in Behandlung befinden oder die eine Behandlung erfordert.

Die gesetzliche Grundlage, um grds. eine Erklärung zum Gesundheitszustand einzuholen, befindet sich im Berliner Juristenausbildungsgesetz (JAG). Dort heißt es, dass die Aufnahme in den Vorbereitungsdienst versagt werden kann, wenn die Bewerberin oder der Bewerber an einer Krankheit leidet, die die ordnungsgemäße Ausbildung ernstlich beeinträchtigen könnte oder die Gesundheit anderer gefährdet.[160]

Bewerber:innen sind in den meisten Fällen nicht verpflichtet, qualifizierte Informationen über ihren Gesundheitszustand preiszugeben. Eine Ausnahme stellt es dar, wenn Bewerber:innen wissen, dass sie aufgrund ihres Gesundheitszustands der angestrebten Tätigkeit nicht nachkommen können. In diesem Fall besteht sogar eine Offenbarungspflicht ggü. möglichen Arbeitgeber:innen. Das Verschweigen kann sonst als arglistige Täuschung gewertet werden, aufgrund derer das Arbeitsverhältnis vonseiten der Arbeitgebenden aufgehoben werden kann.

Wegen dieser eindeutigen Zielrichtung der gesetzlichen Vorgaben haben wir das Kammergericht gebeten, die Abfrage des Gesundheitszustands an den

[160] § 10a Abs. 2 Nr. 2 JAG (bis zum 24. September 2021 in § 20 Abs. 2 Nr. 1 Berliner Juristenausbildungsordnung – JAO – geregelt)

Gesetzeswortlaut anzupassen, was das Kammergericht Ende letzten Jahres getan hat. Künftige Bewerber:innen müssen nun nur noch ggf. angeben, dass sie an einer Erkrankung leiden, die geeignet ist, die ordnungsgemäße Ausbildung ernstlich zu beeinträchtigen oder die geeignet ist, die Gesundheit anderer zu gefährden. Angaben zu der Krankheit selbst sind freiwillig. Diese freiwillige Zusatzangabe ermöglicht es dem Kammergericht, ggf. selbst eine abweichende Bewertung vorzunehmen und einer Person trotz dieser Erklärung Zugang zu der Ausbildung zu gewähren.

Künftige Arbeitgeber:innen und Ausbildungsstellen dürfen auch im öffentlichen Dienst nur Gesundheitsdaten erheben, zu deren Erhebung sie gesetzlich befugt sind. Hierzu zählen nur solche Informationen, die einen unmittelbaren Einfluss auf das Arbeitsverhältnis haben.

8.3 Freier Zugriff auf Daten von Bewerber:innen

Ende August erhielten wir einen Hinweis, dass durch eine Sicherheitslücke in einer Software für Stipendienportale der Zugriff auf eine große Menge personenbezogener Daten verschiedener Studienstiftungen möglich sei. Die unsichere Software wurde hauptsächlich zum Bereitstellen von Stipendienbewerbungsportalen genutzt, wo eine große Menge von zum Teil höchstpersönlichen Daten gespeichert werden. Aufgrund der jeweiligen Ausrichtung der betroffenen Studienstiftungen waren zudem besondere Kategorien personenbezogener Daten, wie Religionszugehörigkeit oder Daten zur politischen Überzeugung und Weltanschauung betroffen.

Durch eine E-Mail wurden wir über kritische Schwachstellen in einer Software informiert, welche zur Bereitstellung von unterschiedlichen Portallösungen verschiedener Studienstiftungen dient. Die Software wird von einem Berliner Unternehmen entwickelt und vertrieben. Die E-Mail wurde außer an uns auch an das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie an den Softwarehersteller selbst versandt und enthielt einen ausführlichen Bericht über mehrere verschiedene Schwachstellen in der Portalsoftware.

Durch die Ausnutzung der Schwachstellen wäre es Angreifer:innen möglich gewesen, sich ein Nutzungskonto anzulegen, die Datenbank abzufragen, hochgeladene Dokumente herunterzuladen und ein Nutzungskonto mit Privilegien zur Administration zu versehen.

Betroffen waren die Bewerbungsportale von vier verschiedenen Studienstiftungen mit unterschiedlichen Ausrichtungen, sowie im Falle einer Stiftung ein Portal, das Stipendiat:innen zum Austausch dient. Bewerber:innen für Stipendien bei den Stiftungen konnten ihre Unterlagen auf den Portalen im Zuge ihrer Bewerbung hochladen und so den Stiftungen zur Verfügung stellen. Insgesamt waren ca. 350.000 Dokumente zugänglich, die höchstpersönliche Daten, wie Ausweiskopien, Immatrikulationsbescheinigungen, Empfehlungs- und Motivationsschreiben umfassten.

Aufgrund der jeweiligen Ausrichtungen und Schwerpunkte der betroffenen Studienstiftungen umfassten diese Daten auch sensitive personenbezogene Angaben, wie z. B. zur Religionszugehörigkeit und zur Nähe zu politischen Parteien. Aufgrund des hohen Risikos für die Rechte und Freiheiten der betroffenen Personen ist bei solchen Daten regelmäßig von einem hohen Schutzbedarf auszugehen und sind entsprechende Maßnahmen zu ergreifen, die geeignet sind, diese Risiken wirksam zu mindern. Dies wurde in diesem Fall aber offensichtlich sträflich versäumt.

Es war uns leicht möglich, die dokumentierten Schwachstellen nachzuvollziehen. Der Softwarehersteller reagierte schnell auf die Meldung und hat Änderungen an der Software vorgenommen, die eine Ausnutzung der Schwachstellen verhindern sollten. Nach einer weiteren Meldung durch Sicherheitsforscher:innen, die auf verbliebene Schwachstellen hinwies, wurden auch diese geschlossen.

Ursache für das Problem war die falsche Nutzung eines Softwareframeworks[161], welche dazu führte, dass die Berechtigungsprüfung nicht wie vorgesehen funktionierte und dass mehr Informationen als notwendig an die Nutzer:innen der Internetseiten ausgeliefert wurden.

Die Herstellerfirma teilte uns mit, dass die gefundenen Schwachstellen als Anlass genommen wurden, eine externe Firma mit einer Sicherheitsüberprüfung des Produkts zu beauftragen.

Anbieter:innen von Serviceportalen müssen sicherstellen, dass die dort gespeicherten Daten gegen unberechtigte Zugriffe geschützt sind. Handelt es

[161] Ein Softwareframework ist eine Art Baukasten, der Softwareentwickler:innen unterschiedliche wiederverwendbare Basisfunktionen zur Verfügung stellt, die diese dann bei der Erstellung komplexerer Programme nutzen können.

sich um besonders sensitive Daten in großem Umfang, sollten die Anbieter:innen, aber auch die Verantwortlichen, die die Software in Anspruch nehmen, besondere Sorgfalt walten lassen und aktiv prüfen, ob die eingesetzten Systeme und deren Konfiguration die notwendigen Sicherheitseigenschaften aufweisen.

9 Wohnen, Stadtentwicklung, Daseinsvorsorge und Umwelt

9.1 Online-Makler veröffentlicht Mieter:innendaten im Internet

Ein auf die Online-Vermarktung von Wohnraum ausgerichtetes Unternehmen bietet auf seiner Internetseite die Möglichkeit, Unterlagen zu dem geplanten Verkauf einer Immobilie abzulegen. Für die Anonymisierung der dort abgelegten Dokumente wurde durch den Online-Makler jedoch nicht hinreichend Sorge getragen.

Das Unternehmen bietet mehrere Dienstleistungen in Kombination an. Neben der Bewertung von Immobilien durch eigene oder mit dem Unternehmen kooperierende Makler:innen gehört zu den Leistungen auch die Erstellung und Betreuung von Verkaufsanzeigen sowie die Beschaffung und Bereitstellung von Unterlagen, die für das Immobiliengeschäft benötigt werden. Diese Unterlagen umfassen regelmäßig Dokumente mit sehr persönlichen Daten, da es um Vermögenswerte, Verbindlichkeiten und oft auch den Wohnraum geht. Außerdem sind Daten von Dritten betroffen, wenn die in Rede stehende Immobilie vermietet ist. Auch Unterlagen ganzer Wohnungseigentumsgemeinschaften werden mitunter im Online-Angebot des Unternehmens abgelegt.

Uns erreichten in den vergangenen Jahren mehrere Beschwerden darüber, dass beim Bereitstellen der Dokumente durch das betroffene Unternehmen die erforderliche Anonymisierung der Unterlagen nicht hinreichend vorgenommen werde. Zudem meldete das Unternehmen selbst regelmäßig Datenlecks, bei denen es zu unberechtigten Abrufen persönlicher Unterlagen gekommen war.

Mit den Beschwerden konfrontiert, verwies das Unternehmen auf ein für die Schwärzung der Unterlagen eingesetztes Subunternehmen. Es sei trotzdem in Einzelfällen nicht ausgeschlossen, dass nicht ausreichend geschwärzte Dokumente veröffentlicht würden. In Bezug auf die gemeldeten Datenlecks werde eine „Task Force“ eingesetzt. Nachdem das

nächste Datenleck gemeldet wurde, erklärte das Unternehmen, die Arbeit der „Task Force“ werde intensiviert. Anlässlich der Mitteilung über ein weiteres, neues Datenleck kündigte das Unternehmen ein Stufenprinzip an, sodass nunmehr nur noch qualifizierte Kaufinteressent:innen Zugang zu den Unterlagen erhielten.

Aus den unterschiedlichen Beschwerden und unternehmenseigenen Meldungen wird ersichtlich, dass es dem Unternehmen an Willen oder Fähigkeit zum datenschutzkonformen Umgang mit den personenbezogenen Daten Dritter mangelt. Es hätte das im eigenen Auftrag handelnde Subunternehmen besser kontrollieren oder die Schwärzungen der personenbezogenen Daten in seinem Online-Angebot selbst überprüfen müssen. Nachdem bereits im letzten Jahr eine Verwarnung gegen das Unternehmen ausgesprochen wurde, läuft nun ein Bußgeldverfahren unserer Sanktionsstelle wegen der benannten Verstöße gegen die Rechte der von einer Veröffentlichung ihrer Unterlagen betroffenen Personen.

Unterlagen, die zur Abwicklung von Verträgen bei Wohnraummiete und Immobilienkauf erforderlich sind, können auch digital durch sichere Online-Plattformen ausgetauscht werden. Nicht erforderliche personenbezogene Daten müssen dann allerdings geschwärzt und die ggf. für diese Tätigkeit beauftragten Unternehmen durch die Portalbetreiber:innen hinreichend kontrolliert werden.

9.2 Datenverarbeitung durch Rauchmelder?

Seit dem 1. Januar 2021 ist der Einbau von Rauchwarnmeldern in privatem Wohnraum gesetzlich verpflichtend. Die hierfür eingesetzten Geräte sind mittlerweile so ausgestaltet, dass sie per Funk auf ihre Funktionsfähigkeit überprüft und gewartet werden können.

Uns erreichten bereits in den Vorjahren immer wieder Beratungsanfragen von Bürger:innen hinsichtlich einer möglichen Überwachung mittels neu einzubauender Rauchwarnmeldegeräte.
Zwar müssen Rauchmelder für die Erfüllung ihres Zwecks über Sensoren verfügen, die bspw. Abstände messen können, um ein Verdecken der Warnmelder durch Möbel etc. zu erkennen. Diese Sensoren sind jedoch nicht dazu geeignet, die Anwesenheit von Personen für Bewegungsprofile zu erfassen oder Tonaufzeichnungen zu machen. Zudem wären die in den Geräten verbauten wenig leistungsstarken Funksender auch nicht in der Lage, größere Datenmengen nach außen zu übertragen.

Ganz ohne Personenbezug kommt ein Rauchwarnmelder jedoch nicht aus. Jedes Gerät muss einer bestimmten Wohneinheit zugeordnet werden können, wenn die Geräte per Funk Auskunft über ihre Funktionstüchtigkeit geben. Dabei werden meist die Gerätenummer sowie die entsprechenden Wartungsprotokolle nach außen gesendet. Die verantwortliche Stelle muss sodann zuordnen können, wo eine ggf. gemeldete Funktionsstörung zu beheben ist. Anhaltspunkte für eine unberechtigte Verarbeitung dieser Daten konnten wir allerdings nicht feststellen.

Auch bei Einbau und Betrieb von Rauchwarnmeldern spielt der Schutz von personenbezogenen Daten eine Rolle, wenn Gerätenummer und Funktionsfähigkeit bei Wartungsarbeiten an verantwortliche Stellen übermittelt werden. Daten über Anwesenheit und Verhalten von Personen innerhalb des Sensorbereichs der Geräte werden nach unseren Erkenntnissen indes nicht erhoben und weiterverarbeitet.

9.3 Zweckentfremdungsverbot-Gesetz

Im September hat das Abgeordnetenhaus eine Änderung des Zweckentfremdungsverbot-Gesetzes (ZwVbG) beschlossen. Das ZwVbG regelt u. a. die Vermietung von Ferienwohnungen in Berlin und die Folgen ungenehmigter Vermietung. Durch die Novelle sollen die Behörden die Möglichkeit erhalten, bei der Bekämpfung illegaler Vermietung von Ferienwohnungen im Verdachtsfall bestimmte Informationen direkt bei den Online-Vermittlungsplattformen abzufragen, um bspw. Ordnungswidrigkeiten ahnden zu können.

Eine Datenabfrage bei digitalen Vermittlungsplattformen zu Anbietenden von bestimmten Wohnungen oder nach abgeschlossenen Verträgen zu einer bestimmten Wohnung, wird dabei als Bestandsdatenabfrage bezeichnet. Die Bestandsdaten sind von den Nutzungsdaten zu unterscheiden: Nutzungsdaten sind Daten, die z. B. für den Verbindungsaufbau zu einer Webseite nötig sind, wie IP-Adressen.

Nach der sog. „Doppeltür-Rechtsprechung“ des Bundesverfassungsgerichts (BVerfG) brauchen alle Datenabfragen zwei Rechtsgrundlagen: Einerseits muss die anfragende Behörde berechtigt sein, die Daten zu erheben. Andererseits müssen aber auch die Unternehmen berechtigt sein, die angefragten Daten herauszugeben.

Das ZwVbG kann insoweit nur die Rechtsgrundlage für die Behörde schaffen, die Daten bei Vermitt-

lungsplattformen abzufragen. Die Rechtsgrundlage für die Datenherausgabe durch die Betreiber:innen dieser Plattformen regelt das Bundesrecht. Deshalb nimmt das ZwVbG Bezug auf das bundesrechtliche Telemediengesetz (TMG).

Darin lag gleichzeitig die Schwierigkeit des Gesetzgebungsprozesses: Die einschlägigen Vorschriften im TMG waren zuletzt im April geändert worden, weil das BVerfG im letzten Jahr festgestellt hatte, dass die Regelungen zur Bestandsdatenauskunft im TMG verfassungswidrig waren.[162] In der Entscheidung des BVerfG ging es insbesondere auch um die Voraussetzungen für Bestandsdatenauskünfte bei der Verfolgung von Ordnungswidrigkeiten. Das Urteil betraf also die Art von Datenabfragen, die das Ziel der Berliner Gesetzesnovelle waren. Das BVerfG hat mit Blick auf die bundesrechtlichen Regelungen ausdrücklich verlangt, es müsse sich „um – auch im Einzelfall – besonders gewichtige Ordnungswidrigkeiten handeln, die der Gesetzgeber zudem ausdrücklich benennen muss“. Das BVerfG hatte in dem Urteil auch die Relevanz der Nutzungsdaten für das Persönlichkeitsrecht erneut bestätigt.

Es ist weder Aufgabe unserer Behörde noch der Landesgesetzgebung, die Änderungen im TMG verfassungsrechtlich zu überprüfen. Dennoch fällt ins Auge, dass bei der Herausgabe von Nutzungsdaten in der aktuellen Fassung des TMG keine Begrenzung auf besonders gewichtige Ordnungswidrigkeiten vorgenommen wurde. Deshalb hat unsere Behörde in ihrer Stellungnahme zur Novelle des ZwVbG angemerkt, dass die Verfassungsgemäßheit der bundesgesetzlichen Rechtsgrundlage im Fall der Nutzungsdaten leider erneut zweifelhaft ist.

Durch eine im September beschlossene Änderung des ZwVbG wurde die Möglichkeit geschaffen, dass Behörden im Verdachtsfall bestimmte Daten direkt bei Unternehmen abfragen können, die Plattformen zur Ferienwohnungsvermittlung betreiben. Im Ergebnis bestehen Zweifel, ob die neuen bundesrechtlichen Regelungen, insbesondere in Bezug auf die (technischen) Nutzungsdaten, den Vorgaben des BVerfG entsprechen. Auf diesen Umstand hat das Land Berlin keinen Einfluss, die Landesbehörden sollten dies aber berücksichtigen, wenn sie im Einzelfall entscheiden, auch (technische) Nutzungsdaten zu erheben.

[162] BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13

9.4 Datenschutzrechtliche Folgen des geplatzten Mietendeckels

Im letzten Jahr hatte das Abgeordnetenhaus den sog. Mietendeckel beschlossen. Im April dieses Jahres veröffentlichte nun das BVerfG einen Beschluss[163], in dem dieser Mietendeckel für nichtig erklärt wurde, da es dem Land Berlin an der erforderlichen Gesetzgebungskompetenz fehlte.

Dieser Beschluss hatte auch datenschutzrechtliche Konsequenzen, denn das Gesetz zur Regelung des Mietendeckels enthielt auch eine Rechtsgrundlage für die diesbezügliche Datenverarbeitung, die nun wegfiel. Die Senatsverwaltung für Stadtentwicklung und Wohnen (SenSW), als eine der wesentlichen Verantwortlichen in diesem Bereich, wandte sich an unsere Behörde. Sie bat um Unterstützung bei der Abwicklung des gescheiterten Gesetzes. Die angefallenen Daten waren grds. umgehend zu löschen. Gleichzeitig stellte sich die Frage, welche Unterlagen die SenSW für künftige Gerichtsverfahren noch benötigt und ob insoweit Rechtsgrundlagen für eine weitere Aufbewahrung gegeben sind.

Für uns hatte die Erstellung eines Gesamtlöschkonzepts für alle aufgrund des Mietendeckels erhobenen Daten Priorität ggü. der sofortigen Umsetzung einzelner Löschverlangen. Dennoch war die Maximalfrist von drei Monaten für die Umsetzung von Betroffenenrechten einzuhalten. Der SenSW gelang es, unter Pandemiebedingungen und mit behördenübergreifender Abstimmung, die Überprüfung weiterer Aufbewahrungsgründe für alle Unterlagen bis Ende Juli zum Abschluss zu bringen. Im Ergebnis fanden sich über die Landeshaushaltsordnung (LHO) hinaus keine Gründe für eine weitere Aufbewahrung der Akten in der zuständigen Senatsverwaltung. Also wurden die Akten, wie im Archivgesetz des Landes Berlin (ArchGB) vorgesehen, dem Landesarchiv angeboten. Anfang September erteilte das Landesarchiv der SenSW die Löschfreigabe. Daraufhin wurden alle aufgrund des Mietendeckels erhobenen Daten, die dem Landesarchiv angeboten worden waren, bei der SenSW gelöscht.

Das Landesarchiv prüft nun die Archivwürdigkeit der Vorgänge in eigener Zuständigkeit. Diese Prüfung dauerte bei Redaktionsschluss noch an. Nach Abschluss der Archivwürdigkeitsprüfung werden die nicht archivwürdigen Unterlagen beim Landesarchiv ebenfalls gelöscht.

[163] BVerfG, Beschluss vom 25. März 2021 – 2 BvF 1/20, 2 BvL 5/20, 2 BvL 4/20

9.5 Funkbasierte Heizkostenmessgeräte

Zum 1. Januar 2022 treten neue Regelungen für die Erfassung von Heizkosten in Kraft,[164] die auch die Übertragung personenbezogener Daten betreffen. Die dann für die Neuinstallation von Geräten verpflichtende elektronische Erfassung von Heizkosten ersetzt den jährlichen Besuch eines Abrechnungsunternehmens, weil die Verbrauchsdaten von z. B. Heizkörpern elektronisch nach außen übertragen werden. Dabei können die Verbrauchsdaten jedoch mitunter sehr detailliert sein und daher eine Gefahr für den Datenschutz bestehen.

Bei der funkgesteuerten Verbrauchsdatenerfassung werden die jeweiligen Verbrauchswerte mittels elektronisch betriebener Geräte erfasst und per Funk oder sonstiger Netzwerktechnik zu den die Kosten abrechnenden Stellen übertragen. Dies geschieht in den meisten Fällen über eine Station – bspw. im Hausflur oder Keller –, die die Daten der einzelnen Verbrauchszähler im Haus einsammelt und zunächst zwischenspeichert. Die Werte in dieser Sammelstation werden dann in bestimmten Zeitintervallen per Funk durch Mitarbeitende des jeweiligen Abrechnungsunternehmens elektronisch abgefragt.

Die Einführung dieser digitalen Form der Verbrauchsabrechnung hat für Verbraucher:innen viele Vorteile in Sachen Transparenz. Abrechnungsunternehmen müssen etwa nach den neuen Regeln auch Vergleichswerte aus vorangegangenen Zeiträumen angeben und grds. auch monatlich Verbrauchsinformationen bereitstellen. So lässt sich der eigene Verbrauch besser analysieren, um bspw. klimaschonender heizen zu können.

Durch die detaillierte Erfassung der Verbrauchsdaten entstehen jedoch auch Risiken für die informationelle Selbstbestimmung betroffener Personen. Die elektronisch erfassten Werte können zum Teil Aufschluss geben über die Anzahl der Bewohner:innen einer Wohnung, deren Anwesenheit, deren Verbrauch und Nutzungsgewohnheiten.

Die Regeln der Datenschutz-Grundverordnung (DS-GVO) begegnen diesen Gefährdungen dadurch, dass nur diejenigen Daten erhoben werden dürfen, die zur Erstellung der gesetzlich geschuldeten Abrechnung erforderlich sind. Die Erhebung und Weiterverarbeitung von Daten, die über diesen Zweck hinausgehen, ist nur mit einer informierten und transparenten Einwilligung durch davon Betroffene zulässig. Dazu

[164] Siehe §§ 6 – 6b Verordnung über Heizkostenabrechnung (HeizkostenV)

müssen Geräte von vorneherein so eingestellt sein, dass nur die abrechnungsrelevanten Daten erhoben werden.

Bei der Umstellung auf funkbasierte Verbrauchserfassungen sollten betroffene Personen stets auf eine umfassende Information über die damit einhergehende Datenverarbeitung bestehen und nicht zögern, z. B. Auskunftsrechte ggü. Abrechnungsunternehmen geltend zu machen.

Funkbasierte Heizkostenabrechnungen bieten Vorteile in Bezug auf Transparenz und bergen gleichzeitig Gefahren für die Privatsphäre, wenn die Datenverarbeitung über abrechnungsrelevante Zwecke hinausgeht. Betroffene sollten ggü. verantwortlichen Stellen und Unternehmen auf volle Transparenz bestehen.

9.6 Streit unter Kleingärtner:innen — Gilt die DS-GVO?

Die DS-GVO ist auf die Verarbeitung von personenbezogenen Daten durch Privatpersonen im ausschließlich persönlichen oder familiären Bereich nicht anwendbar (sog. Haushaltsausnahme).[165] Mit dieser Haushaltsausnahme soll die freie Entfaltung der Persönlichkeit von Privatpersonen vor Regulierung geschützt werden. Typische persönliche oder familiäre Tätigkeiten werden i. d. R. in den Bereichen Freizeit, Sport oder Urlaub ausgeübt.

Im Privatleben, in Freundschaftsbeziehungen oder in der Familie kommt häufig die Frage auf, ob Fälle aus diesen Bereichen in den Anwendungsbereich der DS-GVO fallen. In einer von uns bearbeiteten Beschwerde herrschte in einem Kleingartenverein zwischen einer Pächterin einer Kleingartenparzelle und ihrer Nachbarin Streit. Die Beschwerdeführerin wendete sich dagegen, dass die Nachbarin ihr ein Schreiben an ihre Privatadresse und nicht an die Parzelle im Kleingartenverein geschickt hatte. Unsere Ermittlungen ergaben, dass die Nachbarin die Privatadresse der Beschwerdeführerin noch aus einer Zeit kannte, in der die Beteiligten befreundet waren. Die damalige Erhebung der Adressdaten erfolgte somit rein privat, d. h. ohne jeden Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit.[166] Für die sog. Haushaltsausnahme sprach auch, dass es sich bei dem besagten Schreiben um einen schriftlichen Austausch zwischen zwei Privatpersonen handelte, der sich ausschließlich auf deren Frei-

[165] Art. 2 Abs. 2 lit. c DS-GVO
[166] Siehe EG 18 DS-GVO

zeitaktivitäten im Rahmen der Nachbarschaft im Kleingartenverein bezog. Die Verarbeitung der personenbezogenen Daten fand demnach im Rahmen einer nachbarschaftlichen und ausschließlich privaten Auseinandersetzung statt. Die Beschwerdeführerin konnte ggü. der Nachbarin daher keine Betroffenenrechte nach der DS-GVO geltend machen.

Der Anwendungsbereich der DS-GVO ist nicht eröffnet, sofern sich um eine Datenverarbeitung einer Privatperson im Rahmen einer persönlichen oder familiären Tätigkeit handelt.

9.2 Herausgabe von Mitgliederlisten im Verein zur Geltendmachung von Minderheitenrechten

Ein Vereinsmitglied sowie der entsprechende Verein wandten sich jeweils mit der Beratungsanfrage an uns, ob die Mitgliederliste des Vereins an das Vereinsmitglied sowie zwei weitere Mitglieder zur Einberufung einer außerordentlichen Mitgliederversammlung herausgegeben werden könne. Der Verein hatte zunächst die Herausgabe und Übermittlung der Mitgliederliste zur Durchführung einer außerordentlichen Mitgliederversammlung verweigert, da die antragstellende Gruppe die laut der Satzung des Vereins für die Einberufung einer außerordentlichen Mitgliederversammlung notwendige Stimmenanzahl[167] von mindestens 25 % der Mitglieder des Vereins nicht erfüllte.

Vereinsrechtlich wird vielfach ein Anspruch auf Einsicht in eine Mitgliederliste zur Durchsetzung von Minderheitenbegehren, wie bspw. die Einberufung einer außerordentlichen Mitgliederversammlung, angenommen. Auch datenschutzrechtlich kann die Herausgabe und Übermittlung der Mitgliederliste im Einzelfall aufgrund der Pflicht des Vereins, die Ausübung der satzungsmäßigen Rechte und/oder Minderheitenbegehren zu ermöglichen, aufgrund von berechtigten Interessen der Antragstellenden erforderlich sein, ohne dass die Interessen der Vereinsmitglieder am Schutz ihrer personenbezogenen Daten überwiegen.[168] Das berechtigte Interesse liegt hier im Recht auf Mitwirkung an der Willensbildung im Verein, das insbesondere durch die Wahrnehmung von Minderheitenrechten ausgeübt wird und das durch die antragstellenden Vereinsmitglieder nachgewiesen werden muss.[169]

[167] Nach § 37 Abs. 1 BGB ist die Mitgliederversammlung eines Vereins zu berufen, wenn entweder der in der Satzung festgelegte Stimmenanteil oder in Ermangelung einer Bestimmung zehn Prozent der Mitglieder die Versammlung schriftlich unter Angabe vom Zweck und Grund verlangt.
[168] Siehe Art. 6 Abs. 1 Satz 1 lit. f. DS-GVO
[169] Siehe AG Hannover, Urteil vom 13. Februar 2019 – 435 C 10856/18

Die Mitglieder können zur Durchsetzung ihrer Minderheitenrechte auf die Mitgliederliste angewiesen sein, um hierüber satzungsgemäß genügend Mitglieder für die Unterstützung eines Antrags zur Einberufung einer außerordentlichen Mitgliederversammlung zu gewinnen.

Bei der Geltendmachung von Minderheitenbegehren ist nach Größe und Art des Vereins zu differenzieren. Zwar erscheint es bei größeren Vereinen unverhältnismäßig, von den Mitgliedern zur Durchsetzung von Minderheitenrechten zu verlangen, erst alle Mitglieder persönlich kennenzulernen und zu dem Thema zu befragen, um das in der Satzung geforderte Stimmenquorum zu erreichen. Jedoch ist es gleichzeitig wenig sachgerecht, z. B. bei bundesweit agierenden Vereinen mit mehreren Millionen Mitgliedern, eine Mitgliederliste an die Antragstellenden herauszugeben.

Insofern hat der Vereinsvorstand zu prüfen, wie einem Minderheitenbegehren datensparsam[170] entsprochen werden kann. Dies kann entweder durch Übermittlung der Mitgliederliste an eine:n Treuhänder:in oder Rechtsanwält:in oder durch Weiterleitung des Minderheitenbegehrens durch den Vereinsvorstand an die Mitglieder umgesetzt werden, ohne dass die Mitgliederliste direkt an die Antragstellenden herausgegeben oder übermittelt werden muss. Sofern die Liste jedoch an die Antragsstellenden herausgegeben wird, ist von diesen eine Zusicherung zu verlangen, dass die personenbezogenen Daten in der Mitgliederliste ausschließlich zu festgelegten Zwecken zu verarbeiten und anschließend zu löschen sind.

Die personenbezogenen Daten der Mitglieder eines Vereins in Form einer Mitgliederliste dürfen nicht ohne Rechtsgrundlage durch den Verein an andere Mitglieder herausgegeben oder übermittelt werden. Sofern einzelne Mitglieder Minderheitenrechte, wie z. B. die Einberufung einer außerordentlichen Mitgliederversammlung, geltend machen wollen, ist das berechtigte Interesse, bspw. das Recht auf Mitwirkung an der Willensbildung im Verein, durch die antragsstellenden Mitglieder nachzuweisen. Der Verein ist verpflichtet, vor der Herausgabe der Daten zu prüfen, ob mildere Mittel in Betracht kommen, die gleichermaßen geeignet sind, den Interessen der Empfänger:in zu genügen.

[170] Siehe Art. 5 Abs. 1 lit. c DS-GVO

10 Wirtschaft

10.1 „Verantwortungsvolle Datenverarbeitung“ durch Banken

Eine Bank informierte alle Kund:innen darüber, dass sie beabsichtige, die Betroffenen zukünftig mit Leistungen und Produkten zu bewerben, die genau der jeweiligen Lebens- und Finanzsituation entsprechen würden. Hierzu sollten fast alle Daten, über die die Bank verfügt, ausgewertet werden. Unter anderem hielt das Schreiben der Bank unter der Überschrift „Zu den verarbeiteten Daten zählen“ die folgenden Angaben:

• „Zahlungsverkehrsdaten, wie z. B. Angaben zu Zahlungsempfängern und Zahlern sowie Angaben aus Verwendungszwecken;

• Daten, die wir bei Ihrer Nutzung unseres Online-Angebots (wie z. B. Webseiten, Online-Banking und Apps) verarbeiten. Hierzu zählen z. B. Informationen über den von Ihnen gewählten Zugangsweg/Kommunikationskanal (wie etwa IP-Adresse, Art des Endgeräts), Datum und Uhrzeit der Nutzung, Informationen zu ihrer Servicehistorie sowie Informationen zu den von Ihnen aufgerufenen Online-Produkten.“

Der Brief hatte den Betreff „Verantwortungsvolle Datenverarbeitung“ und enthielt den Hinweis, dass gegen die Werbung ein Widerrufsrecht besteht.[171] *Mehrere Betroffene haben sich bei uns über die Vorgehensweise der Bank beschwert.*

Die Bank gehört zum Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V. (BVR). Dieser hatte seinen Mitgliedsbanken die beschriebene Vorgehensweise empfohlen und einen entsprechenden Text zur Verfügung gestellt. Da dieser von Banken aus verschiedenen Bundesländern verwendet wurde, haben wir das Ergebnis unserer Überprüfung bundesweit mit den anderen Aufsichtsbehörden abgestimmt.

Der BVR ging davon aus, dass die hier vorgenommene Datenauswertung für Werbezwecke ohne Vorliegen einer Einwilligung rechtmäßig sei. Die Datenschutz-Grundverordnung (DS-GVO) würde die Datenverarbeitung auch ohne Vorhandensein einer Einwilligung der Betroffenen gestatten.[172] Direkt-

[171] Siehe Art. 21 Abs. 2 Datenschutz-Grundverordnung (DS-GVO)
[172] Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO

werbung stelle ein berechtigtes Interesse dar.[173] Schutzwürdige Interessen der Betroffenen seien auch nicht tangiert, da sie rechtzeitig über die geplante Werbung und das Widerspruchsrecht informiert worden seien.

Die Rechtsauffassung des Bankenverbandes ist rechtsfehlerhaft. In den Erwägungsgründen der DS-GVO wird festgestellt, dass insbesondere dann, wenn eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, ihre -Interessen und Grundrechte ggü. dem Interesse des Verantwortlichen überwiegen können.[174]

Betroffene werden grds. nicht damit rechnen, dass Banken Zahlungsverkehrsdaten und Internetverhalten ihrer Kund:innen auswerten, um sie besser bewerben zu können. Hieran ändert auch die Information der Betroffenen nichts. Die Erwartungen der betroffenen Personen können dabei nicht durch die nach der DS-GVO vorgesehenen Pflichtinformationen[175] erweitert werden.[176] Während die Nicht- oder Schlechterfüllung der Informationspflicht das Abwägungsergebnis also aus Sicht des Verantwortlichen negativ beeinflusst, hat die ordnungsgemäße Erfüllung der Informationspflichten keine Auswirkung auf die Abwägung der Interessen.[177] Das Informationsschreiben der Bank führt also nicht zur Rechtmäßigkeit der Datenverarbeitung.

Die schutzwürdigen Interessen der Betroffenen sind auch deshalb höher als die Wirtschaftsinteressen der Bank zu bewerten, da durch die Zahlungsverkehrsdaten sehr genaue Profile über die Betroffenen erstellt werden können. Auch die Daten zur Nutzung des Online-Angebots sind sehr schützenswert, denn diese enthalten Informationen über Lebensgewohnheiten der Betroffenen.

Die schutzwürdigen Interessen der Betroffenen sind auch deshalb höher als die Wirtschaftsinteressen der Bank zu bewerten, da durch die Zahlungsverkehrsdaten sehr genaue Profile über die Betroffenen erstellt werden können. Auch die Daten zur Nutzung des Online-Angebots sind sehr schützenswert, denn

[173] Siehe EG 47 letzter Satz DS-GVO
[174] EG 47 Satz 4 DS-GVO
[175] Siehe Art. 13, 14 DS-GVO
[176] Siehe Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, S. 16; abrufbar unter https://www. datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf
[177] So auch der Europäische Datenschutzausschuss (EDSA), Guidelines 8/2020 on the targeting of social media users, Version 1.0, Par. 60, S. 18; abrufbar unter https://edpb.europa.eu/our-work-tools/public-consultations- art-704/2020/guidelines-082020-targeting-socialmedia-users_en

diese enthalten Informationen über Lebensgewohnheiten der Betroffenen.

Die Verhandlungen mit dem Bankenverband sind noch nicht abgeschlossen, die betroffene Bank muss allerdings damit rechnen, dass wir gegen ihre Werbemaßnahme – soweit das Verfahren nicht verändert wird – eine Verbotsverfügung erlassen werden.

Zahlungsverkehrsdaten und Daten über die Nutzung des Online-Angebots einer Bank dürfen nur mit Einwilligung der Betroffenen für Werbezwecke verwendet werden.

10.2 Transparenz bei Scoring-Verfahren

Ein Kunde beantragte bei seiner Bank eine Kreditkarte. Der Antrag wurde von der Bank mit der Begründung abgelehnt, sie habe anhand von Wahrscheinlichkeitswerten eine Bonitätseinschätzung durchgeführt (sog. Scoring), diese habe ergeben, dass er nicht über eine ausreichende Bonität verfüge.

Da der Bankkunde einen guten SCHUFA-Score hat und erfolgreicher Rechtsanwalt ist, bezweifelte er die Richtigkeit des von der Bank errechneten Scorewerts. Er beantragte eine Auskunft darüber, aufgrund welcher Daten die Bank zu der negativen Krediteinschätzung gekommen ist. Die Bank informierte ihn daraufhin über die zu seiner Person gespeicherten Daten und gab allgemeine Hinweise zu ihrer Kreditberechnung, weigerte sich aber, ihm mitzuteilen, warum sie in seinem Fall von einer schlechten Bonität ausging. Der Auskunftsanspruch[178] würde nicht so weit gehen, außerdem könne die Bank sich auf ein Betriebsgeheimnis berufen.

Der Bankkunde forderte die Bank zudem auf, seine Bonität noch einmal zu prüfen. Die Bank teilte ihm daraufhin mit, die zweite Prüfung habe erneut ergeben, dass seine Bonität für eine Kreditkarte nicht ausreichend sei. Der Betroffene beschwerte sich über die mangelnde Transparenz des Kredit-Scorings.

Die Bank hat gegen die Transparenzvorgaben bei Scoring-Verfahren verstoßen. Bei automatisierten Einzelentscheidungen wie dem Kredit-Scoring, die zu der Ablehnung eines Vertragsschlusses führt, haben die Betroffenen das Recht, die Entscheidung anzufechten und ihren eigenen Standpunkt darzule-

[178] Siehe Art. 15 DS-GVO

gen.[179] Zur Wahrnehmung dieser Einwirkungsrechte müssen den Betroffenen zumindest auch die wesentlichen Gründe für die betreffende automatisierte Einzelentscheidung und deren Auswirkung mitgeteilt und näher erläutert werden, ansonsten ist eine Einwendung gegen die Entscheidung nicht möglich. Bei erfolgten Kredit-Scorings gibt es ein sog. „right to explanation", also eine Begründungs- und Darlegungspflicht hinsichtlich bereits erfolgter automatisierter Entscheidungen.[180] Die Bank ist also verpflichtet, die Kundinnen und Kunden bei automatisierten Kreditentscheidungen über die tragenden Gründe einer Kreditablehnung zu unterrichten. Hierzu zählen Informationen zur Datenbasis und zum Einsatz bestimmter Faktoren bzw. Parameter, die der konkreten Entscheidung zugrunde gelegt wurden. Dabei müssen die Informationen nur insoweit detailliert erfolgen, als dies für die Nachvollziehbarkeit, nicht hingegen für die Nachrechenbarkeit der automatisierten Entscheidungsfindung erforderlich ist. „Kernanliegen jeglicher Transparenz ist es, die betroffene Person Verarbeitungsprozesse verstehen zu lassen und die Möglichkeit des Eingreifens zu eröffnen."[181]

Da die Bank sich weigerte, die Kreditentscheidung transparent zu machen, wurde der Vorgang an unsere Sanktionsstelle abgegeben.

Wird bei einer automatisierten Kreditentscheidung Betroffenen aufgrund eines Kredit-Scorings eine Leistung nicht erbracht, ist die Entscheidung den Betroffenen ggü. transparent zu machen.

10.3 Einwilligung in Werbung bei Telefongespräch

Eine Bank informierte ihre Kund:innen telefonisch darüber, wie man zukünftig mit der Kreditkarte im Internet bezahlt (Service-Call). Am Ende des Gesprächs wurden die Betroffenen gefragt, ob sie damit einverstanden seien, telefonisch zukünftig auch - beworben zu werden. Die Einwilligung in die Telefonwerbung wurde im Anschluss schriftlich bestätigt. Einige der Angeschriebenen bestritten, telefonisch eine Einwilligung erteilt zu haben und legten bei uns Beschwerde ein.

Die Frage, ob die Bank in den Beschwerdefällen versehentlich gar keine Einwilligung eingeholt hatte, kann offenbleiben, da die Vorgehensweise der Bank unabhängig davon rechtswidrig war. Die Verarbei-

[179] Siehe Art. 22 Abs. 3 DS-GVO
[180] Siehe Gola, DS-GVO, Franck, Art. 15, Rn. 19 m. w. N.
[181] Gola, DS-GVO, Franck, Art. 15, Rn. 19

tung der Telefonnummer zum Zweck der Einholung einer Einwilligung in zukünftige Werbemaßnahmen war mangels Rechtsgrundlage unzulässig, insbesondere handelte es sich nicht um eine rechtmäßige Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen.[182] Aufgrund der Rechtsprechung des OVG Berlin-Brandenburg ist davon auszugehen, dass bereits die Einholung der Einwilligung für zukünftige Werbemaßnahmen als (Direkt-)Werbung einzuordnen ist.[183] Direktwerbung kann zwar grds. ein berechtigtes Interesse der verantwortlichen Stelle für die Verarbeitung personenbezogener Daten sein.[184] Der deutsche Gesetzgeber hat aber in Umsetzung europäischen Rechts entschieden, dass Werbung bei einem Telefonanruf ggü. einer Verbraucherin bzw. einem Verbraucher ohne vorherige ausdrückliche Einwilligung der Betroffenen nicht rechtmäßig ist.[185]

Die Bank hat die Möglichkeit, sich die Einwilligung in Telefonwerbung mithilfe anderer Kommunikationsmittel als per Telefon geben zu lassen. Ein Telefonat mit zwei unterschiedlichen Zwecken (Service-Call, Einwilligung in Werbung) wohnt ein gewisser „Überrumpelungseffekt“ inne. Denn die betroffene Person wird regelmäßig nicht erwarten, dass ihr:e Vertragspartner:innen bei einem Anruf zum Zwecke der Vertragserfüllung einen weiteren, eigennützigen Zweck verfolgen.

Wir haben die Bank aufgrund ihres Verhaltens verwarnt. Die Bank hat uns mitgeteilt, dass sie zukünftig nicht mehr per Telefon Einwilligungen in Werbung einholt. Die bisherigen Einwilligungen werden zudem nicht mehr von der Bank genutzt.

Service-Calls dürfen nicht dazu genutzt werden, sich Einwilligungen in Telefonwerbung geben zu lassen.

10.4 Unerwünschte Werbung nach angeblicher Teilnahme an einem Gewinnspiel — Nachweis der Einwilligungserklärung

Immer wieder erreichen uns Beschwerden von betroffenen Personen, die Werbung von ihnen unbekannten Unternehmen erhalten. Im Rahmen der Beantwortung von Auskunftsersuchen verweisen werbende Unternehmen dann oft auf eine von den betroffenen Personen ggü. einem dritten Unterneh-

[182] Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO
[183] Siehe OVG Berlin-Brandenburg, Beschluss vom 31. Juli 2015 – OVG 12 N 71.14
[184] Siehe EG 47 letzter Satz DS-GVO
[185] Siehe § 7 Abs. 2 Nr. 2 Gesetz gegen den unlauteren Wettbewerb (UWG) i. V. m. Art. 13 Abs. 3 Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)

men im Rahmen eines Gewinnspiels abgegebene Einwilligungserklärung.

Nach der DS-GVO muss die verantwortliche Stelle nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat[186]. Insoweit bleibt die bisherige Rechtsprechung des Bundesgerichtshofs (BGH) zum Gesetz gegen den unlauteren Wettbewerb (UWG)[187] auch weiterhin anwendbar, wonach es nicht ausreicht, wenn lediglich abstrakt dargelegt wird, dass eine Einwilligung erteilt wurde. „Wird etwa im Rahmen einer datenschutzrechtlichen Streitigkeit das Vorliegen einer wirksamen Einwilligung bestritten und kann die verantwortliche Stelle keinen zweifelsfreien Nachweis darüber erbringen, ist im Zweifel davon auszugehen, dass keine rechtswirksame Einwilligung vorliegt."[188]

Kann die Einwilligung nicht oder nicht in der Form und unter den Bedingungen, die sich aus der DS-GVO ergeben[189], nachgewiesen werden, ist die Verarbeitung personenbezogener Daten für den Zweck, für den eine Einwilligungserklärung mangels eines sonstigen Erlaubnistatbestandes vorliegen müsste, unzulässig. Erwägungsgrund 42 DS-GVO führt aus, dass die verantwortliche Stelle nachweisen können sollte, „dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat". Die verantwortliche Stelle hat deshalb nachzuweisen, in welcher Weise und aufgrund welcher vor Beginn der Verarbeitung erfolgten Erklärung oder aktiven Handlung die betroffene Person die Einwilligung vorgenommen hat. Es muss nachweisbar sein, dass die Erklärung vorab erfolgte.[190] Außerdem ist nachzuweisen, was der Inhalt der Einwilligung ist, insbesondere in welche Verarbeitung welcher Daten zu welchem Zweck eingewilligt wurde. Des Weiteren ist der Nachweis zu erbringen, dass der betroffenen Person vor Erteilung ihrer Einwilligung alle erforderlichen Informationen gegeben wurden, damit diese die Entscheidung auf der Basis hinreichender Informationen über Risiken und Folgen der Einwilligung erkennen konnte. Zu protokollieren und zu dokumentieren sind daher nicht nur der Inhalt der Erklärung, sondern auch das Verfahren, wie die Erklärung zustande kam, einschließlich der Angabe, welche Informationen über den Umfang und den Zweck der Datenverarbeitung sowie das Widerrufs-

[186] Siehe Art. 7 Abs. 1 DS-GVO
[187] Siehe BGH, Urteil vom 10. Februar 2011 – I ZR164/09
[188] Ehmann/Selmayr/Heckmann/Paschke DS-GVO, Art. 7, Rn. 68
[189] Siehe Art. 4 Nr. 11 DS-GVO und Art. 7 DS-GVO
[190] Siehe Art. 6 Abs. 1 Satz 1 lit. a DS-GVO („hat ... gegeben")

recht der betroffenen Person vor Abgabe der Erklärung zur Entscheidungsfindung gegeben wurden.[191]

In zahlreichen Beschwerdeverfahren konnte ein Unternehmen eine angeblich im Rahmen eines Gewinnspiels ggü. einer dritten Stelle abgegebene Einwilligung betroffener Personen zum Erhalt von Werbung regelmäßig nicht zweifelsfrei nachweisen. Unsere Bußgeldstelle wird nun entsprechende Sanktionierungen prüfen.

Verantwortliche Stellen sind zum zweifelsfreien Nachweis verpflichtet, dass betroffene Personen in die Verarbeitung ihrer personenbezogenen Daten zu Werbezwecken eingewilligt haben.

10.5 Anwendbarkeit der DS-GVO zugunsten von juristischen Personen?

Gegenstand zahlreicher bei uns eintreffender Anfragen ist die Anwendbarkeit der DS-GVO zugunsten von juristischen Personen. So erreichten uns bspw. Beschwerden zu Werbe-E-Mails, die an allgemeine Funktions-E-Mail-Adressen juristischer Personen gerichtet waren, jedoch im Textteil die Geschäftsführung namentlich ansprachen.

Die DS-GVO findet Anwendung, soweit personenbezogene Daten betroffen sind.[192] „Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[193] Erwägungsgrund 14 DS-GVO erklärt einschränkend die Verordnung auf „personenbezogene Daten juristischer Personen und insbesondere als juristische Person gegründete Unternehmen" als nicht anwendbar. Einzelne Mitglieder einer juristischen Person bzw. eine oder mehrere hinter der juristischen Person stehende natürliche Personen sind jedoch geschützt, wenn sich die Angaben über die Personengemeinschaft auch auf sie beziehen. So können Angaben über eine GmbH zu Gesellschafter:innen oder Geschäftsführer:innen dieser GmbH Bezug haben, sofern zwischen der GmbH und den hinter ihr stehenden Personen eine enge finanzielle, personelle oder wirtschaftliche Verflechtung besteht. Bei derartigen Verbindungen zwischen einer natürlichen und einer juristischen Person, die häufig bei der „Ein-Personen-GmbH" auftreten, kann in der Regel davon ausgegangen werden, dass ein Bezug zu der hinter der juristischen Person stehenden na-

[191] Siehe Taeger/Gabel/Taeger DS-GVO, Art. 7, Rn. 37-40
[192] Siehe Art. 2 Abs. 1 DS-GVO
[193] Siehe Art. 4 Nr. 1 DS-GVO

türlichen Person besteht und somit der Anwendungsbereich der DS-GVO eröffnet ist.[194]

In den uns vorliegenden Beschwerdefällen, in denen Geschäftsführer:innen einer GmbH von dem werbenden Unternehmen, mit dem sie zu keinem Zeitpunkt vorher in Kontakt standen, in Werbeschreiben namentlich angesprochen wurden, haben wir jeweils eine Verwarnung ausgesprochen.

Es bleibt bei dem Grundsatz, dass die DS-GVO für juristische Personen als solche keine Anwendung findet. Dies gilt allerdings nicht, sofern es um den Schutz der hinter der juristischen Person stehenden natürlichen Personen geht.

10.6 Die – begrenzten – Befugnisse von Konzerndatenschutzbeauftragten

Das Datenschutzrecht sieht vor, dass Unternehmen eine/n Datenschutzbeauftragte:n berufen müssen, wenn u. a. mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.[195] Unternehmen in einer Unternehmensgruppe[196] ist es möglich, eine/n gemeinsame/n Konzerndatenschutzbeauftragte:n zu benennen,[197] die bzw. der die Aufgaben für jedes juristisch selbstständige Unternehmen der Unternehmensgruppe wahrnimmt. In diesem Fall muss nicht mehr jedes Unternehmen eine/n eigene/n Datenschutzbeauftragte:n benennen.

Uns erreichten Anfragen von Unternehmen und Betriebsräten zur Rolle der Konzerndatenschutzbeauftragten. Dabei haben sich Unternehmen in erster Linie nach den Rechten und Pflichten der Konzerndatenschutzbeauftragten erkundigt. Die Betriebsräte interessierten sich hingegen insbesondere für die Rechte der Mitarbeitenden. Seit Beginn der Pandemie gab es zudem vermehrt Fragen zur Erreichbarkeit von Konzerndatenschutzbeauftragten.

Konzerndatenschutzbeauftragte dürfen vom Unternehmen nicht in ihrer Arbeit behindert werden. Die Unternehmensgruppe muss den Datenschutzbeauftragten Zugang zu allen personenbezogenen Daten und Verarbeitungsvorgängen gewähren, deren Kenntnis für die Ausübung der Funktion erforderlich sind. Die nötigen Ressourcen[198] müssen in dem

[194] Siehe Gola, DS-GVO, Gola, Art. 4, Rn. 25 sowie EuGH, Urteil vom 9. November 2010 – C-92/09, C-93/09
[195] Siehe § 38 BDSG
[196] Art. 4 Nr. 19 DS-GVO definiert eine Unternehmensgruppe als: „[E]ine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht“.
[197] Siehe Art. 37 Abs. 2 DS-GVO
[198] Bspw. Mitarbeitende, Räumlichkeiten, IT-Infrastruktur und finanzielle Mittel

Umfang vorhanden sein, dass die Datenschutzbeauftragten ihrer Arbeit ungehindert nachgehen können. Zwar darf die/der Arbeitgeber:in grds. das Zeitkontingent für die Ausübung der Funktion festlegen. Es muss aber so bemessen werden, dass die Person die Aufgabe ordnungsgemäß wahrnehmen kann.[199] Aufgrund des Umfangs der anfallenden Aufgaben innerhalb eines Konzerns werden die Datenschutzbeauftragten hier oftmals von einem größeren Team flankiert. In diesem Fall gilt nicht nur für die bzw. den Konzerndatenschutzbeauftragte:n, sondern auch für die Mitarbeitenden des Teams die Verschwiegenheitsverpflichtung[200].

Konzerndatenschutzbeauftragte sollten von jeder Niederlassung des Unternehmens aus leicht zu erreichen sein. Die Mitarbeitenden sollten diese innerhalb eines Werktages persönlich erreichen können. Die Mitarbeitenden sollen sich mit allen Fragen in Bezug auf die Verarbeitung ihrer Daten und mit der Wahrnehmung ihrer Rechte an die Person wenden können.[201] Die Vorgaben sind gerade bei internationalen Unternehmensgruppen oft nur schwer zu erfüllen. Zur Unterstützung der Arbeit kann das - jeweilige Einzelunternehmen deshalb zusätzlich Datenschutzkoordinator:innen berufen. Diese unterstützen die Konzerndatenschutzbeauftragten bei der Umsetzung von deren Aufgaben an ihrem Standort bzw. in ihrem Fachbereich. Sie sind zudem - Ansprechpartner:innen für Anfragen der Mitarbeitenden vor Ort.

11 Verkehr, Tourismus und Auskunfteien

11.1 „Jelbi“ – Die Mobilitäts-App der BVG — Ein Zwischenfazit

Die BVG betreibt die App „Jelbi“, mit der verschiedene Mobilitätsangebote kombiniert werden. Mit der App können Fahrauskünfte eingeholt und Buchungen sowohl von Bus und Bahn als auch bspw. von Roller, Fahrrad, Taxi oder Auto, auch in Kombination, vorgenommen werden.

Die App wurde entwickelt und 2019 in Betrieb genommen, ohne dass wir eingebunden wurden. Wir haben erst aus der Presse davon erfahren. Bereits bei kursorischer Prüfung der App haben wir zahlreiche Datenschutzverstöße festgestellt. Über diese haben

[199] Siehe Art. 38 Abs. 2 DS-GVO
[200] Siehe Art. 38 Abs. 5 DS-GVO; Mitarbeitende müssen sich vertraulich an die bzw. den Konzerndatenschutzbeauftragten wenden können. Die bzw. der Konzerndatenschutzbeauftragte darf einen Datenschutzverstoß der Aufsichtsbehörde melden.
[201] Siehe Art. 38 Abs. 4 DS-GVO

wir in unserem Jahresbericht 2019 ausführlich berichtet.[202]

Seitdem uns die App bekannt wurde, befinden wir uns in einem andauernden Austausch mit der BVG. In dessen Verlauf haben wir einige Verbesserungen des Datenschutzniveaus bei „Jelbi“ erreichen können. Die BVG hat Widersprüche und Unklarheiten in den Einwilligungserklärungen und Datenschutzhinweisen bereinigt. Sie weist nunmehr bspw. darauf hin, dass sie ihre Forderungen an ein Unternehmen abtritt, das diese dann im eigenen Namen geltend macht. Anders als vorher wird bei Neukund:innen, die mit Kreditkarte zahlen wollen, auch keine SCHUFA-Abfrage mehr durchgeführt. Bei diesen ist mangels Ausfallrisiko eine Beurteilung der Bonität nicht erforderlich. Zudem gibt die BVG keine Angaben mehr über das jeweilige Geschlecht der Nutzer:innen an das Unternehmen, an das sie etwaige Forderungen abtritt, weiter. Innerhalb der App werden zudem keine Cookies von Dritten gesetzt. Das US-amerikanische Unternehmen, das zuvor für die BVG die Telefonnummern der Nutzer:innen verifizierte, wird ebenfalls nicht mehr eingesetzt. [203] Diese Auflistung erhebt keinen Anspruch auf Vollständigkeit.

Gleichwohl gibt es nach wie vor Punkte, wegen derer wir „Jelbi“ auch über zwei Jahre nach Start der App keine Datenschutzkonformität bestätigen können. Dies betrifft vor allem den Einsatz weiterer US-amerikanischer Dienste, insbesondere eines Cloud-Providers.

„Jelbi“ befindet sich derzeit in einem Neuausschreibungsprozess. 2022 soll eine Neuauflage der App erfolgen. Im Rahmen der Ausschreibung hat die BVG verschiedene Datenschutz- und IT-Sicherheits-Anforderungen aufgestellt. Eine feste Zusicherung, auf den Einsatz der von uns angesprochenen problematischen Dienstleister:innen zu verzichten, haben wir allerdings von der BVG nicht erhalten. Klärungsbedürftig sind des Weiteren etwa die Dauer der Speicherung der Führerscheindaten, die Übermittlung von E-Mail-Adressen an die Forderungskäufer:innen oder die derzeit bestehende Pflicht zur Angabe der Handynummer bei der Anmeldung bei der App.

Wir halten ein Konzept wie „Jelbi“ für grds. datenschutzkonform umsetzbar. Hierbei sind aber be-

[202] JB 2019, 4.1
[203] Siehe zur allgemeinen Problematik 1.1

stimmte rechtliche und technische Anforderungen zu beachten. Die BVG geht davon aus, diese spätestens in der Neuauflage der App erfüllen zu können. Wir werden die Umsetzung von Beginn an aufmerksam begleiten, damit nicht nochmal eine im Hinblick auf den Datenschutz unfertige App auf den Markt kommt.

11.2 Check-In/Check-Out per Smartphone im ÖPNV

Deutschlandweit bieten Verkehrsunternehmen in jüngerer Zeit sog. Check-In/Check-Out-Systeme auf digitaler Basis an. Fahrgäste geben in einer App Beginn und Ende einer Fahrt an. Die App erfasst die gefahrene Strecke und rechnet sodann auf Grundlage des günstigsten möglichen Fahrpreises ab. In vergleichbaren Check-In/Be-Out- oder Be-In/Be-Out-Systemen erfasst die App Beginn und/oder Ende einer Fahrt eigenständig. Ebenfalls vergleichbar, aber weitergehend, werden auf Grundlage solcher Systeme sog. Luftlinientarife eingeführt. Die Abrechnung erfolgt hier nicht mehr auf Basis von Tarifzonen, sondern nach der Entfernung zwischen Start- und Zielstation. Auch die BVG hat uns ein Projekt zur Erprobung eines entsprechenden Check-In/Check-Out-Systems in begrenztem Rahmen vorgestellt.

Bei der Nutzung solcher Systeme wird im Vergleich zum Kauf herkömmlicher Tickets ein Vielfaches an personenbezogenen Daten der Fahrgäste verarbeitet. Dies betrifft insbesondere die umfassende Erhebung und Speicherung von Fortbewegungsdaten. So sollen in dem System der BVG sämtliche abgefahrene Stationen nicht nur erfasst, sondern darüber hinausgehend für ein Jahr gespeichert werden. Neben den passierten Stationen werden insbesondere Standortdaten der Fahrgäste verarbeitet. Sollten die Fahrgäste sich versehentlich oder aufgrund technischer Probleme nicht ausloggen, werden deren Standortdaten auch über die Fahrt hinaus verarbeitet.

Anhand dieser Daten können umfassende Bewegungsprofile erstellt werden. So können Rückschlüsse etwa auf Wohn- und Arbeitsort sowie Freizeitverhalten der Fahrgäste gezogen werden. Insbesondere sind auch Rückschlüsse auf sensitive Daten möglich, etwa über den Besuch von Arztpraxen oder Religionsstätten. Derartige Systeme sind daher nicht unproblematisch.

Daneben gibt es für Verkehrsunternehmen, die solche Systeme einführen möchten, bestimmte Fallstricke bei der konkreten Umsetzung, insbesondere,

wenn auf bestehende Apps von Drittanbieter:innen zurückgegriffen wird. In anderen Staaten sind solche Apps teilweise umfassender im Einsatz als bisher in Deutschland. Naturgemäß sind die Anbieter:innen dieser Apps wenig bestrebt, ihre Produkte an die hiesigen Vorgaben anzupassen, da dies mit zusätzlichem Aufwand und Kosten verbunden ist. Zudem möchten solche Drittanbieter:innen die im Rahmen der Nutzung der App des jeweiligen Verkehrsunternehmens erhobenen Daten oftmals auch für die Weiterentwicklung ihrer eigenen App nutzen. Dies ist für öffentliche Verkehrsunternehmen problematisch, da die Unterstützung der Weiterentwicklung einer App eines privaten Unternehmens nicht Teil ihrer Aufgabe „Durchführung von öffentlichem Personennahverkehr“ ist.

Der von der BVG im Zusammenhang mit dem Projekt beauftragte Dienstleister plant zudem, zahlreiche Daten der Fahrgäste, bspw. deren Kontakt- und Fortbewegungsdaten, an US-amerikanische Unternehmen, wie etwa Cloud-Dienste, zu übermitteln. Der Einsatz derartiger Dienstleister ist mit erheblichen Risiken für die betroffenen Personen verbunden, da die übermittelten Daten auch dem Zugriff US-amerikanischer Behörden unterliegen, und nur unter sehr engen Voraussetzungen überhaupt zulässig.[204] Diese Voraussetzungen werden derzeit von der BVG nicht erfüllt.

Wir haben diese Einwände ggü. der BVG geltend gemacht und stehen in einem intensiven Austausch mit der BVG über das Projekt. Hierbei konnten bereits einige Erfolge erzielt werden. Beispielsweise hat die BVG umfassend Unterlagen angepasst, in denen die Fahrgäste bislang nur unzureichend über die Risiken des Systems informiert wurden. Außerdem wurde auf den Einsatz eines Unterdienstleisters verzichtet. Ob die App der BVG letztlich datenschutzkonform realisierbar ist, wird sich zeigen.

App-basierte Check-In/Check-Out- oder vergleichbare Systeme bergen erhebliche Risiken für die Nutzenden. Dies ist insbesondere der Fall, wenn Verkehrsunternehmen auf bestehende Apps von Drittanbieter:innen und auf Dienstleister:innen in den USA zurückgreifen. Daneben sind bestimmte technische Vorgaben zu beachten. Zudem unterliegen derartige Systeme der grundlegenden Problematik, dass mittels der zahlreichen, zum Teil sensitiven Daten Bewegungsprofile der Fahrgäste erstellt werden können. Sie sind daher bereits konzeptionell

[204] Siehe 1.1

problematisch. Sollte ein Verkehrsunternehmen dennoch an der Einführung eines solchen Systems festhalten wollen, sollte es dem Datenschutz bereits von Beginn der Planungsphase an große Beachtung widmen, u. a. durch enge Zweckbindung und kurze Speicherfristen der notwendigerweise zu verarbeitenden Daten.

11.3 Verarbeitung von Daten zu Energieversorgerverträgen durch Auskunfteien

Bei einigen Auskunfteien gab es Überlegungen, einen „Pool" aus Datensätzen zu Strom- und Gasverträgen zwischen Privatpersonen und Energieversorgungsunternehmen (sog. Energieversorgerpool) zu schaffen. In diesen sollten auch Daten über Verträge übermittelt werden, bei denen es nicht zu Zahlungsausfällen kam (sog. Positivdaten).

Auskunfteien dürfen Positivdaten zu Privatpersonen grds. nicht aufgrund überwiegender berechtigter Interessen[205] erheben. Regelmäßig überwiegt das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Dies hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits 2018 festgestellt.[206] Nachdem die Überlegungen zur Schaffung des Energieversorgerpools bekannt wurden, hat die DSK diesen Beschluss für den Energieversorgerpool nochmals bestätigt.[207] Die Vorlage für den neuerlichen Beschluss wurde im Wesentlichen durch unsere Behörde zusammen mit der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen erarbeitet.

Energieversorgungsunternehmen bieten regelmäßig Neukund:innenrabatte an. Mittels einiger Positivdaten zu Energieversorgerverträgen (Anzahl und Dauer der jeweiligen Verträge) wäre es möglich, festzustellen, ob Verbraucher:innen regelmäßig ihr Energieversorgungsunternehmen wechseln, um dauerhaft günstige Konditionen zu erhalten. Die betroffenen Personen könnten sodann von Neukund:innen-rabatten ausgeschlossen werden. „Schnäppchenjäger:innen" auszuschließen stellt aber kein berechtigtes Interesse dar. Die betroffenen Personen haben das Recht, den Wettbewerb zwischen den Energieversorgungsunternehmen zu nutzen, zumal diese die

[205] Siehe Art. 6 Abs. 1 Satz 1 lit. f DS-GVO

[206] Beschluss der DSK vom 11. Juni 2018: „Verarbeitung von Positivdaten zu Privatpersonen durch Auskunfteien"; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

[207] Beschluss der DSK vom 15. März 2021: „'Energieversorgerpool' darf nicht zu gläsernen Verbraucher*innen führen"; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

Anreize, zwischen den Unternehmen zu wechseln, selbst geschaffen haben.

Selbst wenn ein berechtigtes Interesse vorliegen würde, überwiegen nach den allgemeinen Grundsätzen zur Verarbeitung von Positivdaten durch Auskunfteien die Interessen der sich vertragstreu verhaltenden Personen. Diese dürfen erwarten, dass ihre Daten nicht, insoweit über den Vertragszweck hinausgehend, an Auskunfteien übermittelt werden.

Die Verarbeitung von Positivdaten zu Energieversorgerverträgen durch Auskunfteien auf Grundlage eines berechtigten überwiegenden Interesses ist unzulässig. Das Interesse der betroffenen Personen an der Hoheit über ihre eigenen Daten überwiegt. Sie sind insbesondere berechtigt, den Wettbewerb zwischen Energieversorgungsunternehmen zu nutzen und mehrfach zwischen diesen zu wechseln. Andernfalls würden sie (weiter) zu gläsernen Verbraucher:innen werden, ohne dass sie durch ihr Verhalten hierzu Anlass gegeben hätten.

12 Videoüberwachung

12.1 Bodycams bei der Deutschen Bahn

In den Jahren 2016 und 2017 hat die Deutsche Bahn Sicherheit GmbH (DB) im Rahmen eines Pilotprojekts die Ausstattung ihrer Sicherheitskräfte mit Bodycams zum Eigenschutz und als Deeskalationsmaßnahme getestet.[208] Seit 2018 erfolgt der Einsatz von Bodycams an ausgewählten Bahnhöfen[209] nun im Regelbetrieb. Einen ersten Evaluierungsbericht zum Regelbetrieb für die Jahre 2019/2020 hat uns die DB nun vorgelegt.

Aus den Erfahrungen der Testphase wurden folgende Grundsätze für den Regelbetrieb festgelegt:

- Der Einsatz von Bodycams erfolgt ausschließlich in Bereichen und zu Dienstzeiten, die mit Blick auf die registrierten Übergriffe auf die Sicherheitskräfte als kritisch bewertet werden. Diese sog. „Kriminalitätsräume“ unterliegen einer jährlichen erneuten Bewertung und damit Überprüfung.

[208] Siehe JB 2016, 3.8.2 und JB 2017, 3.5

[209] In Berlin: Ostbahnhof, Alexanderplatz, Zoologischer Garten sowie in den Zügen zwischen den Bahnhöfen Westkreuz und Ostkreuz

- Bodycams werden im ausgeschalteten Zustand und nicht im Stand-By-Modus eingesetzt. Ein Pre-Recording ist ausgeschlossen. Eine Tonaufzeichnung erfolgt nicht

- Bei einer sich abzeichnenden kritisch entwickelnden Situation weisen die Sicherheitskräfte auf eine mögliche Aufzeichnung durch die Bodycam hin. Sollte sich aufgrund dieses Hinweises die Situation deutlich entspannen, erfolgt keine Aufzeichnung. Bleibt die Situation jedoch unverändert, schaltet die Sicherheitskraft, wie angekündigt, das Gerät ein. Damit wird ein Kamerabild live auf dem Display sichtbar. Aufgezeichnet wird dieses jedoch noch nicht. Erst wenn die Situation weiter als eskalierend eingeschätzt wird, erfolgt durch die Sicherheitskraft die tatsächliche Aufzeichnung nach entsprechender weiterer Ankündigung (Stufen-Deeskalationsmodell).

- Zur Umsetzung der Transparenzpflicht[210] führen die Sicherheitskräfte eine Hinweiskarte zur Datenerhebung mit sich und überreichen diese im Fall einer aus der Situation heraus erfolgten Aufzeichnung. Ferner ist die Bekleidung der Sicherheitskräfte vorn mit einem Kamera-Piktogramm und auf dem Rücken mit dem Aufdruck „Video“ gekennzeichnet.

- Der Fokus der Kamera ist so grundeingestellt, dass Unbeteiligte im Hintergrund in der Regel kaum wahrnehmbar sind.

- Aufgezeichnete Daten werden unmittelbar nach Dienstende, spätestens aber 24 Stunden nach Beendigung der Aufzeichnung, soweit eine Übergabe an die Sicherheitsbehörden nicht erforderlich ist, systemseitig gelöscht.

- Ein Zugriff auf die Videodaten durch die DB ist nicht möglich. Das Bildmaterial kann ausschließlich durch die Bundespolizei eingesehen werden.

Unseren Forderungen entsprechend hat die DB in den Folgejahren 2019 und 2020 nach Einführung des Regelbetriebs die Gesamtlage der Übergriffe auf die Beschäftigten, die Wirksamkeit der Technik und die Wahrnehmung der Mitarbeitenden in Bezug auf die Wirkung der Bodycams bei Streifengängen weiter beobachtet und evaluiert.

[210] Siehe Art. 13 Datenschutz-Grundverordnung (DS-GVO)

Insgesamt haben Beschäftigte der DB im Evaluierungszeitraum 350.000 Stunden lang eine Bodycam getragen. Während dieses Zeitraums wurde die Bodycam lediglich 23 Mal aktiviert. Davon erschien das aufgenommene Material in nur 14 Fällen dazu geeignet, dieses der Bundespolizei zu Beweiszwecken zu übergeben. In wie vielen Fällen davon die Polizei das Material verwendet hat, ist nicht bekannt. Diese Zahlen lassen für sich genommen den Nutzen von Bodycams als sehr gering erscheinen und begründen Zweifel an der Erforderlichkeit dieser Maßnahme.

Allerdings meinte die DB, in ihrer Evaluierung eine präventive Wirkung der sichtbar getragenen Bodycams feststellen zu können, auch wenn diese nicht eingeschaltet sind. Denn in dem Evaluierungszeitraum wurden lediglich 116 der 2.196 Übergriffe auf Bahnbeschäftigte auf Personal verübt, das eine Bodycam trug. Das entspricht einer Quote von ca. 5,3 %. Gleichwohl musste die DB auf unsere Nachfrage hin einräumen, dass lediglich in 7,9 % der Gesamtarbeitsstunden eine Bodycam getragen wurde, was die genannten Zahlen deutlich relativiert.

Nach den subjektiven Eindrücken der Bahnbeschäftigten war hingegen ein deutlicher Erfolg zu verzeichnen. Aufgrund des Tragens einer Bodycam sei z. B. die Dauer einer Maßnahme oder eine Eskalation in gefährlichen Situationen deutlich verringert oder sogar verhindert worden. Dies zeige, dass das Tragen der Bodycams als präventive Sicherungs- und Deeskalationsmaßnahme ein geeignetes Mittel darstelle.

Da aber mit Videoüberwachungen Grundrechtseingriffe einhergehen, kann die Zulässigkeit dieser Maßnahme nicht maßgeblich an subjektiven Eindrücken gemessen werden, sondern ist anhand der objektiven Erforderlichkeit der Maßnahme zu beurteilen. Da die festgestellten Zahlen hier keinen eindeutigen Befund zulassen, werden wir den Einsatz der Bodycam durch die DB weiter beobachten. Allerdings haben wir in den 23 genannten Fällen auch keine Beschwerden der Betroffenen oder sonstige Hinweise auf eine Datenschutzverletzung im Einzelfall erhalten.

Da Bodycams kaum eingesetzt wurden, ist es schwer zu überprüfen, inwieweit diese Technik zur Sicherheit auf Bahnhöfen beigetragen hat. Aus demselben Grund kam es allerdings auch kaum zu Eingriffen in das informationelle Selbstbestimmungs-

recht. Wir werden den Einsatz dieser Technik weiter beobachten.

12.2 Auskunftsansprüche bei Videoüberwachung

Seit einigen Jahren führt nicht nur die BVG, sondern auch die S-Bahn Berlin GmbH eine Videoüberwachung in bestimmten Zügen auf einzelnen Teilstrecken durch. Als Zwecke für die Videoüberwachung gibt die S-Bahn Berlin GmbH u. a. „Wahrnehmung des Hausrechts", „Schutz von Leben, Gesundheit und Freiheit von Kunden und Beschäftigten" und „Beweissicherung im Ereignisfall" an. Die Videodaten werden in einem Blackbox-Verfahren gespeichert und nach 48 Stunden gelöscht, wenn sie nicht aufgrund entsprechender Vorfälle benötigt werden.

Ein Fahrgast hatte die S-Bahn Berlin GmbH gebeten mitzuteilen, welche Daten zu seiner Person während einer S-Bahnfahrt mittels der im Zug installierten Videokamera von ihm gespeichert wurden. Zur Konkretisierung seines Anliegens und zur Identifizierung seiner Person hat der Fahrgast die Zugnummer und den Zeitpunkt der Aufnahme mitgeteilt. Darüber hinaus hat er sein Aussehen und seine Kleidung beschrieben, die er bei der Bahnfahrt trug und ergänzt, auf das im Zug angebrachte Hinweisschild gezeigt zu haben. Sein Auskunftsersuchen (mit der Bitte um Übersendung einer Kopie der entsprechenden Videoaufnahmen) hat der Fahrgast zeitnah, d. h. innerhalb der Speicherfrist, bei der S-Bahn Berlin GmbH eingereicht.

Der Fahrgast berief sich auf seinen Auskunftsanspruch nach Art. 15 Datenschutz-Grundverordnung (DS-GVO). Demnach hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten.

Die S-Bahn Berlin GmbH teilte daraufhin dem Fahrgast mit, dass die Herausgabe einer Kopie von Videoaufnahmen nicht möglich sei und berief sich ebenfalls auf den Datenschutz. Zum Schutz der Persönlichkeitsrechte anderer Fahrgäste erfolge eine Herausgabe nur auf polizeiliche Anforderung und nicht an Privatpersonen. Sogar die S-Bahn selbst nehme keine Einsicht in die Videodaten. Auskünfte an die Strafverfolgungsbehörden würden nur anhand eines Zeitstempels, nicht aber mittels Sichtung der Inhalte des Videomaterials erfolgen. Nach Auffassung der S-Bahn Berlin GmbH handelt es sich bei

den Videodaten nicht um personenbezogene Daten, da diese von der S-Bahn Berlin GmbH nicht eingesehen würden.

Wir haben der S-Bahn Berlin GmbH mitgeteilt, dass es sich bei den Videodaten um personenbezogene Daten handelt. Die angefertigten Videoaufnahmen dienen gerade dazu, bei bestimmten Ereignissen wie Schäden oder Übergriffen, die Verursachenden zu identifizieren. Dazu ist es nicht erheblich, ob die Daten von S-Bahn-Beschäftigen eingesehen werden oder nicht. Da es sich bei dem Videomaterial um personenbezogene Daten handelt, haben Betroffene das Recht, Auskunft über diese zu verlangen. Diese Auskunft kann auch in Form einer Kopie verlangt werden.

Eine Auskunft in Form einer Kopie kann auch nicht pauschal deshalb verweigert werden, weil womöglich die Persönlichkeitsrechte anderer Fahrgäste betroffen sind. Zwar sieht die DS-GVO vor, dass das Recht auf eine Datenkopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen darf. Dem hätte allerdings hier Rechnung getragen werden können, indem die Aufnahmen anderer Fahrgäste vor der Übermittlung geschwärzt oder verpixelt werden. Auch ein hoher Aufwand ist kein Grund, die Auskunft zu verweigern. In diesem Fall zeigt die regelmäßige Datenübermittlung an die Polizeibehörden, dass eine Auskunftserteilung durchaus möglich ist.

Wir haben die S-Bahn Berlin GmbH aufgefordert, ein Verfahren zu entwickeln, wie Videodaten zukünftig korrekt beauskunftet werden. Dies lehnt die S-Bahn Berlin GmbH bislang ab und möchte die Angelegenheit nunmehr gerichtlich mit uns klären.

Wer personenbezogene Daten verarbeitet, muss damit rechnen, dass Betroffene ihr Auskunftsrecht geltend machen.[211] Dieses besteht auch bei personenbezogenen Daten, die über eine Videoüberwachungsanlage erhoben werden.[212] Eine Auskunft kann nur in wenigen Ausnahmefällen verweigert werden. Ein zu hoher Aufwand gehört regelmäßig nicht dazu.

[211] Siehe Art. 15 DS-GVO

[212] So auch der Europäische Datenschutzausschuss (EDSA), Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Version 2.0, Ziff. 6.1, S. 24 f.; abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien

13. Sanktionen

13.1 Corona-Fälle

Vor allem in der Anfangszeit der Pandemie lagen viele Kontaktdatenformulare offen in Restaurants, Cafés oder Bars aus, auf welchen sich mehrere Personen unabhängig voneinander eintragen mussten. Damit Gesundheitsämter Infektionsketten effektiv nachverfolgen können, sahen die jeweiligen Versionen der SARS-CoV-2-Infektionsschutzmaßnahmenverordnung Regelungen zur Erhebung von Kontaktdaten wie Name, Telefonnummer, Anschrift oder E-Mail-Adresse vor.

Solche Datensammlungen bergen die Gefahr des Missbrauchs. In drei von uns mit jeweils einem Bußgeld versehenen Fällen wurden die Kontaktdaten durch zwei Mitarbeiter zweckentfremdet.

So haben ein Mitarbeiter eines Fast-Food-Restaurants und ein Mitarbeiter eines Friedhofs jeweils Vornamen, Nachnamen und Telefonnummern von Frauen aus bei den Stellen geführten Kontaktlisten entnommen, um die Frauen privat anzuschreiben und u. a. nach deren Beziehungsstatus zu fragen.

Die Verwendung von personenbezogenen Daten aus Kontaktlisten zur infektionsschutzrechtlichen Anwesenheitsdokumentation außerhalb der Kontaktnachverfolgung ist rechtswidrig und wird durch unsere Behörde sanktioniert.

13.2 Bußgelder wegen unbefugter Nutzung der Polizeidatenbank POLIKS

Die Sanktionsstelle führt regelmäßig Verfahren gegen Polizeibeamt:innen durch, die unbefugt, d. h. zu nicht-dienstlichen Zwecken, personenbezogene Daten von Dritten aus den polizeiinternen Datenbanken abrufen.

POLIKS ist eines der wichtigsten elektronischen Informationssysteme der Polizei und enthält dementsprechend viele, zum Teil sehr sensitive personenbezogene Daten. In POLIKS werden insbesondere Daten von Beschuldigten, Straftäter:innen, Tatverdächtigen, Betroffenen sowie Daten von Opfern und Zeug:innen erfasst und gespeichert; darunter bspw. Namen, Geburtsdaten, Anschriften und Familienstand, aber auch Vorstrafen und Aussagen von Zeug:innen. Die Polizei nutzt POLIKS als Informationssystem für ihre gesetzlichen Aufgaben im Bereich der Strafverfolgung und der Gefahrenabwehr. Bedienstete der Polizei werden in regelmäßigen

Die Polizei hat in den vergangenen Jahren verschiedene technische und organisatorische Maßnahmen erfolgreich umgesetzt, um unrechtmäßige Zugriffe auf POLIKS zu verhindern und gleichzeitig die Aufklärung von etwaigen missbräuchlichen Datenabrufen zu erleichtern.

Zu den Maßnahmen zählen regelmäßige Belehrungen, systematische Stichprobenkontrollen und eine sogenannte „Negativliste“, die bestimmte Eingaben zum Abfragezweck nicht zulassen. Zusätzlich erfolgt bei jedem Aufruf von POLIKS ein Hinweis an den Nutzenden, dass nur rechtmäßige Abfragen gestattet sind und bei Zuwiderhandlung entsprechende Konsequenzen folgen.

Abständen über die datenschutzrechtlichen Vorschriften informiert und darüber belehrt, dass es ihnen ausdrücklich untersagt ist, Daten aus POLIKS und anderen polizeilichen Informationssystemen für private Zwecke zu nutzen.

Der Zugang zu POLIKS wird aber immer wieder dazu missbraucht, Freund:innen, Familienmitglieder, Nachbar:innen oder Dritte und deren Lebensumstände abzufragen.

So fragte ein Polizeibeamter alle Personen aus dem Umfeld seiner Ex-Lebensgefährtin ab, die mit dem Umstand der Trennung hätten vertraut sein können.

In einem anderen Fall schrieb ein Polizeibeamter eine Zeugin nach deren Vernehmung über ihre private Handynummer an, um diese nach einer Verabredung zu fragen, nachdem er die Telefonnummer aus POLIKS abgerufen hatte.

In einem weiteren Fall fragte ein Polizeibeamter den Ermittlungsvorgang seines Stiefsohnes ab, um diesen auf seine Zeugenaussage vorzubereiten und um den zuständigen Sachbearbeiter von einem anderen Tathergang zu überzeugen.

Zudem hatte ein Polizist den neuen Lebensgefährten der Ex-Frau eines Freundes abgefragt, weil er befürchtete, dass das gemeinsame Kind durch den neuen Partner gefährdet sei. Abfragen in POLIKS sind nur zu dienstlichen Zwecken zulässig, was voraussetzt, dass die polizeilichen Ermittlungen in der jeweiligen Angelegenheit den Abfragenden dienstlich übertragen wurden. Dies war hier nicht gegeben. Der Polizist handelte auf eigene Initiative, ohne den Verdacht der zuständigen Dienststelle zu melden.

In einem anderen Fall wollte ein in einem Strafverfahren beschuldigter Polizeibeamter die Informationen aus POLIKS verwenden, um sich auf seine Aussage vor Gericht vorzubereiten.

In diesem Jahr haben wir fünfzehn Verfahren gegen Polizeibeamtinnen und -beamte eingeleitet und bereits insgesamt elf Bußgeldbescheide mit insgesamt 42 Bußgeldern gegen Polizeibeamt:innen erlassen.

13.3 Unbefugte Datenbankabfragen von Jobcenter-Mitarbeitenden

Immer wieder sanktionieren wir auch Mitarbeitende der Jobcenter, wenn diese unbefugte Abfragen im Online-Melderegister oder den Sozialdatenbanksys-

temen vornehmen, ohne dass eine rechtliche Grundlage für die Datenverarbeitung vorliegt.

In einem von uns eingeleiteten Verfahren wollten Mitarbeitende nachweisen, dass zwei ihrer Kolleg:innen eine Beziehung miteinander haben und überprüften dafür die Meldeadressen der beiden.

In einem weiteren Fall fragte eine Mitarbeitende die Meldedaten der Ex-Frau ihres Bruders ab, die den Kontakt zum Ex-Mann abgebrochen hatte.

In diesem Jahr haben wir insgesamt vier Verfahren gegen Mitarbeiter:innen der Jobcenter eingeleitet und bereits ein Bußgeld erlassen.

13.4 Anordnung und Bußgelder wegen unzulässiger Videoüberwachung

Unsere Sanktionspraxis zeigt, dass Videoüberwachung häufig zu leichtfertig und ohne fundierte Begründung aus Präventionsgesichtspunkten eingesetzt wird, ohne dabei die Rechte der betroffenen Personen ausreichend zu würdigen.

In einem Fall haben wir daher Immobilieneigentümer:innen die Verarbeitung personenbezogener Daten durch die in einem gemischt genutzten Gebäude angebrachten Videokameras verboten. [213] Die Videoüberwachung diente dem Zweck der Prävention und Aufklärung von Straftaten in Form von Sachbeschädigungen durch „Schmierereien“, Einbrüche oder Drogenmissbrauch, da sich das Gebäude in einem Kriminalitätsschwerpunkt befindet. Allerdings konnte kein Fall nachgewiesen werden, bei dem die Videoüberwachung tatsächlich zur Aufdeckung von Straftaten führte. Die drei Kameras ermöglichten durch ihre Positionierung im Eingangsbereich, im Innenhof und vor dem Kellerzugang, die Mieter:innen rund um die Uhr anlasslos insbesondere dahingehend zu beobachten, wann und wie oft sie das Haus und den Keller betreten und verlassen (inkl. An- und Abwesenheit), und ob sie ordnungsgemäß ihren Müll entsorgen. Dazu kam noch, dass auch die Patient:innen der ebenfalls im Gebäude befindlichen Arztpraxen beim Betreten des Gebäudes gefilmt wurden. Im konkreten Fall war die Videoüberwachung bereits nicht erforderlich, denn schon durch gut positionierte Bewegungsmelder und Absprachen mit den Arztpraxen, wem Einlass ins Gebäude gewährt wird, war es möglich, ungebetenen Dritten den Zugang zum Gebäude zu erschweren. Sie war auch im engeren Sinne nicht

[213] Siehe Art. 58 Abs. 2 lit. f DS-GVO

verhältnismäßig, denn eine ständige Videoüberwachung eines Wohngebäudes zum Schutz gegen Sachbeschädigungen ist grds. unzulässig. Es bedarf konkreter Tatsachen, die das Vorliegen einer tatsächlichen Gefährdungslage in dem Ausmaß begründen, dass eine Videoüberwachung als letzter Lösungsweg[214] notwendig ist.

In einem Bußgeldfall ging es um die Videoüberwachung einer Fachklinik durch insgesamt 21 Kameras in den Räumen der Klinik. Rund um die Uhr wurden so die Patient:innen und Mitarbeitenden gefilmt, weil die Klinikleitung sich vor Straftaten und Eigentumsschäden in der Klinik schützen wollte. Eine angebliche Einwilligung der Mitarbeitenden im Arbeitsvertrag scheiterte bereits an der Freiwilligkeit der Einwilligung wegen der Drucksituation im Arbeitsverhältnis. Auch deutlich sichtbar angebrachte Hinweise auf die Videoüberwachung berechtigen nicht den Schluss, dass die Patient:innen durch das Betreten der überwachten Räumlichkeiten rechtswirksam ihr Einverständnis mit der Beobachtung zum Ausdruck bringen. Auch sonst konnte die Fachklinik keine Anhaltspunkte vortragen, die diese umfangreiche Videoüberwachung der Klinik rechtfertigten.

In einem weiteren Fall haben wir ein Bußgeld gegen ein Getränkehandelsunternehmen verhängt, das die öffentliche Straße neben dem Unternehmensgebäude filmte.

Die Videoüberwachung von Gebäuden und öffentlichen Straßen sollte datenschutzrechtlich grds. als ultima ratio zum Schutz von Eigentum und vor Straftaten angesehen werden. Für die Zulässigkeit einer solchen Videoüberwachung bedarf es konkreter Tatsachen für das Vorliegen einer tatsächlichen Gefährdungslage, die über das allgemeine Lebensrisiko hinausgeht und der nicht mit anderen Mitteln begegnet werden kann.

13.5 Datenschutz ist Leitungssache, aber nicht so

Ein Bußgeldfall zeigt exemplarisch die Wichtigkeit der Auswahl der betrieblichen Datenschutzbeauftragten auf. Eine Fachklinik hatte den Klinikleiter, der gleichzeitig Gesellschafter der Klinik war, zum Datenschutzbeauftragten ernannt.

Ein:e Datenschutzbeauftragte:r kann zwar andere Aufgaben und Pflichten wahrnehmen, das Unternehmen hat allerdings sicherzustellen, dass andere

[214] Ultima ratio

Aufgaben und Pflichten der/des Datenschutzbeauftragten nicht zu einem Interessenkonflikt führen.[215] Die/Der Datenschutzbeauftragte hat im Rahmen ihrer/seiner Aufgabenwahrnehmung[216] gerade bei einem Konflikt zwischen wirtschaftlichen oder fachlichen Zielvorgaben und Interessen mit datenschutzrechtlichen Belangen (z. B. von Beschäftigten oder Kund:innen) die Geschäftsleitung zu beraten, ohne selbst diesem Konflikt ausgesetzt zu sein. Sofern Datenschutzbeauftragte selbst über die Datenverarbeitung entscheiden, führt dies grds. zu einem Interessenkonflikt, da diese sich insofern nicht selbst - kontrollieren können. Ein unzulässiger Interessenkonflikt kann sich daher zunächst schon aus der Stellung der Person im Unternehmen ergeben, insbesondere darf ein:e Datenschutzbeauftragte:r nicht Inhaber:in des jeweiligen Unternehmens oder Mitglied des geschäftsführenden Organs sein.

Einem solchen Interessenkonflikt unterlag der Klinikleiter, da er zum einen in seiner Leitungsposition strategische und operative Entscheidungen über die Zwecke und Mittel der Verarbeitung von Beschäftigten- und Patient:innendaten zu treffen und als Gesellschafter ein wirtschaftliches Interesse am Erfolg der Klinik hat, er andererseits als Datenschutzbeauftragter die Einhaltung des Datenschutzrechts durch die Klinik kontrollieren muss.

Aus einer solchen Doppelrolle folgt auch die Gefahr, dass eine erhebliche psychische Barriere für Patient:innen und Mitarbeitende besteht, mit kritischen Fragen zur Verarbeitung personenbezogener Daten zum Datenschutzbeauftragten, der gleichzeitig Klinikleiter ist, zu gehen.

Zwar sollte die Unternehmensleitung die Einhaltung des Datenschutzrechts immer im Blick behalten, die Entscheidungsbefugnis der Leitungspersonen über die Verarbeitung personenbezogener Daten sorgt allerdings dafür, dass sie sich nicht selbst als Datenschutzbeauftragte benennen können. Wenn es bisher keine Mitarbeitenden im Unternehmen gibt, die datenschutzrechtliches Wissen haben, können solche eingestellt werden oder vorhandene Mitarbeitende für diese Position auf Kosten des Unternehmens geschult werden. Ansonsten besteht die Möglichkeit, externe Datenschutzbeauftragte zu engagieren.

[215] Siehe Art. 38 Abs. 6 DS-GVO
[216] Siehe Art. 39 DS-GVO

13.6 Veröffentlichung von Daten zur Erzwingung einer Forderungsbegleichung

Wir haben ein Bußgeld gegen einen Rechtsanwalt verhängt, der seit Jahren mit einem ehemaligen Mandanten über eine Geldforderung streitet. Er veröffentlichte dessen Vor- und Nachnamen, die Wohnanschriften des Mandanten und dessen Familienmitgliedern sowie diverse ungeschwärzte Aktenbestandteile zwei Jahre lang auf seinem Blog – und berief sich dabei auf das Presseprivileg.

In dem Fall handelte es sich aber nicht um eine ausschließlich journalistische Veröffentlichung, da die Gesamtbewertung des Sachverhaltes ergab, dass der Rechtsanwalt mit der Veröffentlichung kein journalistisches Interesse verfolgte. Es ging ihm vielmehr darum, die Zahlung des nach seiner Auffassung ihm zustehenden Geldbetrages zu erwirken. Daten werden jedoch nur dann zu journalistischen Zwecken verarbeitet, wenn „sie ausschließlich zum Ziel haben, Informationen, Meinungen oder Ideen in der Öffentlichkeit zu verbreiten…“[217].

Die Datenverarbeitung erfolgte auch nicht aufgrund eines berechtigten Interesses. Aufgrund der zweifelhaften Absichten bei der Veröffentlichung überwogen im Ergebnis die schutzwürdigen Interessen der Geschädigten. Gerade aufgrund des bereits anhängigen gerichtlichen Verfahrens wäre es für den Rechtsanwalt zumutbar gewesen, den Ausgang des Verfahrens abzuwarten, ohne im Vorfeld hierüber auf seiner Webseite zu berichten.

Der Rechtsanwalt hat den Beitrag nach der Einleitung unseres Bußgeldverfahrens gelöscht und sich kooperativ im aufsichtsrechtlichen Verfahren und dem Bußgeldverfahren verhalten, was wir bußgeldmindernd berücksichtigt haben.

14 Telekommunikation und Medien

14.1 Mängel auf allen Ebenen: Wir konfrontieren Webseiten-Betreibende mit rechtswidrigem Tracking

Angesichts der andauernden Defizite beim Einsatz von Tracking-Techniken und Drittdiensten auf Webseiten haben wir im August eine Schwerpunktaktion gestartet. Rund fünfzig Unternehmen erhielten postalisch die Aufforderung, das Tracking auf ihren Webseiten in Einklang mit den geltenden Datenschutzregeln zu bringen. In den Schreiben haben wir

[217] EuGH, Urteil vom 16. Dezember 2008 – C-73/07, Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy

sowohl allgemein die rechtlichen Bestimmungen erläutert, als auch auf besonders kritische Punkte hingewiesen, die wir im Einzelfall festgestellt haben. Die meisten der angeschriebenen Unternehmen haben unsere Hinweise zwar zum Anlass genommen, optische und funktionale Veränderungen auf ihren Webseiten vorzunehmen. Vielfach wurden jedoch nur einzelne der identifizierten Mängel ausgeräumt, sodass weiterhin Handlungsbedarf besteht.

Bei uns gehen neben Individualbeschwerden in großer Anzahl auch allgemeine Prüfanregungen zu Tracking-Prozessen auf Webseiten ein. Die Masse an Hinweisen zeigt nicht nur die Bedenken der Bürger:innen, sondern ist auch Indikator dafür, wie viele Webseitenbetreiber:innen sich nach wie vor schwertun, den rechtlichen Rahmenbedingungen gerecht zu werden.

Mit dem Einsatz von Tracking-Techniken, wie z. B. sog. Cookies, geht die Verarbeitung personenbezogener Daten, mindestens der IP-Adresse der Besuchenden, einher. Dies dient meist nicht nur dazu, das Verhalten von Nutzer:innen nachzuverfolgen, sondern auch Persönlichkeitsprofile über die gesamte Internetnutzung zu erstellen und anzureichern. Diese Daten werden regelmäßig an eine Vielzahl von Akteuren von Werbenetzwerken in der ganzen Welt übermittelt, z. B. um die Betroffenen personalisiert zu bewerben.

Wenn Betreiber:innen von Webseiten das Verhalten ihrer Nutzer:innen mithilfe von Cookies und anderen Technologien nachverfolgen wollen, benötigen sie dafür eine Rechtsgrundlage. In den meisten Anwendungsfällen kommt hierfür nur eine Einwilligung in Betracht. Auch wenn viele Webseitenbetreibende mittlerweile differenzierte Cookie-Banner auf ihren Webseiten anzeigen, sind diese häufig gar nicht geeignet, eine wirksame Einwilligung einzuholen. Besonders eklatant fällt dabei auf, dass die Ablehnung des Tracking meist wesentlich komplizierter und aufwendiger möglich ist als die Zustimmung. Eingebettet wird dies vielfach auch in unvollständige oder missverständliche Angaben oder Beschriftungen. Wie die Webseitenbetreibenden bei einer solchen Gestaltung nachweisen wollen, dass die Nutzer:innen freiwillig und informiert zugestimmt haben, ist unklar.

Um zu erreichen, dass beim Einsatz von Tracking-Techniken und Drittdiensten auf Webseiten großflächig Mängel beseitigt werden, haben wir in diesem

Jahr eine Aktion gestartet, die besonders viele Webseitenbetreibende erreichen soll.

Hierfür haben wir optische Gestaltungsmerkmale, technische Prozesse und konkrete Datenströme auf knapp fünfzig Webseiten dokumentiert, zu denen wir zuvor Prüfanregungen erhalten haben. Die Betreiber:innen der Webseiten haben wir mit konkreten datenschutzrechtlichen Defiziten konfrontiert, die uns dabei aufgefallen sind. Wir haben die dokumentierten Sachverhalte in Relation zu den rechtlichen Bestimmungen gesetzt und auf besonders kritische Punkte im Einzelfall hingewiesen. Neben der fehlenden gleichwertigen Ablehnungsmöglichkeit auf erster Ebene erweisen sich auch die weiteren Ebenen der Einwilligungsdialoge häufig als mangelhaft. So entsprechen die in den Cookie-Bannern enthaltenen Informationen vielfach nicht den Informationen in den Datenschutzerklärungen. Auch werden die Datenverarbeitungsprozesse im Kontext des Trackings in etlichen Fällen nicht auf eine Einwilligung, sondern auf eine andere Rechtsgrundlage gestützt, ohne dass die gesetzlichen Anforderungen hierfür erfüllt sind.

Die Hinweisschreiben wurden an Unternehmen gesendet, deren Cookie-Banner als besonders mangelhaft aufgefallen sind, die vergleichsweise viele Nutzer:innen haben oder die möglicherweise besonders sensitive Daten verarbeiten. Betroffen sind Unternehmen aus diversen Branchen, insbesondere Online-Handel, Immobilien, Finanzen, Soziale Netzwerke, Software, Gesundheit, Bildung und Vergleichsportale. Die Verantwortlichen wurden aufgefordert, die Datenverarbeitung unverzüglich in Einklang mit den datenschutzrechtlichen Vorgaben zu bringen. Unsere Aktion ergänzt die bereits laufenden Prüfverfahren, die auf persönlichen Beschwerden beruhen und dient auch als Signal an Webseitenbetreibende.

Bei einer erneuten Sichtung der Webseiten hat sich gezeigt, dass die Cookie-Banner auf den meisten Webseiten optisch und funktional verändert oder zumindest die Menge an gesetzten Cookies und Datenströmen an Dritte reduziert wurden. Insgesamt wurden hierdurch auf vielen Webseiten Defizite reduziert. Überwiegend reichen die ergriffenen Maßnahmen jedoch nicht, um alle identifizierten Mängel zu beseitigen. Auf einigen Webseiten konnten wir sogar feststellen, dass sich die Situation noch verschlechtert hat, indem nunmehr z. B. noch mehr einwilligungsbedürftige Cookies ohne vorherige wirksame Zustimmung gesetzt werden. Auch wur-

den in Einzelfällen Ablehnungsmöglichkeiten auf erster Bannerebene ergänzt, die jedoch scheinbar wirkungslos sind. Schließlich fiel bei unserer Nachprüfung ins Auge, dass die meisten Webseitenbetreibenden das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) nach dessen Inkrafttreten im Dezember[218] noch nicht berücksichtigt haben. Mithin besteht seitens der Webseitenbetreiber:innen in vielen Fällen weiterhin Handlungsbedarf, um einen rechtskonformen Zustand herbeizuführen.

Sollten im Rahmen der Prüfung andauernde datenschutzrechtliche Verstöße festgestellt werden, müssen die Unternehmen mit aufsichtsrechtlichen Maßnahmen rechnen. Gegen Verantwortliche, die weiterhin datenschutzwidrig das Nutzungsverhalten auf ihrer Webseite überwachen, werden wir die Einleitung von Anordnungs- sowie Bußgeldverfahren prüfen.

14.2 Das Telekommunikation-Telemedien-Datenschutz-Gesetz — Mehr Rechtsklarheit für Cookies

Am 1. Dezember 2021 ist das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft getreten. Das TTDSG regelt u. a. den Schutz der Vertraulichkeit und Privatsphäre bei der Nutzung von technischen Endgeräten, die mit dem Internet verbunden werden können. Durch das Gesetz werden mit jahrelanger Verzögerung endlich die europäischen Vorgaben der ePrivacy-Richtlinie in deutsches Recht umgesetzt. Hierdurch ändern sich auch die rechtlichen Rahmenbedingungen für den Einsatz von Cookies. Unter anderem Betreiber:innen von Webseiten und Apps sollten ihre Prozesse dahingehend überprüfen. Zur Unterstützung haben die deutschen Aufsichtsbehörden eine neue Orientierungshilfe veröffentlicht.

Beim Betrieb sog. Telemedien, wie z. B. Webseiten oder Apps, werden regelmäßig Technologien eingesetzt, die es ermöglichen, das Verhalten von Nutzer:innen zu verfolgen. In der Praxis geschieht dies häufig – aber nicht nur – durch Cookies. Unabhängig von der technischen Ausgestaltung oder den verfolgten Zwecken wird die technische Erhebung und weitere Verarbeitung dieser Informationen meist als ein einheitlicher Lebenssachverhalt wahrgenommen. Rechtlich sind hier jedoch zwei Schritte zu unterscheiden: Der Einsatz von Cookies und ähnlichen Technologien dient zunächst der Erhebung

[218] Siehe 14.2

von Nutzer:innendaten, um diese personenbezogenen Daten dann in einem zweiten Schritt für diverse Zwecke weiterzuverarbeiten, bspw. zur Personalisierung von Werbung und Inhalten, für die Sicherheit einer Webseite, für Untersuchungen zur Nutzung des Angebots u. v. m.

Die Rechtmäßigkeit dieser (Folge-)Verarbeitungen richtet sich im Grundsatz nach den Anforderungen der Datenschutz-Grundverordnung (DS-GVO). Die vorgelagerten technischen Prozesse – insbesondere das Setzen von Cookies und Auslesen von Informationen aus diesen – berühren jedoch auch die Integrität der Endgeräte und die Privatsphäre der Nutzer:innen. Hierfür gibt es einen spezialgesetzlichen Rechtsrahmen auf europäischer Ebene – die ePrivacy-Richtlinie.[219]

Nach der Bewertung der Aufsichtsbehörden war der für Telemedien seit 2009 geltende Art. 5 Abs. 3 ePrivacy-Richtlinie durch § 15 Telemediengesetz (TMG) bisher nicht hinreichend in nationales Recht umgesetzt worden.[220]

Zum 1. Dezember 2021 wurde die Vorschrift endlich in deutsches Recht umgesetzt.[221] Diese Vorschrift ist zukünftig beim Einsatz jeglicher Technologien zu beachten, mittels derer Informationen auf Endgeräten gespeichert oder aus diesen ausgelesen werden. In der Norm wird der Grundsatz geregelt, dass die Speicherung von Informationen in technischen Endgeräten oder der Zugriff auf dort bereits gespeicherte Informationen nur mit der Einwilligung der Endnutzer:innen zulässig ist. Für Einwilligungen gelten dieselben Voraussetzungen wie sie schon jetzt für Einwilligungen nach der DS-GVO gelten.[222] Einer Einwilligung bedarf es dann nicht, wenn die Speicherung von und der Zugriff auf Informationen in den Endgeräten unbedingt erforderlich sind, damit ein von Nutzer:innen ausdrücklich gewünschter Telemediendienst zur Verfügung gestellt werden kann.

[219] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz

[220] Siehe Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) für Anbieter von Telemedien vom 29. März 2019; abrufbar unter https://www.datenschutzkonferenz-online.de/orientierungshilfen.html

[221] Siehe § 25 TTDSG

[222] § 25 Abs. 1 Satz 2 TTDSG

Mit Blick auf die neue Rechtslage haben die Aufsichtsbehörden die Orientierungshilfe von 2019[223] vollständig überarbeitet und die neue Version im Dezember veröffentlicht.[224] Darin geben die Aufsichtsbehörden Hinweise für die Praxis, welche Cookies und ähnliche Technologien unter den strengen Voraussetzungen des TTDSG überhaupt noch ohne Einwilligung zum Einsatz kommen können. Zusätzlich sind in der Orientierungshilfe ausführliche Hinweise zu den Voraussetzungen einer wirksamen Einwilligung enthalten. Hier haben wir in der Vergangenheit bei der Prüfung der Cookie- oder Einwilligungsbanner auf diversen Webseiten große Defizite festgestellt.

14.3 Nachbesserungsbedarf beim Online-Wegweiser zu Testzentren

Datenschutzrechtliche Mängel wirken sich bei solchen Webseiten besonders deutlich aus, auf deren Inhalte Bürger:innen alternativlos angewiesen sind. Eine solche Konstellation bestand bei einer Online-Informationsplattform der Senatsverwaltung für Gesundheit, Pflege und Gleichstellung (SenGPG), die als zentrale staatliche Anlaufstelle für Corona-Tests eingerichtet wurde. Bei einer Überprüfung der Webseite haben wir verschiedene Verstöße festgestellt. Auf unsere Anhörung wurde zeitnah reagiert. Es wurden diverse Maßnahmen getroffen, um die Mängel weitestgehend zu beheben.

Im März sind bei uns gehäuft Beschwerden zu möglichen Rechtsverstößen auf der Webseite test-to-go.berlin eingegangen. Die Webseite, die von SenGPG betrieben wurde, diente damals als zentrale Informationsplattform für Corona-Tests. Unter anderem wurde auf der Webseite eine tagesaktuelle Übersicht aller Testzentren und Teststellen zur Verfügung gestellt, teilweise direkt mit einer Möglichkeit zur Terminbuchung.

Die Beschwerdeführer:innen haben einerseits Bedenken über den Einsatz von Tracking-Techniken internationaler Konzerne geäußert. Andererseits seien die datenschutzrechtlichen Informationen auf der Webseite unvollständig, fehlerhaft und verwirrend gewesen. Es sei insbesondere nicht möglich gewesen zu verstehen, welche Daten an welche Dritten bei Inanspruchnahme der Funktionen der Webseite offenbart wurden.

Wie im Jahresbericht ausgeführt, wurde der Betrieb der Internetseite https://test-to-go.berlin/ im Oktober 2021 eingestellt. Inzwischen wurde für die Bürgerinnen und Bürger ein neues Angebot auf der Internetseite https://www.direkttesten.berlin/ eingerichtet, bei dessen Gestaltung die angemerkten Kritikpunkte berücksichtigt wurden.

[223] Siehe Fn. 2
[224] Siehe https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf

Wir haben daraufhin ein Prüfverfahren eröffnet, in dem sich die Bedenken der Bürger:innen bestätigt haben. Zwar wurde beim ersten Aufruf der Webseite ein Banner am unteren Rand eingeblendet, mit dem über den Einsatz von Techniken zu Analysezwecken informiert und eine Zustimmung hierzu abgefragt wurde. Jedoch konnten wir feststellen, dass einwilligungsbedürftige Prozesse bereits stattfanden, bevor der Button „Akzeptieren“ im Banner geklickt wurde. Unter anderem wurde unmittelbar nach Aufruf der Seite ein interaktiver Stadtplan angezeigt, wodurch personenbezogene Daten an einen US-basierten Drittdienst offenbart wurden. Hinzu kam, dass das Banner den Zugriff auf das Impressum und die Datenschutzerklärung versperrte, sodass Nutzer:innen keine Möglichkeit hatten, sich über die Hintergründe und Verantwortlichkeiten der Datenverarbeitungsprozesse zu informieren. Letztlich hätte es den Nutzer:innen auch gar nicht geholfen, die Datenschutzerklärung ungehindert aufrufen zu können, denn diese enthielt gänzlich unzureichende Informationen. Es fehlten nicht nur etliche Angaben zu den Datenverarbeitungsprozessen, die auf der Webseite tatsächlich stattfanden. Vielmehr enthielt die Datenschutzerklärung stattdessen diverse Informationen zu Prozessen, die überhaupt nicht existierten. Es drängte sich der Eindruck auf, dass die Erklärung ein Duplikat einer anderen Webseite oder ein Muster war, das nicht ausreichend an den Einzelfall angepasst wurde.

Aufgrund der mangelhaften Informationen konnten sich betroffene Personen kein Bild darüber machen, welche weiteren Akteure an welchem Schritt der integrierten Terminbuchungsfunktion beteiligt und wie die Verantwortlichkeiten jeweils geregelt waren. Klarstellende Informationen waren hier dringend angezeigt, da die Gestaltung der Unterseiten, in die die Buchungsfunktion integriert waren, enormes Verwirrungspotential enthielt.

Beachtlich war zudem, dass uns in der Liste an Testzentren keinerlei Adressen mehr angezeigt wurden, als wir beim Besuch der Webseite ein Programm aktivierten, mit welchem Browserverbindungen zu Drittdienstleistern blockiert werden. Nutzer:innen, die ihre Browser besonders datensparsam eingestellt haben, konnten damit keine einzige Information des staatlichen Angebots einsehen.

Auf unsere Anhörung hin hat der technische Dienstleister, der die SenGPG damals beim Betrieb der Webseite unterstützt hat, reagiert. Es wurden zeitnah diverse Maßnahmen getroffen, um die Mängel zu

beheben. Unter anderem wurde eine neue Cookie-Banner-Lösung implementiert, die technisch sicherstellte, dass einwilligungsbedürftige Prozesse erst nach einer Zustimmung aktiviert und durch das Banner keine Inhalte verdeckt wurden. Auch wurden Tracking-Techniken von Drittdienstleiter:innen durch lokal gehostete Lösungen ersetzt. Die Adressliste wurde unabhängig von etwaigen Browsereinstellungen abrufbar gemacht und die Stadtkarte wurde nun erst geladen, wenn Nutzer:innen diese aktivierten. Schließlich wurden die Datenschutzhinweise und die Gestaltung der Terminbuchung vollständig überarbeitet, sodass die Verantwortlichkeitsverhältnisse nachvollziehbarer wurden. Offenbar wurde jedoch auch, dass die erforderlichen Formalien für etwaige Auftragsbeziehungen nicht rechtzeitig erledigt waren.

Bei einer Nachkontrolle der Webseite im September musste festgestellt werden, dass hinsichtlich potenzieller Drittlandtransfers und der Rolle einiger Dienstleister:innen noch Klärungsbedarf bestand. Jedoch wurde das Angebot auf test-to-go.berlin im Oktober eingestellt. Die Webseite dient seither nur noch als Wegweiser auf ein neues Informationsangebot, bei dessen Gestaltung unsere Hinweise offenbar vollumfänglich berücksichtigt wurden. Wegen der gravierenden und vielfältigen Mängel wurde ggü. der SenGPG eine Verwarnung ausgesprochen.

14.4 Verarbeitung personenbezogener Daten im Internet-Angebot der Wikimedia Foundation Inc. – Wikipedia

Die in den USA ansässige Wikimedia Foundation Inc. bietet – als gemeinsame Verantwortliche zusammen mit den Autor:innen der Artikel[225] – im Internet u. a. die deutschsprachige Fassung der Online-Enzyklopädie Wikipedia an. Zu einzelnen Artikeln in diesem Angebot erreichten uns Beschwerden betroffener Personen.

Die Beschwerden betrafen u. a. die Weigerung der Verantwortlichen, personenbezogene Daten betroffener Personen zu korrigieren oder einzelne Angaben aus den Artikeln zu löschen. Andere betroffene Personen hatten darüber hinaus die vollständige Löschung ihrer Daten bzw. des gesamten sie betreffenden Artikels aus dem Angebot verlangt. Einige der Beschwerdeführer:innen gingen davon aus, dass unsere Behörde für die Kontrolle der Einhaltung von Datenschutzbestimmungen im deutschsprachigen Angebot der Wikipedia zuständig sei, weil die nationale Länderorganisation (Chapter) der Wikimedia

[225] Siehe Art. 26 DS-GVO

Foundation, der „Wikimedia Deutschland – Gesellschaft zur Förderung Freien Wissens e. V.“ (Wikimedia Deutschland e. V.), seinen Sitz in Berlin hat.

Mit der Frage, ob und ggf. in welchem Umfang das nationale bzw. europäische Datenschutzrecht auf die Veröffentlichung personenbezogener Daten in der deutschsprachigen Wikipedia Anwendung findet, hatten wir uns bereits vor Inkrafttreten der DS-GVO beschäftigt. Dabei waren wir zu dem Ergebnis gekommen, dass eine datenschutzrechtliche Verantwortlichkeit des in Berlin ansässigen Wikimedia Deutschland e. V. nicht gegeben war. Datenschutzrechtlich verantwortlich war bereits zu dieser Zeit die in den USA ansässige Wikimedia Foundation Inc. als Betreiberin des Internet-Angebots, die nicht unserer Kontrolle unterlag.[226] Dies war nach Inkrafttreten der DS-GVO erneut zu überprüfen, da diese im Gegensatz zu dem davor anzuwendenden Bundesdatenschutzgesetz (BDSG) auch für Verantwortliche in Drittstaaten außerhalb der Europäischen Union (wie hier den USA) gelten kann.[227]

Die DS-GVO ist grds. auch für Veröffentlichungen in der deutschsprachigen Wikipedia anzuwenden, da es sich auch ggü. den von der Veröffentlichung personenbezogener Daten betroffenen Personen, die sich in der Europäischen Union befinden, um eine Dienstleistung handelt, die (jedenfalls auch) diesen Personen angeboten wird.[228]

Dies hatte die Wikipedia Foundation Inc. in ihrer Stellungnahme zunächst mit der Begründung bestritten, die dort angebotenen Veröffentlichungen richteten sich gerade nicht an die davon betroffenen Personen, und diese würden auch nicht ermutigt, über sich selbst Artikel mit personenbezogenen Daten in der Wikipedia zu verfassen. Diese Aussage stimmte aber so nicht: Einige der Artikel, die Gegenstand von Beschwerden waren, stammten nach Angaben der betroffenen Personen jedenfalls ursprünglich von diesen selbst. Es waren auch keine Hinweise darauf zu finden, dass die Verantwortliche die Erstellung und Veröffentlichung solcher Artikel durch betroffene Personen verbietet oder gar wirksam verhindert. Darüber hinaus sind betroffene Personen auch als Rezipient:innen der über sie veröffentlichten Artikel nicht von deren Nutzung ausgenommen. Es handelt sich also um das Angebot einer Dienstleistung, das sich jedenfalls zumindest auch an von der Veröffentlichung betroffene Personen richtet.

[226] Siehe JB 2016, 12.5
[227] Siehe Art. 3 Abs. 2 DS-GVO
[228] Siehe Art. 3 Abs. 2 lit. a DS-GVO

Gleichzeitig ist die Verarbeitung personenbezogener Daten in Wikipedia im Ergebnis zum größten Teil von der Geltung der DS-GVO ausgenommen. Insbesondere ist eine Kontrollkompetenz der Datenschutzbehörden nicht gegeben: Bei den Veröffentlichungen personenbezogener Daten in der Wikipedia handelt es sich grds. um eine Verarbeitung personenbezogener Daten für literarische Zwecke.[229] Zur Literatur zählen nicht nur Werke der Belletristik, sondern auch solche der Sachliteratur. Um ebensolche Sachliteratur handelt es sich bei der Online-Enzyklopädie Wikipedia. Voraussetzung dafür ist zwar ein gewisses Mindestmaß an literarischer Bearbeitung in dem jeweiligen Artikel. Jedoch ist der Begriff der „Verarbeitung personenbezogener Daten für literarische Zwecke“ weit auszulegen, um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen.[230]

Nach den Regelungen des Berliner Landesrechts gelten für die Verarbeitung personenbezogener Daten für literarische Zwecke nur einige wenige Bestimmungen der DS-GVO, die insbesondere die Verpflichtungen Verantwortlicher zu technischen und organisatorischen Maßnahmen und den ggf. zu leistenden Schadensersatz bei diesbezüglichen Verstößen zum Gegenstand haben. Zu den anwendbaren Bestimmungen zählt zwar auch das Recht betroffener Personen auf Beschwerde bei einer Aufsichtsbehörde für den Datenschutz[231]. Gleichzeitig findet aber das gesamte Kapitel der DS-GVO, das die Befugnisse der Aufsichtsbehörden regelt, auf die Verarbeitung personenbezogener Daten für literarische Zwecke keine Anwendung, sodass eine Kontrolle durch unsere Behörde in diesen Fällen nicht stattfinden kann.

Die derzeit geltenden Bestimmungen des Landesrechts erstrecken die genannten Ausnahmen ohne weitere Einschränkungen auf nicht-öffentliche Stellen[232]. Sie finden auch auf Verantwortliche Anwendung, die ihren Sitz in einem Drittland außerhalb der Europäischen Union haben.

Die Verarbeitung personenbezogener Daten betroffener Personen, die sich in der Europäischen Union befinden, in Artikeln der Wikipedia stellt

[229] Siehe Art. 85 Abs. 2 DS-GVO, § 19 Abs. 1 BlnDSG
[230] Siehe EG 153 Satz 7 DS-GVO
[231] Siehe Art. 77 Abs. 1 DS-GVO

[232] Siehe § 2 Abs. 7 Satz 1 BlnDSG

grds. eine Verarbeitung für literarische Zwecke dar und ist damit der Kontrolle durch die Aufsichtsbehörden entzogen.

15. Politische Parteien und Gesellschaft

15.1 Elektronischer Haustürwahlkampf

Seit 2017 setzt die CDU eine App für den Haustürwahlkampf ein. Unterstützer:innen sollen dort Hausbesuche bei potentiellen Wähler:innen dokumentieren und dabei Altersgruppe und Geschlecht der Person, mit der gesprochen wurde, deren Einstellung zur CDU und ob überhaupt die Tür geöffnet wurde, festhalten. Zeitweise gab es auch ein Freitextfeld für Anmerkungen. Automatisch dokumentiert die App Straße und Ort, also den ungefähren Standort des Wahlkampfeinsatzes. Freiwillig konnten und können die Bürger:innen weitere personenbezogene Daten für Informations- und Kontaktzwecke angeben. Im Mai wurde uns durch Meldung einer Sicherheitsforscherin bekannt, dass diese Daten unzureichend geschützt waren. Zudem waren die Daten der Hausbesuche anscheinend nicht so anonym wie geplant.

Bereits zur vorletzten Bundestagswahl setzte die CDU die App „Connect17“ für den Haustürwahlkampf ein. Die Unterstützer:innen sollten durch spielerische Elemente, sog. Gamification, animiert werden, sich möglichst aktiv am Wahlkampf zu beteiligen. So gab es für jeden dokumentierten Hausbesuch Punkte. Die jeweils 15 besten Unterstützer:innen auf den verschiedenen Ebenen (regional und bundesweit) konnte die App anzeigen.[233]

Schon damals kam es zu einer Datenpanne: Das Hintergrundsystem lieferte auf Anfrage nicht nur die besten fünfzehn Unterstützer:innen, sondern auf Wunsch bis zu tausend. Dafür musste nur der Internet-Link, den auch die App aufruft, um den Wert für die gewünschte Anzahl an Daten zu Unterstützer:innen zu ändern, aufgerufen werden. Für an Informatik interessierte Personen war es daher kein Problem, die von der App aufgerufenen Links zu ermitteln und mit anderen Programmen, im einfachsten Fall mit einem Webbrowser, aufzurufen. Wir sprachen bereits damals mit der CDU. Sie sagte zu, für einen angemessenen Schutz der Daten zu sorgen.

[233] Siehe JB 2017, 10.1

Nunmehr wurde wiederum eine Datenpanne bei der jetzt „CDU.Connect“ genannten App entdeckt.[234] Diese war wesentlich problematischer: Das Hintergrundsystem lieferte auf Grund des unsicheren Einsatzes einer Softwarekomponente praktisch beliebige Inhalte der gesamten Datenbank. Durch Beobachtung der Kommunikation der App mit dem Hintergrundsystem war es einfach zu erkennen, mit welchen Anfragen dies zu erreichen ist. In dem Artikel der Sicherheitsforscherin, die diese Sicherheitslücke entdeckt hat, wurden eindrückliche Beispiele der abrufbaren Einträge publiziert.

Die CDU hat unverzüglich, nachdem sie von der Datenpanne erfahren hat, das angreifbare Hintergrundsystem vorläufig stillgelegt und uns über den Sachverhalt informiert. Wir haben umfangreiche Nachfragen gestellt, wie es zu einer solchen Datenpanne kommen konnte. Zudem haben unsere Kolleg:innen vom Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit für uns in Amtshilfe bei dem damaligen Auftragsverarbeitungs- und Entwicklungsunternehmen eine Vorortprüfung durchgeführt und Unterlagen sichergestellt. Ebenso haben wir die Datenbankinhalte zu Beweiszwecken gesichert.

Die CDU hatte nach eigener Darstellung zum Zeitpunkt der Offenlegung der Datenpanne die Verarbeitung der Daten bereits an eine eigene Gesellschaft übertragen. Der bisherige Auftragsverarbeiter habe jedoch ohne Wissen der CDU noch eine Kopie der Daten gespeichert.

Insgesamt waren Datensätze von fast 20.000 Unterstützer:innen mit Namen, E-Mail-Adressen und Fotos sowie ca. 100.000 Datensätze von Hausbesuchen erfasst. Die Datensätze der 20.000 Unterstützer:innen sind dabei ganz klar besonders sensitive personenbezogene Daten, da hier Informationen zu politischen Überzeugungen offenbart werden.

Bei den Hausbesuchen ist die Lage nicht von vornherein so eindeutig: Die Daten durften nur unter der Voraussetzung erhoben werden, dass dies unter Wahrung der Anonymität der betroffenen Personen geschieht. Deswegen werden nicht der genaue Standort bzw. die Adresse gespeichert, sondern nur Ort und Straße. Bei den Gesprächen im Jahr 2017 wurde zudem vereinbart, dass Straßen mit wenigen Hausbesuchen nicht länger als einige Tage gespei-

[234] Blog-Artikel vom 12. Mai 2021; siehe https://lilithwittmann.medium.com/wenn-die-cdu-ihren-wahlkampf-digitalisiert-a3e9a0398b4d

chert und nicht für statistische Zwecke verarbeitet werden. Zudem wurde uns damals zugesagt, dass die Zeitpunkte der Hausbesuche nicht gespeichert würden, da man ansonsten den Laufweg des Unterstützenden nachvollziehen könne. Dies würde dazu führen, dass u. U. die Hausnummer zu einem Besuchseintrag bestimmt oder gar die betroffene Person identifiziert werden kann.

Die Auswertung der sichergestellten Daten zeigte nun, dass entgegen der Zusicherung die Einträge zu den Hausbesuchen sogar mehrere Zeitpunkte und zudem fortlaufende Nummern enthielten. Bei einigen Datensätzen enthielten die Freitextfelder auch -Namen, die vermutlich den Besuchten zuzuordnen sind. Im Ergebnis muss voraussichtlich davon ausgegangen werden, dass die Daten der Hausbesuche ebenfalls als personenbezogene Daten anzusehen sind. In diesem Fall wären sie zudem als besonders sensitiv einzuordnen, da Angaben zur Zustimmung zur CDU oder die Einträge im Freitext Rückschlüsse zur politischen Einstellung ermöglichen. Die Erhebung und die Speicherung dieser Daten über Jahre war unzulässig, da diese eben nicht (zuverlässig) anonymisiert wurden und keine Rechtsgrundlage für die personenbezogene Speicherung vorlag.

Sicherlich können Parteien zeitgemäße digitale Techniken für Parteiarbeit und Wahlkampf nutzen, wenn dies datenschutzgerecht geschieht. Es ist in Deutschland jedoch nicht zulässig, Profile über die Wählenden anzulegen, wie dies bspw. in den USA üblich ist. Daran halten sich die Parteien im Großen und Ganzen. Doch auch weniger umfassende Daten über Unterstützer:innen und Wählende brauchen Schutz. Daher müssen politische Parteien die erforderliche Sorgfalt walten lassen und konsequent Datenminimierung und Anonymisierung umsetzen.

15.2 Auch für gemeinnützige Organisationen gibt es Regeln für die E-Mail-Werbung

Regelmäßig erhalten wir Beschwerden über gemeinnützige Organisationen, die persönliche E-Mail-Adressen von Amtsträger:innen oder Unternehmer:innen im Internet recherchieren bzw. sammeln, um dann Einladungen zu ihren Veranstaltungen oder Informationen über ihre Arbeit zu verschicken.

Auf unsere Ansprache erwidern diese Organisationen häufig, es handele sich nicht um Werbung, sondern um die Erfüllung ihres Satzungszweckes. Als gemeinnützige Organisationen unterlägen sie nicht dem Gesetz gegen den unlauteren Wettbewerb (UWG). Dort ist die Zulässigkeit von E-Mail-

Werbung durch Anbieter:innen von Waren und Dienstleistungen geregelt.[235] Außerdem seien die E-Mail-Adressen, so die Organisationen, im Internet öffentlich gemacht worden.

Der Begriff der Werbung im Sinne der Datenschutz-Grundverordnung (DS-GVO) umfasst nicht nur die kommerzielle Werbung mit dem Ziel des Absatzes von Waren und Dienstleistungen, vielmehr fällt darunter auch die Kontaktaufnahme durch Parteien, Verbände und Vereine oder karitative und soziale Organisationen mit betroffenen Personen, um ihre Ziele bekannt zu machen oder zu fördern.[236] Auch die Einladung zu öffentlichen Veranstaltungen dient in der Regel der Bekanntmachung der Ziele einer Organisation.

Selbst wenn personenbezogene E-Mail-Adressen im Internet veröffentlicht sind, dürfen diese nur weiterverarbeitet werden, wenn dies auf einen gesetzlichen Erlaubnistatbestand gestützt werden kann. Für den oben geschilderten Sachverhalt kommt nur eine Verarbeitung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO in Betracht. Danach ist eine Datenverarbeitung zulässig, soweit sie zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Gemeinnützige Organisationen haben ein berechtigtes Interesse, ihre Arbeit bekannt zu machen. Der Versendung von Werbe-E-Mails zu diesem Zweck stehen jedoch regelmäßig die überwiegenden Interessen der betroffenen Personen entgegen.

Personen veröffentlichen ihre E-Mail-Adressen aus unterschiedlichen Gründen. Dies geschieht bspw. aufgrund der gesetzlichen Impressumspflicht[237] oder, um für Kund:innen erreichbar zu sein. Personen, die ihre Kontaktdaten aus beruflichen Gründen im Internet veröffentlichen (müssen), haben jedoch ein Interesse daran, dass diese Daten nur für Belange verwendet werden, für die sie auch veröffentlicht wurden.

Das Versenden von E-Mails mit unerbetener Werbung, die die Empfänger:innen jeweils einzeln sich-

[235] Siehe § 7 UWG

[236] Siehe Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO); abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-dsk

[237] Siehe § 5 Abs. 1 TMG

ten müssen und bei denen ein Widerspruch erforderlich ist, um eine weitere Zusendung zu unterbinden, führt zu einer nicht unerheblichen Belästigung. Für den Belästigungscharakter macht es keinen Unterschied, ob diese von einem kommerziellen Unternehmen versandt werden oder von einer gemeinnützigen Organisation, sodass die Grundsätze aus dem UWG auch auf andere Situationen übertragen werden können.[238] Danach stellen Werbe-E-Mails i. d. R. jedenfalls dann eine unzumutbare Belästigung dar, wenn zuvor kein Kontakt zwischen dem Werbenden und der betroffenen Person bestanden hat.[239]

Im Ergebnis stellen die Sammlung von E-Mail-Adressen im Internet zu Werbezwecken sowie die anschließende Nutzung für Werbe-E-Mails ohne die Einwilligung der betroffenen Personen regelmäßig eine unzulässige Datenverarbeitung dar. Wir haben gegen mehrere Organisationen wegen dieser Praxis eine Verwarnung ausgesprochen.

Auch gemeinnützige Organisationen dürfen grds. ohne Einwilligung keine Werbe- und Informations-E-Mails an personenbezogene E-Mail-Adressen, die sie im Internet gesammelt haben, versenden.

16 Europa, Zertifizierung

16.1 Neue Leitlinien des Europäischen Datenschutzausschusses

Der Europäische Datenschutzausschuss (EDSA) ist das Gremium der Aufsichtsbehörden der Mitgliedsstaaten der EU. Deutschland wird in dem Ausschuss und seinen Unterarbeitsgruppen durch Vertreter:innen der Aufsichtsbehörden des Bundes und der Länder repräsentiert. Der Ausschuss entscheidet bei strittigen Einzelfällen und stellt allgemeine Leitlinien, Empfehlungen und bewährte Verfahren bereit, um für Rechtsklarheit zu sorgen. Unsere Behörde vertritt in mehreren Unterarbeitsgruppen die Aufsichtsbehörden der Länder, die die Dokumente des Ausschusses vorbereiten.

Im vergangenen Jahr hat der EDSA mehrere wichtige Leitlinien verabschiedet. Da die Datenschutz-Grundverordnung (DS-GVO) technikneutral formuliert wurde, um auch einen rechtlichen Rahmen für neue Verarbeitungsformen zu bieten, besteht stetig ein Bedarf, die relativ allgemeinen Regelungen der DS-GVO für bestimmte Anwendungen zu konkreti-

[238] Siehe auch BGH, Urteil vom 14. März 2017 – VI ZR 721/15 m. w. N.
[239] Siehe § 7 Abs. 2 Nr. 3, Abs. 3 UWG

sieren. In diese Kategorie fallen insbesondere die Leitlinien zu virtuellen Sprachassistenten[240], die Leitlinien über die gezielte Ansprache von Nutzer:innen sozialer Medien[241] und die Leitlinien zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen.[242]

Andere Leitlinien betrafen datenschutzrechtliche Grundsatzfragen, wie z. B. die Leitlinien zu den Konzepten des Verantwortlichen und des Verarbeiters.[243] Diese enthalten wichtige Aussagen zur Rechtsfigur der gemeinsamen Verantwortung, welche durch die DS-GVO und die Rechtsprechung des Europäischen Gerichtshofs (EuGH) gesteigerte Bedeutung erlangt hat. Ebenfalls zu den Grundsatzfragen gehören die Leitlinien zu Art. 23 DS-GVO, die die Frage behandeln, unter welchen Umständen die Betroffenenrechte der DS-GVO eingeschränkt werden dürfen.[244] Auch von hoher Bedeutung ist die Empfehlung des EDSA zu Maßnahmen, die bei Datentransfers in Drittstaaten zu beachten sind. Damit reagiert der EDSA auf das Urteil des EuGH vom 16. Juli 2020 („Schrems II“).[245]

Hochumstritten waren die Leitlinien zum Begriff des maßgeblichen und begründeten Einspruchs[246] an welchen unsere Behörde als Berichterstatterin beteiligt war. Dabei geht es um einen wichtigen Teil des Kohärenzverfahrens. Dieses Verfahren wird ausgelöst, wenn sich die europäischen Aufsichtsbehörden in bestimmten grenzüberschreitenden Einzelfällen nicht einigen können und dient dazu, eine Lösung für diese Fälle zu finden. Leider wird das Verfahren von vielen europäischen Aufsichtsbehörden oft als allerletztes Mittel der Streitbeilegung verstanden, welches es unbedingt zu vermeiden gilt. Daher wurden die formalen Hürden für ein solches Verfahren in den Leitlinien sehr hoch gelegt. Wir haben uns bei der Erstellung der Leitlinien dafür eingesetzt, dass mehr Fälle in das Kohärenzverfahren kommen, um – i. S. d. DS-GVO – sicherzustellen, dass eine möglichst einheitliche Spruchpraxis der Aufsichts-

[240] Siehe https://edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf (englische Fassung)
[241] Siehe https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_targeting_of_social_media_users_de_0.pdf
[242] Siehe https://edpb.europa.eu/system/files/2021-08/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_de.pdf
[243] Siehe https://edpb.europa.eu/system/files/2021-07/eppb_guidelines_202007_controllerprocessor_final_en.pdf (englische Fassung)
[244] Siehe https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf (englische Fassung)
[245] Siehe 1.1
[246] Abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien

behörden in der EU entsteht. Wir konnten uns aber damit nur zum Teil durchsetzen.

Auch in diesem Jahr hat der EDSA zahlreiche wichtige Leitlinien erlassen. Soweit eine deutsche Übersetzung vorliegt, können diese und weitere Leitlinien grds. auf unserer Internetseite abgerufen werden.[247] Weitere Sprachversionen von Leitlinien des EDSA sind direkt auf dessen Internetseite abrufbar.[248]

16.2 Entwicklungen in der Servicestelle Europaangelegenheiten

Die DS-GVO sieht eine enge Zusammenarbeit zwischen den europäischen Aufsichtsbehörden vor. Dabei geht es insbesondere um Fälle, die eine grenzüberschreitende Verarbeitung personenbezogener Daten beinhalten. Unsere Behörde bearbeitet diejenigen Fälle federführend, in denen das für eine bestimmte Datenverarbeitung verantwortliche Unternehmen seinen Hauptsitz in Berlin hat. Befindet sich der Hauptsitz des Unternehmens in einem anderen Mitgliedsstaat der EU bzw. des EWR, übermitteln wir die bei uns eingegangenen Fälle an die insoweit federführenden Aufsichtsbehörden. Unsere interne Servicestelle Europaangelegenheiten agiert dabei als Scharnier zwischen den europäischen Aufsichtsbehörden und unseren Fachreferent:innen.

Nach Wirksamwerden der DS-GVO im Jahr 2018 bestand ein Schwerpunkt der Tätigkeit zunächst in der Feststellung der Federführung für spezifische Verantwortliche. Zudem mussten in den ersten Jahren grundsätzliche Fragen der Zusammenarbeit und der Ausgestaltung der dafür genutzten technischen Systeme[249] geklärt werden. Nachdem die grundlegendsten Strukturen gebildet waren, konnten vermehrt Fälle zur Abstimmung in das Kooperationsverfahren[250] gegeben werden.[251]

Unsere Behörde hat auch im Berichtszeitraum wieder zu einer Vielzahl der zwischen den europäischen Aufsichtsbehörden abstimmungsbedürftigen Fragen Stellung genommen. Wir haben die Beschlussentwürfe anderer federführender Aufsichtsbehörden gesichtet und bei abweichenden Positionen Einspruch eingelegt. Auf diesem Wege haben wir inhaltliche Aspekte in die Verfahren eingebracht, die teilweise anschließend in den überarbeiteten Be-

[247] Siehe https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/leitlinien
[248] Siehe https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_de
[249] Siehe Art. 60 Abs. 12 DS-GVO
[250] Siehe Art. 60 DS-GVO
[251] Siehe auch JB 2020, 17.2

schlussentwürfen und in den endgültigen Beschlüssen berücksichtigt wurden. Außerdem haben wir natürlich auch eigene Beschlussentwürfe im -Kooperationsverfahren zur Diskussion gestellt. In vierzehn Fällen konnten wir im Konsens mit den betroffenen Aufsichtsbehörden endgültige Beschlüsse erlassen und somit Klarheit für betroffene Personen und Verantwortliche schaffen.

Kann zwischen den betroffenen Behörden und der federführenden Aufsichtsbehörde kein Einvernehmen hergestellt werden, ist ein Streitbeilegungsverfahren[252] vor dem EDSA vorgesehen. Der EDSA besteht aus den Leitungspersonen aller europäischen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten.[253] Die deutschen Aufsichtsbehörden werden von der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie einer Stellvertreterin bzw. einem Stellvertreter aus den Ländern vertreten.[254] Diese Konstruktion erfordert eine der EDSA-Entscheidung vorgelagerte deutschlandinterne Abstimmung.[255]

Die DS-GVO sieht vor, dass der EDSA am Ende eines Streitbeilegungsverfahrens verbindliche Beschlüsse erlässt. Allerdings hat sich in der Praxis gezeigt, dass der EDSA keine eigenen Entscheidungen zu Beschwerden trifft. Vielmehr überprüft er den Beschluss der federführenden Aufsichtsbehörde ausschließlich anhand der eingegangenen maßgeblichen und begründeten Einsprüche, soweit sich die federführende Behörde den Einsprüchen nicht angeschlossen hat.

Unsere Behörde hat im Berichtszeitraum ein Streitbeilegungsverfahren vor dem EDSA selbst betrieben und somit Pionierarbeit geleistet. Es war eines der ersten Streitbeilegungsverfahren, mit dem der EDSA überhaupt konfrontiert war. Anlass war eine in Berlin eingelegte Beschwerde gegen einen Online-Shop mit Sitz in Spanien. Wegen der Niederlassung des Verantwortlichen in Spanien war der Fall zur federführenden Bearbeitung an die spanische Aufsichtsbehörde abzugeben. Das Kooperationsverfahren wurde durchgeführt. Die spanische Aufsichtsbehörde legte uns als betroffener Aufsichtsbehörde einen Beschlussentwurf und in Folge unserer Einwendungen überarbeitete Beschlussentwürfe zu der Beschwerde vor.

[252] Siehe Art. 65 DS-GVO; Zur Anwendung des Art. 65 Abs. 1 lit. a DS-GVO hat der EDSA Leitlinien erlassen: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_032021_article65-1-a_ en. pdf (englische Fassung)
[253] Art. 68 Abs. 3 DS-GVO
[254] § 17 Abs. 1 Satz 1, 2 Bundesdatenschutzgesetz (BDSG)
[255] Siehe § 18 BDSG

Bezüglich mehrerer Datenschutzverstöße und der angemessenen Rechtsfolge konnte allerdings trotz starker Bemühungen, z. B. im Rahmen von Vermittlungsgesprächen, keine Einigung mit der spanischen Aufsichtsbehörde erzielt werden. Wir legten jeweils Einsprüche gegen die Beschlussentwürfe ein, denen sich Spanien überwiegend nicht anschloss. Daraufhin wurde das Streitbeilegungsverfahren eingeleitet.

In einer Arbeitsgruppe des EDSA erfolgte eine Diskussion des Falles in einem größeren Kreis der europäischen Aufsichtsbehörden. Dort wurde eine informelle Streitbeilegung erzielt. Danach verhängte die spanische Aufsichtsbehörde statt der ursprünglich vorgesehenen Verwarnung ein Bußgeld gegen den Online-Shop. Wegen der informellen Einigung in wesentlichen Kritikpunkten kam es nicht zu einem förmlichen Beschluss des EDSA. Im Ergebnis konnte durch die Diskussion und die informelle Streitbeilegung Klarheit geschaffen und der Datenschutz für betroffene Personen gestärkt werden.

Wir haben unser erstes Streitbeilegungsverfahren intensiv ausgewertet. In einem Arbeitskreis der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) haben wir eine Auswertung auch gemeinsam mit anderen deutschen Aufsichtsbehörden veranlasst. Denn bisher konnten nur einzelne Aufsichtsbehörden als aktiv Beteiligte Erfahrungen mit Streitbeilegungsverfahren sammeln. Zukünftig werden diese Verfahren in der Praxis der Aufsichtsbehörden eine größere Rolle spielen. Dies ist gdrs. zu begrüßen, da das Streitbeilegungsverfahren ein Baustein des Kohärenzmechanismus der DS-GVO darstellt. Dieser Mechanismus beabsichtigt eine europaweit einheitliche, ordnungsgemäße Anwendung der DS-GVO.

16.3 Neues zu Akkreditierung und Zertifizierung

Um die Transparenz zu erhöhen und die Einhaltung der DS-GVO zu erleichtern, wurden mit der DS-GVO Zertifizierungsverfahren eingeführt, die den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen ermöglichen sollen. Im Rahmen von Zertifizierungsverfahren wird der sog. Zertifizierungsgegenstand auf die Einhaltung von vorher festgelegten Zertifizierungskriterien geprüft. Diese Kriterien sind ein wesentlicher Teil von Zertifizierungsprogrammen und müssen vor ihrem Einsatz in der Praxis von der zuständigen Aufsichtsbehörde geprüft und genehmigt werden. Die deutschen Aufsichtsbehörden haben gemeinsame Anforderungen

an datenschutzrechtliche Zertifizierungsprogramme erarbeitet. Das dabei erstellte Dokument[256] *bildet die Basis für die Genehmigung der Zertifizierungskriterien durch die jeweils zuständige Aufsichtsbehörde.*

Zur Vorbereitung einer Akkreditierung müssen die Zertifizierungsstelle oder die Programmeigner:innen[257] ein Zertifizierungsprogramm erstellen und durch die Deutsche Akkreditierungsstelle (DAkkS) auf Eignung prüfen lassen. Wesentlicher Teil eines solchen Zertifizierungsprogramms sind die Zertifizierungskriterien zur Umsetzung der –datenschutzrechtlichen Anforderungen. Diese Kriterien prüft und genehmigt ggf. die zuständige Aufsichtsbehörde.[258]

Die DSK hat in ihrer Frühjahrssitzung „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ verabschiedet. Das Dokument soll den deutschen Aufsichtsbehörden bei der Bewertung von Zertifizierungsprogrammen als einheitliche Bewertungsgrundlage dienen. Programmeignern sowie Zertifizierungsstellen steht es bei der Erstellung ihrer Dokumente als Orientierungshilfe zur Verfügung.

Unsere Behörde hat sich intensiv an der Erarbeitung der „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ beteiligt. Aktuell liegen ihr zwei Anträge auf Genehmigung von Zertifizierungskriterien vor. Beide beschäftigen sich mit Auftragsverarbeitung. Für Auftragsverarbeiter:innen sind Zertifizierungen besonders interessant, um die von der DS-GVO geforderten Garantien hinsichtlich der Datenschutzkonformität zu erbringen. Wir prüfen die in Zertifizierungsprogramme eingebetteten Zertifizierungskriterien anhand der einheitlichen Anforderungen.

Es liegt ein ausführliches Papier der Aufsichtsbehörden vor, das die grundlegenden Anforderungen an Zertifizierungsprogramme beschreibt. Angehende Zertifizierungsstellen und Programmeigner:innen können mithilfe dieses Dokuments prüfen, ob sich ihre Programme und insbesondere die Zertifizierungskriterien für eine Genehmigung durch die Auf-

[256] Siehe https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/themen-a-z/a/2021-DSK-Anwendungshinweis_Zertifizierungskriterien.pdf

[257] Eine Stelle, die nicht selbst zertifizieren möchte, aber ein Zertifizierungsprogramm und -kriterien erstellt, z. B. aufgrund besonderer Datenschutzexpertise in einem bestimmten Bereich

[258] Siehe Art. 57 Abs. 1 lit. n DS-GVO i. V. m. Art. 42 Abs. 5 Satz 1 DS-GVO. Werden die Kriterien vom EDSA genehmigt, kann dies zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen (Art. 42 Abs. 5 Satz 2 DS-GVO).

sichtsbehörde eignen. Damit ist unsere Aufgabe im Zertifizierungsbereich jedoch nicht abgeschlossen. Liegen auf Eignung geprüfte Zertifizierungsprogramme und genehmigte Kriterien vor, werden wir bei entsprechenden Anträgen gemeinsam mit der DAkkS Akkreditierungsverfahren durchführen. Dabei werden angehende Zertifizierungsstellen anhand von festgelegten Kriterien auf Herz und Nieren geprüft.[259] An die Akkreditierungsphase und die Befugniserteilung durch die Aufsichtsbehörden schließt sich eine Überwachungsphase sowohl hinsichtlich der Akkreditierungen als auch hinsichtlich der Zertifizierungen an.[260]

17 Informationsfreiheit

17.1 Entwicklungen in Deutschland

17.1.1 Ergebnisse der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

In diesem Jahr tagte die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) turnusgemäß unter dem Vorsitz des Landesbeauftragten für den Datenschutz und für die Informationsfreiheit Sachsen-Anhalt zweimal. Beide Sitzungen waren ertragreich: Es wurden insgesamt sechs Entschließungen gefasst, die Forderungen nach mehr Transparenz in ganz unterschiedlichen Bereichen beinhalten. So fordert die IFK die Gesetzgeber in Bund und Ländern auf, den Zugang zu Informationen auch bei den Verfassungsschutzbehörden zu gewährleisten und Ausnahmeregelungen auf den Schutz konkreter Sicherheitsbelange zu beschränken.[261] In einer weiteren Entschließung wird für die Einführung von behördlichen Informationsfreiheitsbeauftragten plädiert, damit in der jeweiligen Behörde eine kompetente Ansprechperson zu Verfügung steht, die Informationszugangsbegehren koordiniert, rechtskundig berät und Unterstützung anbietet.[262] An den neuen Bundesgesetzgeber richtet sich ein Zwölf-Punkte-Papier, mit dem die IFK Vorschläge zur Weiterentwicklung des Informationsfreiheitsgesetzes in ein Transparenzgesetz mit einem Transparenzregister, aber auch zu mehr Eingriffsbefugnissen des Bundesbeauftragten für den Daten-

[259] Siehe JB 2020, 1.5
[260] Siehe zum Akkreditierungsprozess https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/themen-a-z/a/2020-DSK-Grafik-Akkreditierungsprozess.pdf
[261] Mehr Transparenz beim Verfassungsschutz – Vertrauen und Legitimation stärken!, abrufbar unter https://www.daten-schutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit
[262] Mehr Transparenz durch behördliche Informationsfreiheitsbeauftragte!, abrufbar unter https://www.daten-schutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit

schutz und die Informationsfreiheit macht.[263] Ebenfalls an den neuen Bundesgesetzgeber ist die Forderung adressiert, die EU-Richtlinie zum Schutz von Personen, die Verstöße gegen Unionsrecht melden, so schnell wie möglich umzusetzen und dabei den Schutz auch auf Hinweisgebende zu erstrecken, die Verstöße gegen nationales Recht melden.[264] Schließlich spricht sich die IFK auch dafür aus, dass in Deutschland endlich ein einheitlicher Mindeststandard für den Zugang zu Informationen geschaffen wird, was durch die Ratifizierung der sog. Tromsø-Konvention, eine Konvention des Europarates über den Zugang zu amtlichen Dokumenten aus dem Jahr 2009, erreicht werden soll.[265] Eine zusätzliche Vereinheitlichung in Deutschland würde dadurch erreicht, dass alle Landesbeauftragten für Informationsfreiheit die Beratungs- und Kontrollkompetenz für die jeweiligen Landesbehörden auch in Bezug auf das Umweltinformationsrecht erhalten,[266] so wie es seit März bereits für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in Bezug auf die Bundesbehörden normiert ist.[267]

17.1.2 Neue Bundesgesetzgebung

Mit dem Gesetz zur Änderung des E-Government-Gesetzes und zur Einführung des Gesetzes für die Nutzung von Daten des öffentlichen Sektors (Datennutzungsgesetz – DNG)[268] wurde die Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors umgesetzt.[269]

Das Änderungsgesetz, das auch als Zweites Open-Data-Gesetz bezeichnet wird, regelt die Pflicht zur Bereitstellung unbearbeiteter maschinenlesbarer Daten durch alle Bundesbehörden, also auch durch die mittelbare Bundesverwaltung mit Ausnahme der Selbstverwaltungskörperschaften und Beliehenen, und sieht zudem die Einrichtung von Open-Data-

[263] Forderungen für die neue Legislaturperiode des Bundes: Ein Transparenzgesetz mit Vorbildfunktion schaffen!, abrufbar unter https://www.daten-schutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit

[264] EU-Richtlinie zum Whistleblowerschutz zeitnah umsetzen! Hinweisgeberinnen und Hinweisgeber umfassend und effektiv schützen!, abrufbar unter https://www.daten-schutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit

[265] Tromsø-Konvention ratifizieren und einheitlichen Mindeststandard für den Zugang zu Informationen in ganz Deutschland schaffen!, abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit

[266] Umweltinformationen: Beratungs- und Kontrollkompetenz auch auf Landesbeauftragte für Informationsfreiheit übertragen!, abrufbar unter https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/beschluesse-informationsfreiheit

[267] Siehe § 7a Umweltinformationsgesetz (UIG)

[268] Siehe Gesetz vom 16. Juli 2021, BGBl. I, S. 2941 ff.

[269] ABl. L 172 vom 26. Juni 2019, S. 56 ff.

Koordinator:innen vor. Das DNG hat das Informationsweiterverwendungsgesetz (IWG) von 2006 abgelöst und gilt nicht nur für den Bund, sondern auch für die Länder. Es bestimmt, dass bereitgestellte Daten zu privaten oder kommerziellen Zwecken genutzt werden können, begründet aber selbst keine Bereitstellungspflicht und auch keinen Anspruch auf Zugang zu Daten.

Unter dem Eindruck der sog. Maskenaffäre, bei der im Frühjahr mehreren Bundestagsabgeordneten vorgeworfen worden war, sie hätten für die Vermittlung des Kaufs von Corona-Schutzmasken durch die Bundesregierung von ausgewählten Unternehmen Provisionen erhalten, verabschiedete der Bundestag zugunsten von mehr Transparenz das Gesetz zur Einführung eines Lobbyregisters[270]. Hier sind die Interessenvertretungen ggü. dem Deutschen Bundestag und ggü. der Bundesregierung ab dem 1. Januar 2022 einzutragen und öffentlich einsehbar.

17.2 Entwicklungen im Land Berlin

17.2.1 Neue Landesgesetzgebung — Erfolge und Misserfolge

Auch in Berlin wurde ein Lobbyregistergesetz verabschiedet.[271] Es sieht die Einrichtung eines öffentlichen Registers beim Abgeordnetenhaus vor, in das die inhaltliche Beteiligung von Externen an Gesetzgebungsverfahren eingetragen werden soll. Im Hinblick auf die dadurch gesteigerte Transparenz im politischen Raum begrüßen wir das Gesetz. Allerdings bedauern wir, dass entgegen unserer Empfehlung und anders als im neuen Bundesgesetz[272] keine Bußgeldvorschriften aufgenommen wurden, mit denen unterbliebene Meldungen sanktioniert werden können. Nur dann ist aber ein verpflichtendes Lobbyregister erfolgversprechend.

Ein Gesetzesvorhaben zur Stärkung der Verbraucher:inneninformation, über das wir im letzten Jahr berichtet hatten,[273] wurde erfreulicherweise umgesetzt: Das Gesetz zur Transparenzmachung von Ergebnissen amtlicher Kontrollen in der Lebensmittelüberwachung[274] wurde verabschiedet und wird am 1. Januar 2023 in Kraft treten. Damit ist es allen Verbraucher:innen möglich, sich über den Hygienezustand eines Lebensmittelbetriebes bereits vor des-

[270] Gesetz zur Einführung eines Lobbyregisters für die Interessenvertretung ggü. dem Deutschen Bundestag und ggü. der Bundesregierung (Lobbyregistergesetz – LobbyRG)
[271] Gesetz über die Einführung des Lobbyregisters beim Abgeordnetenhaus (Lobbyregistergesetz – BerlLG)

[272] Siehe § 7 LobbyRG
[273] JB 2020, 19.2.3
[274] Lebensmittelüberwachungstransparenzgesetz (LMÜTranspG)

sen Betreten zu informieren.

Wir haben im letzten Jahr ausführlich über den Entwurf eines Berliner Transparenzgesetzes (BlnTranspG) berichtet, zu dem das „antiquierte" Berliner Informationsfreiheitsgesetz (IFG) von 1999 laut Koalitionsvereinbarung von 2016 weiterentwickelt werden sollte.[275] Unsere massive Kritik an dem Gesetzentwurf, die insbesondere die zahlreichen, ausufernden Bereichsausnahmen betraf, hat leider nicht „gefruchtet", denn der Gesetzentwurf wurde nahezu unverändert in das Abgeordnetenhaus eingebracht.[276] Hierzu fand zwar eine Ausschuss-Anhörung mit externen Sachverständigen statt, in der diese noch weitere Kritikpunkte zum Gesetzentwurf vorgebracht haben.[277] Leider wurde diese Anhörung aber nicht ausgewertet; die Abgeordneten haben den Gesetzentwurf im Ausschuss inhaltlich nicht beraten. Grund hierfür war dem Vernehmen nach, dass sich die drei Regierungsfraktionen nicht über die Streichung von Bereichsausnahmen verständigen konnten. Deshalb ist dieses Gesetzesvorhaben schließlich ebenso gescheitert wie schon ein früherer Entwurf der oppositionellen FDP-Fraktion für ein - Berliner Transparenzgesetz (BlnTG).[278]

Zu dem Antrag von zivilgesellschaftlichen Organisationen wie dem Mehr Demokratie e. V. und dem Open Knowledge Foundation Deutschland e. V. auf Einleitung des Volksbegehrens „Einführung eines Berliner Transparenzgesetzes" [279] hat der Hauptausschuss zu Beginn der neuen Legislaturperiode im Herbst die gesetzlich vorgesehene Anhörung der Vertrauenspersonen durchgeführt.[280] Nach Beratung im Plenum wurde das von der Verfassung von Berlin und dem Abstimmungsgesetz vorgesehene - Verfahren fristgerecht abgeschlossen.[281] Einen Beschluss zur Annahme oder ausdrücklichen Ablehnung des Volksbegehrens hat das Abgeordnetenhaus nicht gefasst. Der neue Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und Die Linke sieht aber vor, im Jahr 2022 ein Transparenzgesetz nach Hamburger Vorbild einzuführen und dabei die hohen Standards des Berliner Informationsfreiheitsgesetzes zu erhalten.

[275] JB 2020, 19.2.2
[276] Siehe Abghs.-Drs. 18/3458 vom 3. März 2021
[277] Siehe Punkt 2 der Tagesordnung im Wortprotokoll des Ausschusses für Kommunikationstechnologie und Datenschutz (KTDat), Sitzung vom 17. Mai 2021, https://www.parlament-berlin.de/ados/18/KTDat/ protokoll/ktd18-040-wp.pdf
[278] Siehe Abghs.-Drs. 18/1595 vom 16. Januar 2019
[279] Antrag vom 3. Dezember 2019, Abghs.-Drs. 18/4044 (alt), Abghs.-Drs. 19/0003 (neu)
[280] § 17a Abs. 1 Gesetz über Volksinitiative, Volksbegehren und Volksentscheid (Abstimmungsgesetz – AbstG)
[281] Art. 62 Abs. 3, Art. 63 VvB, § 17a AbstG

Die Schaffung eines Berliner Transparenzgesetzes, das seinem Namen gerecht wird, bleibt das vordringlichste Thema im Bereich der Informationsfreiheit. Wir hoffen, dass dies von der neuen Landesregierung und den neuen Regierungsfraktionen ebenfalls so gesehen wird.

17.2.2 Erhöhtes Beschwerdeaufkommen — Auch massiver struktureller Defizite in einigen Verwaltungen

Uns erreichten verstärkt Beschwerden, denen wir in unserer Funktion als Schiedsstelle[282] nachgehen. Die Zahl der neuen Fälle lag bei 132 ggü. 57 im Vorjahr, was eine Zunahme um 132 Prozent bedeutete. Ein negatives Bild bei der Bearbeitung – auch: Nichtbearbeitung – von IFG-Anträgen haben insbesondere zwei Verwaltungen hinterlassen: 27 Eingaben betrafen den Geschäftsbereich der Polizei wegen nicht erfolgter, verspäteter bzw. unzureichender Reaktion auf Antragsgegenstände wie die Anlage zu einer konkreten Geschäftsanweisung, Schulungs- und Informationsmaterialien, Einsatzberichten oder Teilnehmendenzahlen bei Demonstrationen, die Anzahl von Suspendierungen/Entlassungen und die Zusammenarbeit mit ausländischen Polizeibehörden.

Um dem dargestellten Problem zu begegnen und eine sachgerechte und zeitnahe Bearbeitung der Anträge nach dem IFG Bln durch die Polizei zu gewährleisten, wurde zum 1. August 2021 ein eigener Bereich (PPr Just 43) innerhalb der Polizei Berlin geschaffen, der ausschließlich IFG-Anträge bearbeitet. Der Rückstau nicht bearbeiteter Anträge konnte von dort bereits weitgehend abgearbeitet werden.

Allein acht Fälle betrafen die für Gesundheit zuständige Senatsverwaltung, bei der IFG-Anträge im Zusammenhang mit der Corona-Pandemiebekämpfung eingingen; so betreffend den Vertrag und die Kosten für die Nutzung der Luca App, Unterlagen zur Vergabe des Impftermin-Buchungsportals an Doctolib, die Vergabe „test to go Berlin“, den Datenschutz und die Datensicherheit bei „test to go Berlin“ und eventuelle Qualitätsmängel in Testzentren.

Die für Gesundheit zuständige Senatsverwaltung ist die Senatsverwaltung, die während der aktuellen COVID-19-Pandemie seit über 2,5 Jahren im besonderen Maße belastet war. Die Beschäftigten der Senatsverwaltung für Gesundheit, Pflege und Gleichtstellung und hierbei insbesondere das im sog. Corona-Krisenstab eingesetzte Personal übernahm im Wesentlichen federführend die Planung, Koordination und Umsetzung der für die Bewältigung der CO-VID-19-Pandemie erforderlichen Maßnahmen für das Land der Berlin wie etwa die Corona-Verordnungsgebung, Prüfung von (Rahmen)Hygienekonzepten oder die Koordination und Umsetzung der Berliner Impfkampagne. Dies führte dazu, dass aufgrund der Anfragen und Arbeitsaufträge eine Priorisierung der Vorgänge zwingend erforderlich wurde und damit zugleich eine Verzögerung bei der Bearbeitung anderer Vorgänge und Anfragen einherging. Zudem war ein Teil des Personals für die Aufgabenwahrnehmung im Krisenstabs abgeordnet, so dass Vorgänge infolge von Personalwechsel nicht konstant betreut werden konnten.

[282] Siehe § 18 IFG

Hier wie auch in anderen Vermittlungsfällen, in denen wir – trotz zahlreicher Erinnerungen – keine für die antragstellenden Personen zufriedenstellende Antwort erreicht haben, konnten wir mangels Anordnungs- oder Sanktionsbefugnissen den Petent:innen leider keine andere Empfehlung geben, als zur Durchsetzung ihres Bescheidungsanspruchs eine sog. Untätigkeitsklage beim Verwaltungsgericht Berlin zu erheben.[283]

Zur Vermeidung dieser unbefriedigenden Situation werden wir dafür eintreten, dass unsere Behörde künftig die gesetzliche Befugnis erhält, die Beseitigung von Gesetzesverstößen anzuordnen und die Offenlegung der Informationen verlangen zu können. Diese Kompetenzerweiterung würde die Bedeutung der Transparenz des Wissens und Handelns öffentlicher Stellen zusätzlich stärken und unserer Behörde im Bedarfsfall mehr Durchsetzungskraft verleihen.

Zu Recht unterliegt im Übrigen auch unsere Behörde, die für die Informationsfreiheit eintritt, dem IFG. Wir erhielten 55 Anträge auf Aktenauskunft bzw. Akteneinsicht (ggf. durch Übersendung von Kopien), eine Steigerung um 72 % ggü. 32 Anträgen im Vorjahr. Die Antragsgegenstände betrafen Zahlen zu Sanktionen, Meldungen von Datenpannen, Datenschutzbeschwerden, Prüfverfahren sowie Bußgeldbescheiden.

Der Zugang zu amtlichen Informationen wird auch 22 Jahre nach Inkrafttreten des IFG in den Verwaltungen oft nur unzureichend umgesetzt. Das muss sich dringend ändern – und die Erkenntnis hierzu sollte auch und insbesondere auf Leitungsebene wachsen.

17.2.3 Einzelfälle

17.2.3.1 Senatskanzlei erfragt Postanschrift zu früh

Ein Petent hatte bei der Senatskanzlei per E-Mail die Übersendung der „Protokolle und sonstigen Unterlagen zur Konferenz der Regierungschef:innen der Länder mit der Bundeskanzlerin zur Bewältigung der Covid19-Pandemie im Jahr 2020“ beantragt. Hierauf teilte ihm die Senatskanzlei Folgendes mit: „Da die Anfrage einen langen Zeitraum betrifft, rechne ich – ohne geprüft zu haben, ob es die von Ihnen angefragten Unterlagen hier gibt – überschlägig mit Gebühren im dreistelligen Eurobereich …“. Für einen Gebührenbescheid würde zudem eine

[283] Siehe § 75 Verwaltungsgerichtsordnung (VwGO)

Postanschrift benötigt; Name und E-Mail-Adresse seien nicht ausreichend. Ohne die Postanschrift würde sein Antrag nicht weiterbearbeitet.

Wir haben die Senatskanzlei darauf hingewiesen, dass der Petent seine personenbezogenen Daten nur in dem Umfang offenbaren muss, wie es für die Bearbeitung seines Begehrens erforderlich ist. Das bedeutet, dass bei Nichtvorhandensein der Unterlagen eine einfache Antwort per E-Mail ausreicht. Weitere personenbezogene Daten wie die Postanschrift sind für diese Kurzmitteilung nicht erforderlich. Deshalb musste zunächst das (Nicht-)Vorhandensein der Unterlagen durch eine kurze Rückfrage im Haus ermittelt werden. Denn laut Mitteilung an den Petenten wurde gerade dies noch nicht geprüft, aber dennoch dem Petenten (insofern widersprüchlich) als Kostenschätzung ein dreistelliger Betrag – also ein Betrag zwischen 100,00 Euro und 500,00 Euro – als Gebühr in Aussicht gestellt.[284]

Darüber hinaus haben wir der Senatskanzlei aber mitgeteilt, dass wir ihre Auffassung teilen, nach der für die ordnungsgemäße Zustellung eines (Gebühren-)Bescheides eine zustellungsfähige Postanschrift mitgeteilt werden muss. Auch haben wir vor dem Hintergrund, dass Berlin den Vorsitz in der besagten Konferenz hatte und es demzufolge Unterlagen dazu geben muss, empfohlen, dem Petenten einen Nachtrag zu schicken.

Hier wäre ihm mitzuteilen, dass die gewünschten Dokumente im Umfang von z. B. einem DIN A4-Ordner oder von soundsoviel Blatt (ggf. geschätzt) im Haus vorhanden sind, aber auf nach dem IFG zu schützende Daten[285] überprüft und u. U. entsprechend geschwärzt werden müssen. Die Offenlegung der hiernach verbliebenen Informationen[286] würde voraussichtlich eine Gebühr in Höhe von – derzeit geschätzt – ca. soundsoviel Euro nach sich ziehen. Vor diesem Hintergrund möge der Petent mitteilen, ob er die Weiterbearbeitung seines Antrags mit der Folge der gebührenpflichtigen Offenlegung der nach Schwärzung verbliebenen Informationen wünscht, und in diesem Fall eine zustellungsfähige Postanschrift senden. Andernfalls würde sein Antrag nicht weiterbearbeitet werden.

[284] Die Rahmengebühr liegt zwischen 5,00 Euro und 500,00 Euro, siehe Tarifstelle 1004 des Gebührenverzeichnisses der Verwaltungsgebührenordnung (VGebO); abrufbar unter https://www.datenschutz-berlin.de/informationsfreiheit/rechtliche-grundlagen/gebuehren

[285] Hier primär nach § 10 Abs. 3 IFG

[286] Siehe § 12 IFG

Die Senatskanzlei hat diese Hinweise aufgegriffen.

Bei dem beanstandeten Verfahren war die Formulierung der Senatskanzlei hinsichtlich des Vorliegens der angefragten Unterlagen und der zu erwartenden Kosten ungenau. Die Senatskanzlei wird die Hinweise der Berliner Beauftragten für Datenschutz und Informationsfreiheit in Zukunft berücksichtigen.

Das skizzierte Verfahren kann von allen öffentlichen Stellen genutzt werden, die elektronisch gestellte IFG-Anträge von Personen erhalten, die ihren Namen und/oder ihre Postanschrift nicht mitteilen.

17.2.3.2 Stellungnahmen der Senatsverwaltung für Finanzen an den Petitionsausschuss

Eine Bürgerin hatte sich mit einer Beschwerde an den Petitionsausschuss des Abgeordnetenhauses gewandt. Entsprechend dem üblichen Verfahren bat der Petitionsausschuss die betroffene Verwaltung, hier die Senatsverwaltung für Finanzen, zu der Beschwerde Stellung zu nehmen. Die Petentin verlangte sodann Kopien dieser Stellungnahme(n), zunächst vom Petitionsausschuss, später von der Senatsverwaltung für Finanzen. Beide Stellen lehnten dies ab.

Wir haben die Senatsverwaltung für Finanzen auf Gerichtsentscheidungen hingewiesen, nach denen auf der Grundlage des Informationsfreiheitsrechts ein Offenlegungsanspruch von Petent:innen ggü. derjenigen Verwaltung besteht, die ggü. dem parlamentarischen Petitionsausschuss Stellung genommen hat.[287] Die Senatsverwaltung für Finanzen hat daraufhin der Petentin die Stellungnahmen übersandt.

Nach neuester Rechtsprechung des Europäischen Gerichtshofs (EuGH) ist auch ein parlamentarischer Petitionsausschuss zur Offenlegung der an ihn gerichteten Stellungnahme der Verwaltung ggü. betroffenen Petent:innen verpflichtet (wenngleich aufgrund von Datenschutzrecht).[288]

Stellungnahmen von Verwaltungen ggü. dem Petitionsausschuss dürfen ggü. den Petent:innen nicht geheim gehalten werden. Diese können ggü. beiden Stellen ihren Anspruch auf Offenlegung geltend machen.

[287] Siehe OVG Berlin, Beschluss vom 18. Oktober 2000 – 2 M 15/00; BVerwG, Urteil vom 3. November 2011 – 7 C 4/11

[288] EuGH, Urteil vom 9. Juli 2020 – Rs. C-272/19; und hiernach VG Wiesbaden, Urteil vom 31. August 2020 – 6 K 1016/15.WI

17.2.3.3 Für Bildung zuständige Senatsverwaltung fordert Umwege bei IFG-Anträgen

Ein Petent wollte von der für Bildung zuständigen Senatsverwaltung wissen, wer – wenn nicht die von ihm konkret bezeichnete Abteilung – die Verantwortung dafür trägt, dass das Videokonferenztool Webex als eLearning-Tool für das Unterrichten im virtuellen Klassenraum nicht mehr genutzt werden darf. Hierauf teilte ihm die Senatsverwaltung zunächst mit, dass für einen Antrag auf Auskunft nach dem IFG der „Dienstweg" nötig sei. Nachdem der Petent insistiert hatte, teilte ihm die Senatsverwaltung Folgendes mit: „Nach Rücksprache mit verschiedenen Stellen hier im Hause kann ich Ihnen mitteilen, dass Sie für Ihre Anfrage gemäß IFG bitte eines der beiden folgenden Portale wählen können: https://fragdenstaat.de/,https://www.parlament-berlin.de/das-parlament/petitionen/online-petition. Auf diese Weise ist gewährleistet, dass Sie eine Antwort der Staatssekretärin für Bildung … oder der zuständigen Stelle in der Senatsverwaltung … erhalten."

Wir haben der Senatsverwaltung mitgeteilt, dass die Voraussetzungen für einen zulässigen IFG-Antrag in § 13 Abs. 1 IFG normiert sind. Danach ist nicht vorgesehen, dass hierfür „der Dienstweg" nötig ist. Ebenso wenig normiert das IFG, dass ein Antrag auch bei fremden Portalen gestellt werden kann.[289] Vielmehr ist der Antrag mündlich, schriftlich oder elektronisch bei der öffentlichen Stelle zu stellen, die die Akte führt.[290] Sofern eine andere Stelle als die adressierte zuständig sein sollte, ist die Weiterleitung des Antrages von dort an die zuständige Stelle zu veranlassen.[291]

Offenbar hat die zuständige Stelle in der Senatsverwaltung erkannt, dass die dem Petenten empfohlenen Umwege keine adäquaten Mittel sind, dem Auskunftsantrag zu begegnen, denn sie hat ihm schließlich stattgegeben.

Die Stellung eines IFG-Antrages darf durch die Verwaltung nicht erschwert werden.

[289] Ohnehin ist das u. a. empfohlene Portal des Petitionsausschusses im Abgeordnetenhaus – wie der Name nahelegt – nur für Petitionen (Beschwerden) nutzbar, nicht aber als Eingangsinstanz für IFG-Anträge, die sich an andere Stellen als den Petitionsausschuss richten.
[290] § 13 Abs. 1 Satz 1 IFG
[291] § 13 Abs. 1 Satz 4 IFG

17.2.3.4 Für Bildung zuständige Senatsverwaltung reklamiert Bereichsausnahme für sich

Das Bundesarbeitsgericht (BAG)[292] hatte einer Muslima eine Entschädigung wegen Diskriminierung zugesprochen, nachdem sie von der für Bildung zuständigen Senatsverwaltung nicht in den Schuldienst übernommen worden war. Hintergrund war das im Berliner Neutralitätsgesetz normierte Verbot des Tragens auffallend religiös oder weltanschaulich geprägter Kleidungsstücke innerhalb des Dienstes. Die Senatsverwaltung kündigte im Februar an, wegen der Entscheidung des BAG das Bundesverfassungsgericht (BVerfG) anzurufen. Vor diesem Hintergrund beantragte ein Petent bei der Senatsverwaltung die Herausgabe von Unterlagen, die die Erfolgsaussichten einer Verfassungsbeschwerde einschätzen, und die Entwürfe bzw. die endgültige Fassung der Verfassungsbeschwerde selbst. Darüber hinaus wurden Schriftstücke erbeten, aus denen hervorgeht, wann das Urteil des BAG dem Land Berlin zugestellt worden war.

Die Senatsverwaltung lehnte den Antrag vollständig mit der folgenden Begründung ab: „Alle diese Unterlagen sind Bestandteil einer Akte über ein gerichtliches Verfahren, das noch nicht abgeschlossen ist. Für Gerichte gilt das IFG nur, soweit diese Verwaltungsaufgaben erledigen (§ 2 Abs. 1 IFG). Die rechtsprechende Gewalt ist somit dem IFG von vornherein nicht unterworfen. Der Informationszugang zu konkreten Rechtsstreitigkeiten steht ausschließlich den Parteien des Rechtsstreits zu. Die hier geführte Prozessakte entspricht ganz wesentlich der Prozessakte des Gerichts. Insofern kann für diesen Akteninhalt nichts Anderes gelten. Unabhängig davon besteht nach § 10 Abs. 4 IFG kein Recht auf Akteneinsicht oder Aktenauskunft, wenn sich der Inhalt der Akten auf den Prozess der Willensbildung innerhalb und zwischen Behörden bezieht. Rechtsbehelfsbelehrung…“ Der Petent bat uns um Unterstützung seines hiergegen gerichteten Widerspruchs.

Wir haben die für Bildung zuständige Senatsverwaltung darüber aufgeklärt, dass sie selbst nicht Adressatin der Bereichsausnahme des § 2 Abs. 1 Satz 2 IFG ist,[293] sondern nach dessen Satz 1 dem IFG unterliegt. Deshalb hat sie zu prüfen, ob ein materiell-rechtlicher Ausschlussgrund[294] ganz oder teilweise vorliegt. Im letztgenannten Fall ist der Informati-

[292] Siehe BAG, Urteil vom 27. August 2020 – 8 AZR 62/19

[293] Danach gilt das IFG für die Gerichte und die Behörden der Staatsanwaltschaft nur, soweit sie Verwaltungsaufgaben erledigen.

[294] Siehe §§ 6 ff. IFG

onszugang zu den nicht schutzbedürftigen Aktenteilen zu gewähren.[295] Darüber hinaus ist der von der Senatsverwaltung angeführte Ausschlussgrund des § 10 Abs. 4 IFG nicht richtig angewandt worden, denn die Aussagen im Bescheid erschöpften sich in der Wiedergabe des Gesetzestextes. Stattdessen war hierzu die ständige verwaltungsgerichtliche Rechtsprechung zu dieser Vorschrift zu berücksichtigen. Diese schützt nur den eigentlichen Vorgang der Entscheidungsfindung, also die Besprechung, Beratschlagung und Abwägung, mithin den eigentlichen Vorgang des Überlegens. Nicht geschützt sind dagegen die Tatsachengrundlagen, die Grundlagen der Willensbildung sowie das Ergebnis der Willensbildung.[296] Schließlich wiesen wir darauf hin, dass der erbetene Nachweis über das Zustellungsdatum des Urteils des BAG unproblematisch dadurch erbracht werden kann, dass dem Petenten eine Kopie der Seite übersandt wird, auf der sich der Eingangsstempel der Verwaltung befindet.
Die Senatsverwaltung hat nur diesem letztgenannten Begehren im Widerspruchsbescheid entsprochen, den Antrag im Übrigen zwar abgelehnt, inzwischen aber zumindest mit nachvollziehbarer Begründung.

Eine derart fehlerhafte Anwendung des IFG, wie sie im vorliegenden Fall zunächst erfolgt ist, darf 22 Jahre nach dem Inkrafttreten nicht mehr passieren.

17.2.3.5 Treuwidriges Handeln durch die BVG

Ein Petent stellte bei der BVG drei Anträge, mit denen er Informationen zu den folgenden (hier gekürzten) Fragen wünschte:

1. Antrag: Kosten für Werbung der BVG aus den Jahren 2018, 2019 und 2020 und erwartete Kosten für Werbung der BVG im Jahr 2021

2. Antrag: Werbekonzept(e) der BVG in den Jahren 2018, 2019 und 2020

3. Antrag: Richtlinien/Vorgaben/Weisungen, nach denen geprüft wird, ob Unternehmen/Privatpersonen/Behörden Werbung an/in Verkehrsmitteln und an/in Bushaltestellen der BVG schalten/in Auftrag geben können/dürfen.

Alle Anträge enthielten die ausdrückliche Bitte des Antragstellers an die BVG, dass sie ihn vorab über den voraussichtlichen Verwaltungsaufwand sowie die voraussichtlichen Kosten für die Akteneinsicht

[295] § 12 IFG
[296] Siehe bereits VG Berlin, Urteil vom 4. Mai 2006 – VG 2 A 121.05

oder Aktenauskunft informiert. Dieser Bitte wurde nicht entsprochen: Die BVG erteilte die gewünschten Auskünfte und setzte hierfür zugleich jeweils eine Gebühr in Höhe von 10,00 Euro fest. Die Bitte um Kostenvorabinformation hatte sie als unzulässige Bedingung eingestuft; denn aufschiebend bedingte Anträge seien nach der Rechtsprechung des Bundesverwaltungsgerichts (BVerwG) unzulässig.[297] Der Petent wandte sich deshalb hilfesuchend an uns.

Zwar sieht das IFG keine Pflicht vor, eine antragstellende Person über die voraussichtlichen Kosten zu informieren. Dennoch ist ein Übergehen dieser ausdrücklichen Bitte einer antragstellenden Person als rechtswidriges Verhalten einzustufen. Denn damit hat die BVG gegen § 242 BGB (Leistung nach Treu und Glauben) verstoßen, der im öffentlichen Recht entsprechend gilt. Danach ist der Schuldner verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern. Die Festsetzung auch einer nur geringen Gebühr von jeweils 10,00 Euro änderte daran nichts.

Dass die Anträge in den vorliegenden Fällen unzulässiger Weise „aufschiebend bedingt“ gestellt worden seien, war eine fehlerhafte Auslegung der eindeutigen Anträge zulasten des Petenten. Auch die zitierte Rechtsprechung konnte die Auffassung der BVG nicht stützen, denn dort ging es um die unter einer Bedingung erklärte Rücknahme (!) eines Asyl(folge)antrags, die unwirksam war. Die Fallkonstellation der Entscheidung des BVerwG wäre allenfalls dann mit der vorliegenden Konstellation vergleichbar gewesen, wenn der Petent die Rücknahme des IFG-Antrages unter der Bedingung erklärt hätte, dass ihm eine Gebühr auferlegt würde. Das war aber nicht der Fall: Er hat jeweils einen eindeutigen IFG-Antrag gestellt und erkennbar getrennt hiervon die Bitte um Kostenvorabinformation geäußert.

Da die BVG an ihrer Auffassung festhielt, mussten wir dem Petenten mitteilen, dass er die strittige Frage nur noch gerichtlich klären lassen kann.

Wir bewerten die Nichtbeachtung der Bitte einer antragstellenden Person um Kostenvorabinformation als treuwidrig. Die Festsetzung einer (wenn auch nur geringen) Gebühr ist deshalb rechtswidrig.

[297] Verweis der BVG auf BVerwG, Urteil vom 25. Oktober 1988 – 9 C 18/88

17.2.3.6 IFG-Antrag beim Ordnungsamt Pankow

Ein Bürger beantragte beim Bezirksamt Pankow die Offenlegung aller Unterlagen, die zum Einsatz des Ordnungsamtes im Bötzowkiez vom März vorliegen. Hierüber hatten die Medien berichtet: Es soll im Zusammenhang mit Radfahrenden-Kontrollen zu einer Rangelei von betroffenen bzw. nicht-betroffenen Bürger:innen mit Beschäftigten des Ordnungsamtes bzw. der Polizei gekommen sein. Das Ordnungsamt lehnte den Antrag mit der Begründung ab, der Anwendungsbereich des IFG sei nicht eröffnet. Denn das Amt sei zur Ahndung/Verfolgung von Ordnungswidrigkeiten und deshalb auf der Grundlage des Gesetzes über Ordnungswidrigkeiten (OWiG) tätig geworden. Als „kleine Staatsanwaltschaft" sei sie – wie die Staatsanwaltschaften selbst – vom Anwendungsbereich des IFG ausgenommen. Gleichwohl hat das Ordnungsamt im Rahmen einer „Aktenauskunft nach dem IFG" Einzelheiten wie die Anzahlen der beim Vorfall nach OWiG ausgesprochenen Sanktionen mitgeteilt. Der Petent hat wegen der Beschränkung seines IFG-Anspruchs Widerspruch erhoben und uns um Unterstützung gebeten.

Nach einer Bereichsausnahme gilt das IFG für die Gerichte und Behörden der Staatsanwaltschaft nur, wenn sie Verwaltungsaufgaben erledigen.[298] Das IFG gilt also im Umkehrschluss nicht für die justiziellen Tätigkeiten der Gerichte und Behörden der Staatsanwaltschaft. Da es sich um eine Ausnahmeregelung handelt, ist sie eng auszulegen. Hieraus folgt, dass nur diese Einrichtungen bei ihren Aufgaben der Justizgewährung vom Anwendungsbereich des IFG ausgenommen sind.

Trotzdem durfte das Ordnungsamt im vorliegenden Fall die Offenlegung der gewünschten Unterlagen ablehnen. Wie sich aus der Medienberichterstattung über den Vorfall, aber auch aus der ggü. dem Petenten erfolgten Aktenauskunft ergab, handelten die Dienstkräfte des Ordnungsamtes bei den in Rede stehenden Fahrradkontrollen mit dem Ziel, Ordnungswidrigkeiten wegen Verstößen gegen die StVO zu ahnden. In diesem Rahmen wurden die in der Aktenauskunft genannten Verwarnungen und Ordnungswidrigkeiten-Anzeigen ausgesprochen. Rechtsgrundlage für dieses repressive Handeln war das OWiG, u. U. in Verbindung mit der Strafprozessordnung (StPO). Deshalb gelten für Akteneinsichts- bzw. Auskunftsgesuche die Regelungen des OWiG i. V. m. der StPO[299], nach denen u. a. ein berechtigtes Interesse vorliegen muss. Diese bundes-

[298] Siehe § 2 Abs. 1 Satz 2 IFG
[299] Siehe § 49b OWiG i. V. m. § 475 StPO

rechtlichen Regelungen verdrängen den allgemeinen Informationszugangsanspruch nach dem IFG, wie sich aus dem IFG selbst[300] und letztlich aus dem Grundgesetz (GG) ergibt.[301] Deshalb musste die strittige Frage, ob repressiv handelnde Ordnungsbehörden als „Behörden der Staatsanwaltschaft“ im Sinne von § 2 Abs. 1 Satz 2 IFG anzusehen sind und deshalb dem Anwendungsbereich des IFG von vornherein nicht unterliegen, hier nicht entschieden werden.

Die Offenlegung von Informationen durch repressiv handelnde Ordnungsbehörden kann nicht auf der Grundlage des IFG verlangt werden, denn dieses wird durch höherrangiges Bundesrecht verdrängt.

17.2.3.7 Fehlerhafte Gebührenentscheidung in Charlottenburg-Wilmersdorf

Ein Bürger beschwerte sich darüber, dass er für eine zweistufige Akteneinsicht in Unterlagen beim Stadtentwicklungsamt Charlottenburg-Wilmersdorf zum „Milieuschutzgebiet Schloßstraße und Amtsgerichtsplatz“ jeweils eine Gebühr in Höhe von 204,20 Euro zahlen musste. Das Amt hatte aber nur für den ersten Termin schutzbedürftige Unterlagen gegen Gebühr abzutrennen; die Unterlagen für den zweiten Termin wurden uneingeschränkt vorgelegt, allerdings zusammen mit den Unterlagen des ersten Termins. Eine teilweise Akteneinsicht sei nicht vorgesehen. Um den Vorgang rechtssicher zu gestalten, sei für den zweiten Termin die gesamte Akte vorzulegen.

Wir haben dem Amt mitgeteilt, dass die zweifache Gebührenerhebung in derselben Höhe von 204,20 Euro rechtswidrig war. Denn die Prüfung auf geheimhaltungsbedürftige Aktenteile war nur für den ersten Termin erfolgt. Für den Folgetermin war ein solcher Aufwand nicht entstanden, sodass für diese einfache Akteneinsicht allenfalls eine geringe Gebühr in Betracht kommen konnte.[302] Bei genauer Betrachtung war hier aber überhaupt keine Gebühr angebracht. Denn die uneingeschränkte Akteneinsicht vor Ort ist bei „Umweltinformationen“ gebührenfrei.[303] Dieser Begriff ist nach höchstrichterlicher Rechtsprechung denkbar weit und umfasst alle auch nur im mittelbaren Zusammenhang mit der Umwelt

[300] § 17 Abs. 4 IFG
[301] Art. 31 GG: „Bundesrecht bricht Landesrecht.“
[302] Zwischen 5,00 Euro und 100,00 Euro, siehe Tarifstelle 1004 b) Ziff. 1 des Gebührenverzeichnisses der Verwaltungsgebührenordnung (VGebO); abrufbar unter https://www.datenschutz-berlin.de/informationsfreiheit/rechtliche-grundlagen/gebuehren
[303] § 18a Abs. 4 Satz 3 Ziff. 1 IFG

stehenden Informationen.[304] Die Tatsache, dass das bezirkliche Stadtentwicklungsamt für den „Milieuschutz Schloßstraße und Amtsgerichtsplatz“ federführend war, sprach bereits dafür, dass es sich bei den Unterlagen der zweiten Akteneinsicht im weitesten Sinne um „Umweltinformationen“ handelte. Denn jede Stadtentwicklung hat immer auch Auswirkungen auf die Umwelt. Das Amt hat daraufhin einen Änderungsbescheid nach § 47 Verwaltungsverfahrensgesetz (VwVfG) erlassen, mit dem die Rückzahlung der zweiten Gebühr in Höhe von 204,20 Euro an den Petenten ausgesprochen wurde.

Die Gebühr für einen Verwaltungsaufwand kann nicht doppelt verlangt werden, wenn der Verwaltungsaufwand nur einmal entstanden ist.

17.2.3.8 Fehlerhafte Gebührenentscheidung in Friedrichshain-Kreuzberg

Ein Bürger beantragte im Straßen- und Grünflächenamt Friedrichshain-Kreuzberg die Offenlegung der Planung für die Umgestaltung der Ostseite des Mehringdamms und erbat hierzu eine Vorabinformation zu den voraussichtlichen Gebühren. Das Amt teilte ihm mit, dass „für diese schriftliche Auskunft … und erneute elektronische Anfragen zur vorgenannten Problematik … eine Gebühr in Höhe von jeweils 100 €“ festgesetzt würde. Des Weiteren würden „zusätzlich je nach Aufwand und Organisation der Akteneinsicht Gebühren bis zu 500 € fällig. Alle Kosten [seien] vor einer Terminierung und Gewährung der Akteneinsicht nach Erhalt eines Gebührenbescheides auf das Bezirkskonto einzuzahlen.“

Wir haben dem Amt mitgeteilt, dass die Aussagen zu den voraussichtlichen Gebühren prohibitiv wirken und das angekündigte Vorgehen, wenn es so umgesetzt würde, rechtswidrig wäre. Denn nach der Rechtsprechung des BVerwG stellt ein Informationszugangsantrag, der einen einheitlichen Lebenssachverhalt betrifft, gebührenrechtlich eine einheitliche Amtshandlung dar.[305] Auch die pauschale Forderung nach „Vorkasse“ war unzulässig, denn eine solche steht im Ermessen der Behörde.[306] Wird dieses Ermessen im Gebührenbescheid nicht ausgeübt, ist er wegen Ermessensausfalls rechtswidrig. Die Vorauszahlung der beabsichtigten Gebühr kann nur ausnahmsweise verlangt werden, etwa bei Anhaltspunkten für die Zahlungsunfähigkeit oder -unwilligkeit, wie sich aus der Rechtsprechung des

[304] Siehe BVerwG, Urteil vom 23. Februar 2017 – 7 C 31.15
[305] Siehe BVerwG, Urteil vom 20. Oktober 2016 – 7 C 6.15
[306] Siehe § 16 Satz 2 IFG i. V. m. § 17 Gesetz über Gebühren und Beiträge

OVG Berlin-Brandenburg ergibt.[307] Der Petent hat hiernach die beantragten Informationen zur Baumaßnahme – gebührenfrei – erhalten.

Gebühren dürfen nicht so hoch bemessen sein, dass interessierte Bürger:innen von ihrem Begehren nach Informationszugang abgeschreckt werden. „Vorkasse“ kann nur im Ausnahmefall verlangt werden.

18 Abgeordnetenhaus

18.1 Löschmoratorien — Jetzt auch mit gesetzlicher Grundlage

Untersuchungsausschüsse bilden ein wichtiges Instrument der parlamentarischen Kontrolle. Damit die Ausschüsse ihrem Untersuchungsauftrag aber tatsächlich nachkommen können, sind sie regelmäßig darauf angewiesen, dass ihnen Behörden und sonstige öffentliche Stellen Akten zugänglich machen, deren Inhalt für die Aufklärung des jeweiligen Sachverhalts relevant ist. Deutlich erschwert wird die Arbeit der Untersuchungsausschüsse daher, wenn die für die Aufklärung notwendigen personenbezogenen Daten aufgrund bestehender Löschvorschriften zum Zeitpunkt der Untersuchung schon nicht mehr in den Akten vorhanden oder die Akten selbst vernichtet worden sind. Um diesem Problem von vornherein zu begegnen, wurden in der - Vergangenheit mitunter weitreichende Löschmoratorien erlassen. Eine gesetzliche Regelung, die die Bedingungen konkret festlegt, unter denen ein solcher Aufschub der Löschung angeordnet werden kann, gab es bisher jedoch nicht. Das hat sich jetzt mit der jüngsten Novellierung des Berliner Datenschutzgesetzes (BlnDSG) geändert.

So misslich es ist, wenn die Aufklärungsarbeit aufgrund bereits erfolgter Löschungen erschwert wird, darf nicht außer Acht gelassen werden, dass mit der Anordnung eines Löschmoratoriums oft tiefgreifende Eingriffe in Persönlichkeitsrechte der betroffenen Personen verbunden sein können. Dies gilt in besonderem Maße, wenn sich die Aussetzung der Löschung auf eine Vielzahl von Daten bezieht, die z. B. vom Verfassungsschutz oder der Polizei verarbeitet werden. Schnell könnten Aufzeichnungen über eine Rangelei unter Jugendlichen, einen gewöhnlichen Verkehrsunfall oder – aktuell – über einen Verstoß gegen coronabedingte Kontaktbeschränkungsmaßnahmen ebenfalls von einem Löschmoratorium umfasst und damit für eine Dauer

[307] Siehe OVG Berlin-Brandenburg, Beschluss vom 26. Mai 2014 – 12 B 22.12

gespeichert werden, die sonst nur schweren oder gar schwersten Straftaten zuteilwird.

Die Anordnung eines Löschmoratoriums ist also ein zweischneidiges Schwert, mit dem man sehr behutsam umgehen muss. Eine neue Regelung im BlnDSG[308] sieht daher u. a. vor, dass eine anstehende Datenlöschung bei öffentlichen Stellen nur dann ausgesetzt werden kann, soweit dies im Rahmen der Mitwirkung an der Erfüllung der Aufgaben eines parlamentarischen Untersuchungsausschusses auch erforderlich ist. In zeitlicher Hinsicht soll die Anordnung einen Zeitraum von zwei Jahren nicht überschreiten; Verlängerungen von jeweils nicht mehr als einem Jahr sollen aber zulässig sein.

Natürlich begegnet die Entscheidung, welche Daten im Laufe der Untersuchung ggf. relevant und damit „erforderlich“ werden können, gewissen Unsicherheiten. Dies gilt erst recht, wenn ein Untersuchungsausschuss zum Zeitpunkt der Anordnung noch gar nicht eingesetzt, sondern lediglich im Parlament beantragt worden ist. Auf der anderen Seite kann dieser Umstand nicht dazu führen, dass z. B. alle in einem gewissen Zeitraum erfassten Daten einer Behörde von dieser als potenziell relevant eingeordnet und damit fortdauernd gespeichert werden. Es muss zumindest anhand nachvollziehbarer Kriterien plausibel dargelegt werden können, aus welchem Grund die von dem Löschmoratorium erfassten personenbezogenen Daten zur Aufklärung des jeweiligen Untersuchungsgegenstandes benötigt werden könnten. Diese Entscheidung ist zudem spätestens bei jeder Verlängerung der Anordnung erneut zu überprüfen und der Kreis der erfassten Daten in diesem Zuge ggf. weiter einzugrenzen.

Im Gesetzgebungsprozess haben wir erfolgreich darauf hingewirkt, dass die Anordnung eines Löschmoratoriums schriftlich durch die jeweilige Hausleitung des Verantwortlichen erfolgt und inhaltlich zu begründen ist. Auf diese Weise wird die Überprüfbarkeit der Entscheidung sichergestellt und gewährleistet, dass sich der Verantwortliche mit der Erforderlichkeit und dem konkreten Umfang des Löschmoratoriums auch tatsächlich auseinandersetzen muss.

Darüber hinaus ist unsere Anregung aufgegriffen worden, dass unsere Behörde über jede Anordnung eines Löschmoratoriums und jede Verlängerung von

[308] § 20a Abs. 2 BlnDSG

dem Verantwortlichen in Kenntnis zu setzen ist. Zum einen wird durch diese Mitteilungspflicht die Bedeutung und der Ausnahmecharakter der Anordnung verdeutlicht. Zum anderen ist es uns nur möglich, unseren allgemeinen Kontrollaufgaben[309] nachzukommen, wenn wir von der Existenz einer solchen Anordnung auch tatsächlich wissen.

Es wird sich zeigen, inwieweit sich die neue Vorschrift zu Löschmoratorien in der Praxis bewährt bzw. ob und an welchen Stellen die Stellschrauben noch etwas fester gezogen werden müssen. Ein Schritt in die richtige Richtung ist mit der Schaffung einer gesetzlichen Grundlage jedenfalls vorerst getan. Die Verantwortlichen sind wiederum gehalten, auch bereits bestehende Löschmoratorien auf die Vereinbarkeit mit der neuen Regelung zu überprüfen.

Dem parlamentarischen Informationsinteresse kommt ein besonders hohes Gewicht zu, soweit es um die Aufdeckung möglicher Rechtsverstöße und vergleichbarer Missstände geht. Gleichzeitig gilt es zu berücksichtigen, dass durch ein Löschmoratorium erheblich in Grundrechte der betroffenen Personen eingegriffen wird, insbesondere dann, wenn diese Personen tatsächlich in keiner lei Bezug zum Untersuchungsgegenstand stehen bzw. gesetzliche Löschungsverpflichtungen suspendiert werden.

Den Hinweisen der Berliner Beauftragten für Datenschutz und Informationsfreiheit trägt der Senat im Rahmen der im konkreten Einzelfall stets gebotenen Abwägung zwischen dem Untersuchungsinteresse parlamentarischer Untersuchungsausschüsse einerseits und den Grundrechten betroffener Personen (Grundrecht auf informationelle Selbstbestimmung) andererseits Rechnung.

18.2 Das Parlament als rechtsfreier Raum

Bereits im vergangenen Jahr hatten wir berichtet,[310] dass das Abgeordnetenhaus bisher versäumt hat, eigene Datenschutzvorschriften bzw. eine eigene Aufsicht zu implementieren und damit einem bekannten Kontrolldefizit nach wie vor nicht abgeholfen worden ist. Das Thema ist zu unserem und zum Leidwesen der betroffenen Bürger:innen auch im dritten Jahr nach dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) noch aktuell.

Das BlnDSG sieht vor, dass das Abgeordnetenhaus, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten vom Anwendungsbereich des BlnDSG ausgenommen sind, soweit sie personenbezogene Daten zur Wahrnehmung parlamentarischer Aufgaben verarbeiten.[311] Die Vorschrift führt in bestimmten Konstellationen also zur Nichtanwendung des BlnDSG und entzieht diese Datenverarbeitungen damit gleichsam der Aufsicht unserer Behörde.

[309] Siehe § 11 Abs. 1 Satz 1 Nr. 1 BlnDSG und § 32a Abs. 2 VSG Bln
[310] JB 2020, 17.1
[311] § 2 Abs. 3 BlnDSG

Problematisch ist hieran nicht in erster Linie, dass unsere Kontrollbefugnis eingeschränkt wird. Problematisch ist vielmehr, dass das Abgeordnetenhaus nach wie vor keine eigene Kontrollstelle implementiert hat, die dieses Vakuum ausfüllt. Dazu ist der Landesgesetzgeber aber europarechtlich verpflichtet.[312] Dass die DS-GVO keine Ausnahme für Parlamente enthält und damit grds. auch für diese gilt, soweit die konkrete Tätigkeit dem Unionsrecht unterfällt, hat der Europäische Gerichtshof (EuGH) in Bezug auf den Petitionsausschuss des Hessischen Landtags im Jahr 2020 bereits klargestellt.[313]

Selbst wenn man davon ausginge, dass das Parlament nicht unmittelbar den Regelungen der DS-GVO unterliegt, also eine Meinung vertritt, die im Übrigen auch die Wissenschaftlichen Dienste des Deutschen Bundestages nicht teilen[314], bedarf es mit Blick auf die Sensitivität der im parlamentarischen Raum verarbeiteten personenbezogenen Daten wirksamer und verlässlicher Schutzmaßnahmen und Kontrollmechanismen auf der Grundlage nachvollziehbarer Regelungen. Aber auch solche Datenschutzvorschriften sind bisher nicht erlassen worden.

Wir hatten in der Vergangenheit bereits darauf hingewiesen, dass dieses Kontrolldefizit auch in der Praxis zu Problemen führt. Hierzu gehört, dass betroffene Bürger:innen Initiativen wie dem damals von der AfD-Fraktion initiierten Projekt „Neutrale Schule“ ohne Kontrollmöglichkeit gegenüberstanden. Aber auch in diesem Jahr gab es Schwierigkeiten. Dieses Mal hatte sich eine betroffene Person mit dem Hinweis an uns gewandt hat, dass der Plenar- und Ausschussdienst des Abgeordnetenhaues bei einer Ausschusssitzung, zu dem sie als Anzuhörende geladen war, ein Videokonferenzsystem einsetzt, das nicht rechtskonform nutzbar ist. Leider fanden wir in diesem Punkt beim Abgeordnetenhaus kein Gehör. Denn auf unser Anschreiben hat uns das Abgeordnetenhaus insbesondere unsere eingeschränkte Kontrollbefugnis entgegengehalten.

Selbst wenn man den Einsatz eines solchen Systems in der konkreten Sachverhaltskonstellation tatsächlich vom Anwendungsbereich des BlnDSG ausgenommen sehen möchte, ist nicht einzusehen, warum das Abgeordnetenhaus beim Einsatz von Videokon-

[312] Siehe Art. 54 Abs. 1 lit. a DS-GVO
[313] Siehe EuGH, Urteil vom 9. Juli 2020 – C-272/19, Petitionsausschuss
[314] Gutachten der Wissenschaftlichen Dienste des Deutschen Bundestages zur Anwendbarkeit der Datenschutz-Grundverordnung vom 17. August 2018, WD 3 – 3000 – 299/18

ferenzsystemen für sich eine Sonderrolle beansprucht. Vielmehr sollte es gerade bei der Verarbeitung von personenbezogenen Daten mit gutem Beispiel vorangehen und damit aktiv zum Grundrechtsschutz beitragen.

Da im Geschäftsbereich des Abgeordnetenhauses auch sensitive Daten verarbeitet werden, sollte zügig ein der DS-GVO entsprechendes Datenschutzniveau sichergestellt werden. Das Abgeordnetenhaus als gesetzgebendes Organ hat hier ohne Zweifel eine Vorbildfunktion. Es wird dem neu gewählten Parlament obliegen, dieser Funktion durch die Etablierung eigener Kontrollmechanismen endlich gerecht zu werden.

19 Aus der Dienststelle

19.1 Entwicklungen

Dieses Jahr war für unsere Dienststelle ein weiteres Ausnahmejahr. Unter dem Eindruck der Corona-Pandemie und den damit verbundenen Herausforderungen mussten wir die an die Pandemielage angepassten arbeitsorganisatorischen Maßnahmen weitgehend fortführen. Konkret bedeutete das, dass der überwiegende Teil der Mitarbeiter:innen weiterhin regelmäßig im Homeoffice gearbeitet hat. Ermöglicht wurde dies durch den verstärkten Einsatz von mobilen Endgeräten. Wir arbeiten mit Hochdruck daran, die technischen Voraussetzungen für die Telearbeit weiter zu optimieren. Auch in diesem Jahr wurden Präsenztermine mit Dritten in der Dienststelle sowie Vor-Ort-Termine und Prüfungen außer Haus auf ein Minimum reduziert.

Durch die besondere Situation haben sich die externen und internen Kommunikationsabläufe nachhaltig verändert. Das vermehrte Arbeiten im Homeoffice, die damit einhergehende antizyklische Anwesenheit der Mitarbeiter:innen in den Diensträumen sowie der Verzicht auf größere Gruppenbesprechungen mit persönlicher Anwesenheit machten es erforderlich, auf eine Kommunikation über technische Hilfsmittel (z. B. Video- und Telefonkonferenzen) zurückzugreifen. Um den Informationsfluss in der Behörde aufrecht zu erhalten, haben wir dabei auch auf neue Formate gesetzt und den Austausch über regelmäßige interne elektronische Infobriefe und Newsletter sowie die Modernisierung unseres Intranets aufrechterhalten. Der Rückgriff auf die Technik kann den persönlichen Kontakt unter den Mitarbeiter:innen jedoch nur bedingt ersetzen.

Auch personell gab es 2021 entscheidende Veränderungen. Nach Beendigung ihrer Amtszeit als Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI) am 27. Januar 2021 hat Maja Smoltczyk die Dienstgeschäfte noch bis zum Ablauf der gesetzlichen Übergangsfrist von neun Monaten weitergeführt. Seit ihrem endgültigen Ausscheiden am 27. Oktober 2021 wird die Dienststelle von ihrem bisherigen Stellvertreter, Volker Brozio, bis zur Wahl einer Nachfolge im Amt des/der BlnBDI durch das Abgeordnetenhaus, kommissarisch geleitet. Angesichts der auch überregionalen Bedeutung des Amtes ist zu hoffen, dass die Nachbesetzung zeitnah erfolgt.

Durch den erfreulichen, aber auch dringend notwendigen Personalzuwachs in den Jahren 2020/2021 reichen die räumlichen Kapazitäten unserer Behörde am Standort Friedrichstraße nicht mehr aus. Der vermehrte Flächenbedarf soll, wie bereits berichtet[315], durch einen Umzug in neue Diensträume in Alt-Moabit gedeckt werden. Bis zum endgültigen Umzug, der im Sommer 2022 geplant ist, sind als Übergangslösung einige Mitarbeiter:innen bereits im Dezember 2020 in die Liegenschaft in Alt-Moabit eingezogen. Die damit einhergehende Aufteilung der Dienststelle auf zwei Standorte hat erhebliche organisatorische und logistische Herausforderungen für unser Haus mit sich gebracht, die jedoch durch den besonders engagierten Einsatz aller Mitarbeiter:innen bewältigt werden konnten.

Eine weitere Veränderung hat sich für die BlnBDI auf internationaler Ebene ergeben. Nach vielen Jahren hat unsere Behörde den Vorsitz in der Internationalen Arbeitsgruppe für Datenschutz in der Technologie, auch bekannt als Berlin Group, an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) übergeben. Damit geht eine Ära zu Ende: Die Berlin Group wurde im Jahr 1983 auf Initiative des damaligen Berliner Datenschutzbeauftragten gegründet und hat seitdem unter Berliner Vorsitz eine Vielzahl von Empfehlungen zur Verbesserung des Datenschutzes in der Telekommunikation erarbeitet und publiziert.

19.2 Aus der Arbeit der Servicestelle Bürgereingaben — Trends und Schwerpunkte

Die Servicestelle Bürgereingaben ist innerhalb unserer Behörde die erste Anlaufstelle für Anfragen, Beschwerden und Eingaben jeglicher Art, die von Bürger:innen als Betroffene von Datenverarbeitun-

[315] JB 2020, 20.1

gen an uns herantragen werden. Die Zahl von Beschwerden über datenschutzrechtliche Verstöße durch Behörden und Unternehmen verblieb auch in diesem Jahr auf einem konstant hohen Niveau. Von den ca. 5.000 Eingaben die uns erreicht haben, mündeten knapp die Hälfte in ein förmliches Beschwerdeverfahren. Den übrigen Eingaben konnte durch die Servicestelle Bürgereingaben mit Hinweisen, Beratungsgesprächen oder mittels Verweis auf Veröffentlichungen der Datenschutzaufsichtsbehörden und -konferenz abgeholfen werden. Der Fokus des Eingabeaufkommens lag im vergangenen Jahr erneut auf den pandemiebezogenen Sachverhalten, aber auch Unternehmen aus dem Bereich der Zahlungsdienste und Wohnungswirtschaft, der Wahlkampf zur Bundestagswahl sowie Vorgänge bei der Polizei waren Schwerpunkte bei den Beschwerden.

Das weitgehend digitalisierte Verfahren unserer Behörde für die Entgegennahme und Bearbeitung von Datenschutzbeschwerden versetzt uns weiterhin in die Lage, diese in nahezu allen Fällen zeitnah zu erfassen und die Beschwerdeführer:innen über das Ergebnis oder den Fortgang ihrer Eingaben zu informieren. Trotz der pandemiebedingt erschwerten Arbeitsumstände konnte die Servicestelle Bürgereingaben ihre Aufgaben erneut vollumfänglich erfüllen. In Bezug auf die andauernde pandemische Lage führte zuletzt das Scannen von Impfzertifikaten im Rahmen von 2G-Regelungen zu einem Anstieg der Anfragen von Bürger:innen. Hier konnten wir beratend tätig werden und die betroffenen Personen über die gesetzlichen Grundlagen der Maßnahmen zur Unterbrechung von Infektionsketten aufklären. Wir bieten zudem auf unserer Internetseite und in der zugehörigen Infothek umfangreiche Informationen zu den datenschutzrechtlichen Aspekten der Corona-Pandemie an.

Vielfach erhielten wir Beschwerden über einen Zahlungsdienstleister, der sich bei der Beantwortung von Betroffenenanfragen durch hartnäckige Zurückhaltung ausgezeichnet hat. Auskunfts- und Löschungsersuchen wurden häufig gar nicht beantwortet, die Daten von Betroffenen aber weiterhin für Werbezwecke verarbeitet. Hier stehen wir nun im europaweiten Austausch mit den anderen Aufsichtsbehörden, da sich die Hauptniederlassung des Unternehmens nicht in Deutschland befindet.

Im Bereich der Wohnungswirtschaft konnten wir einer Vielzahl von Betroffenen helfen, indem wir ein Unternehmen, das durch schnelle Zukäufe in den Berliner Wohnungsmarkt eingetreten ist, überzeugten, auf die Vermessung der neu erworbenen Woh-

nungen durch 3D-Laserscanverfahren zu verzichten. Nach unserem Hinweis der datenschutzrechtlichen Unzulässigkeit stellte das Unternehmen die Aktion ein.

Die Bundestagswahlen im September und insbesondere der Wahlkampf im Vorfeld waren ebenfalls Gegenstand eines erhöhten Beschwerdeaufkommens. Es besteht zwar im Hinblick auf den Wahlkampf eine gesetzliche Grundlage, nach der Parteien personenbezogene Daten von Wähler:innen für Wahlwerbung verarbeiten dürfen. Dass diese Wahlwerbung jedoch dann teilweise im Namen nicht einer Partei zuzuordnender Absender:innen verschickt wurde, sorgte bei vielen Berliner:innen für Unmut. Der Einsatz einer App, die Wahlkämpfer:innen durch dieselbe Partei zur Verfügung gestellt wurde, führte zudem zu einer nicht unerheblichen Zahl von Datenschutzverstößen, da hierbei mitunter die politische Gesinnung von Personen erfasst wurde.[316]

Eine Wiedergängerin in den Schwerpunkten der Beschwerdenbearbeitung in unserer Behörde ist auch die Polizei. Neben einem besonders frappierenden Fall, in dem die Polizei durch die nicht erforderliche Übersendung von ungeschwärzten Akten an das Verwaltungsgericht die Gefahr geschaffen hat, dass z. T. besonders schutzbedürftige Daten von Demonstrationsanmelder:innen in die Hände von Unbefugten gelangen können[317], erreichten uns auch in diesem Jahr mehrere Fälle, in denen Polizeibeamt:innen widerrechtlich personenbezogene Daten aus den ihnen zugänglichen Registern abriefen.[318]

19.3 Datenschutz und Medienkompetenz

Wir haben uns zum Ziel gesetzt, bereits Grundschulkindern frühzeitig zu vermitteln, was personenbezogene Daten sind, was sich hinter dem Begriff Datenschutz verbirgt und wie sie selbst Einfluss darauf nehmen können, was mit ihren Daten geschieht.

Pünktlich zum Schuljahresbeginn 2021/22 im Herbst veröffentlichten wir unser überarbeitetes medienpädagogisches Angebot und boten Grundschulen wieder ein neues kostenloses Workshop-Format an. Der Workshop „Datenschutz für Kinder“ richtet sich speziell an die Jahrgangsstufen 4 bis 6. Verteilt über fünf Unterrichtsstunden vermittelt er

[316] Siehe 15.1
[317] Siehe 3.1
[318] Siehe 13.2

digitale Kompetenzen und führt in die Datenschutzwelt ein. Die Schüler:innen entdecken spielerisch, was Daten sind, wie sie erhoben werden und wieso sie schützenswert sind. Ein weiterer Schwerpunkt liegt in der Information über personalisierte Werbung: Durch die Gestaltung von fiktiven Werbeanzeigen vertiefen die Schüler:innen ihr Verständnis von personalisierter Werbung und der Nutzung bereits veröffentlichter Daten. Anhand praxisnaher Fallbeispiele, diskutieren die Schüler:innen, wie sie sich z. B. im Falle von Datendiebstahl persönlich verhalten würden. Am Ende des Workshops wird ein " Datenschutzvertrag" geschlossen, in den die gewonnenen Erkenntnisse einfließen.

Der Workshop stieß auf großes Interesse. Bis zum Jahresende haben wir in vier Berliner Bezirken insgesamt acht Ganztages-Workshops (à fünf Stunden) durchgeführt und damit über 160 Schüler:innen erreicht. Der steigende Bedarf an Schulungen und begleitendem Lehrmaterial ist auch angesichts der anhaltenden Corona-Pandemie und der damit verstärkten Nutzung digitaler Medien nochmals deutlich geworden. Durch die Arbeit an den Schulen wurden zudem thematische Schwerpunkte sichtbar, bei denen eine besondere Hilfestellung für Lehrpersonal und Eltern erforderlich ist. Zu nennen sind hier vor allem die zunehmende Verbreitung von Messenger-Diensten unter Grundschüler:innen und die damit einhergehenden Gefahren von Cybermobbing.

Zu diesen und weiteren Themen werden wir unser medienpädagogisches Angebot stetig erweitern und umfangreiches Informations- und Unterrichtsmaterial anbieten. Um weitere Workshops und Projekte an Schulen und in Bildungseinrichtungen in der Fläche durchführen zu können, wollen wir künftig dazu übergehen, auch Multiplikator:innen zu schulen.

Des Weiteren bauen wir unser digitales Angebot unter www.data-kids.de kontinuierlich aus. Auf der Webseite finden Grundschulkinder, Lehrkräfte und Eltern vielfältige Materialien zum sicheren Umgang mit den eigenen Daten im Internet. Die Webseite wurde auch in diesem Jahr um audiovisuelle Medien und interaktive Spiele ergänzt. Warum Datenschutz auch im Homeschooling wichtig ist, wird bspw. in einem neuen Video erläutert. Ergänzende Informationsmaterialien für Kinder, Lehrkräfte und Eltern stellen wir dort weiterhin zum kostenlosen Download zur Verfügung. Neben der Weiterentwicklung von Data-Kids (Altersgruppe 6 bis 12) haben wir in einer länderübergreifenden Arbeitsgruppe an der

Neukonzipierung der Webseite www.youngdata.de (Altersgruppe 12+), die von der Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) betrieben wird, mitgearbeitet. Der Relaunch von Young-Data ist für 2022 geplant.

19.4 Zusammenarbeit mit dem Abgeordnetenhaus von Berlin

Der Ausschuss für Kommunikationstechnologie und Datenschutz (KtDat) kam in diesem Jahr insgesamt acht Mal zusammen und befasste sich mit vielen Themen aus dem Bereich Digitalisierung und Datenschutz. Die BlnBDI hat an allen Sitzungen teilgenommen und das Gremium mit ihren Expert:innen umfassend beraten. Die Digitalisierung der Schulen[319], die elektronische Kontaktnachverfolgung zur Pandemiebekämpfung[320] und die Mobilitäts-Apps der BVG[321] waren einige der besonders wichtigen Punkte auf der Agenda des Ausschusses. Ein wesentliches Thema war auch der datenschutzkonforme Einsatz digitaler Lehr- und Lernmittel an den Schulen[322]. Wir haben uns in diesem Zusammenhang mit Nachdruck dafür eingesetzt, dass das Schulgesetz (SchulG) hinsichtlich des Datenschutzes modernisiert wird. Der Einsatz hat sich gelohnt. Das reformierte SchulG enthält nun Regelungen zum Datenschutz, die auf explizite Empfehlungen unserer Behörde zurückgehen und ist damit eines der modernsten Schulgesetze in Deutschland[323]. Auch das geplante neue Berliner Transparenzgesetz (BlnTranspG)[324] wurde immer wieder auf die Tagesordnung des KtDat gesetzt. Gleichwohl gelang es dem Abgeordnetenhaus nicht, es bis zum Ende der 18. Wahlperiode zu verabschieden. Dies ist einerseits bedauerlich, andererseits bietet dieser Umstand für das neu zusammengesetzte Abgeordnetenhaus gleichzeitig die Chance, die gravierenden Mängel in dem zuletzt vorgelegten Gesetzentwurf zu beseitigen und in dieser Legislaturperiode tatsächlich ein modernes Berliner Transparenzgesetz zu schaffen.

19.5 Zusammenarbeit mit anderen Stellen

In diesem Jahr stand die DSK unter dem Vorsitz des Saarlands. Sie tagte am 27./28. April und am 25./26. November jeweils virtuell. Daneben fanden drei

[319] Siehe 1.2
[320] Siehe 1.5
[321] Siehe 11.1 und 11.2
[322] Siehe auch unsere Pressemitteilung vom 22. Januar 2021; abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210122-PM-Digitaler_Unterricht_Misstaende_beheben.pdf
[323] Siehe auch unsere Pressemitteilung vom 17. September 2021; abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/20210917-PM_Schulgesetz.pdf
[324] Siehe 17.2.1

Zwischenkonferenzen als Videokonferenzen am 27. Januar, 16. Juni und 22. September statt. Die DSK fasste während ihrer Sitzungen zahlreiche Entschließungen und Beschlüsse zu aktuellen datenschutzrechtlichen Fragen,[325] u. a. zur Verarbeitung von Positivdaten in einem sog. „Energieversorgerpool“,[326] zum Einsatz von Kontaktnachverfolgungssystemen[327] und zur Verarbeitung des Datums „Impfstatus“ von Beschäftigten durch ihre Arbeitge-ber:innen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) tagte unter dem Vorsitz von Sachsen-Anhalt am 2. Juni und 3. November jeweils als Videokonferenz.

Die Global Privacy Assembly (GPA)[328] fand als zweitägige Videokonferenz am 20./21. Oktober statt. Im Vordergrund der Konferenz stand der Datenschutz und der Schutz der Privatsphäre im digitalen Zeitalter. Auch die zukünftige strategische Ausrichtung der GPA war erneut ein wichtiges Thema.
Die GPA nahm zahlreiche Berichte und Entschließungen[329] an, u. a. zu digitalen Kinderrechten.

19.6 Pressearbeit

In diesem Jahr stellte sich unsere Pressestelle personell neu auf. Auch auf organisatorischer Ebene gab es einige Veränderungen, mit dem Ziel das stetig steigende Interesse an den Themen und Tätigkeiten unserer Behörde auch künftig fundiert und zuverlässig zu bedienen.

Insgesamt haben wir über 200 Presseanfragen beantwortet. Wie auch schon im Jahr zuvor dominierten dabei insbesondere Anfragen zum Datenschutz im Zusammenhang mit der Corona-Pandemie. Während 2020 die analoge Kontaktdatenerfassung im Vordergrund stand, bildeten in diesem Jahr Anfragen zur digitalen Kontaktnachverfolgung einen Schwerpunkt. Hierbei interessierten sich die Medien vor allem für den (Zwischen-) Stand der laufenden Prüfung in unserem Haus.[330] Viele Anfragen erreichten uns zudem zu Datenpannen bei Corona-

[325] Alle Entschließungen und Beschlüsse der DSK sind auf der Webseite der DSK unter https://www.datenschutzkonferenz-online.de/entschliessungen.html und https://www.datenschutzkonferenz-online.de/ beschluesse-dsk.html abrufbar.
[326] Siehe 11.3
[327] Siehe 1.5, 6.1 und 6.5
[328] Ehemals International Conference of Data Protection and Privacy Commissioners
[329] Alle Entschließungen und Berichte der GPA sind auf der Webseite der GPA unter https://globalprivacyassembly .org/document-archive/adopted-resolutions/ und https://globalprivacyassembly.org/document-archive/ working-group-reports/ abrufbar.
[330] Siehe 1.5

Testzentren sowie dem Impfmanagement des Landes Berlin.

Im Superwahljahr 2021 erhielten wir zudem viele Anfragen zur Zulässigkeit von personalisierter Wahlwerbung per Post und zum Haustürwahlkampf per App. Weitere wichtige Themen waren die Folgen des Schrems-II-Urteils sowie Datenpannen bei diversen Betreibern von Online-Shops, Essenslieferdiensten und öffentlichen Stellen. Immer wieder sind wir auch durch Medienanfragen auf mutmaßliche Datenschutzverstöße aufmerksam geworden und haben diese zum Anlass genommen, die zugrundeliegende Datenverarbeitung zu prüfen. Für weiterhin großes überregionales Interesse sorgten unsere Hinweise und Prüfergebnisse zum datenschutzkonformen Einsatz von Videokonferenzdiensten. Das erstmals 2020 veröffentlichte Papier haben wir im Februar dieses Jahres umfassend überarbeitet und aktualisiert.[331]

Mit insgesamt vierzehn Pressemitteilungen haben wir uns an die Öffentlichkeit gewandt. Wir haben u. a. auf die datenschutzrechtlichen Missstände beim digitalen Unterricht im Land Berlin aufmerksam gemacht und die Offenlegung von sensitiven Daten bei Kontrollen in Bus und Bahn für Anspruchsberechtigte des „berlinpass“ kritisiert. Außerdem wiesen wir die Öffentlichkeit auf neue Prüfverfahren im Bereich internationaler Datentransfers von Unternehmen und den Einsatz von Tracking-Techniken und Drittdiensten auf Webseiten hin. Zum Ende ihrer Amtszeit hat Maja Smoltczyk, im Rahmen einer Pressemitteilung, über ihre mehr als fünfjährige Tätigkeit als BlnBDI Bilanz gezogen.

Zusätzlich beantworteten die Behördenleitung sowie Fachreferent:innen in dutzenden Interviews und Hintergrundgesprächen vielfältige Fragen von A wie Auftragsverarbeitung bis Z wie Zertifizierung. In einem gemeinsamen Meinungsbeitrag wiesen Prof. Dr. Dieter Kugelmann als rheinland-pfälzischer Landesbeauftragter für den Datenschutz und die Informationsfreiheit und Maja Smoltczyk als BlnBDI die wiederkehrenden haltlosen Attacken auf den Datenschutz zurück. Sie stellten klar, dass der Datenschutz gesellschaftlichen Herausforderungen wie der Corona-Pandemie nicht im Wege steht, sondern vielmehr zu Akzeptanz und Vertrauen in der Bevölkerung beiträgt.[332]

[331] Siehe 2.2

[332] Siehe https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2021/2021-BlnBDI-LfdRLP-Standpunkt_Attacke_auf_Datenschutz.pdf

Folgende Pressemitteilungen haben wir in diesem Jahr veröffentlicht:

- Digitaler Unterricht – Missstände müssen so schnell wie möglich behoben werden (22. Januar)
- Datenschutzbeauftragte von Berlin und Rheinland-Pfalz weisen haltlose ¬Attacken auf das informationelle Selbstbestimmungsrecht zurück – Smoltczyk und Kugelmann: Der Datenschutz ist eine europäische Erfolgsgeschichte (5. Februar)
- Mehr „Grün“: Berliner Datenschutzbeauftragte veröffentlicht aktualisierte Hinweise zu datenschutzgerechten Videokonferenzdiensten (18. Februar)
- Leistungsbescheid statt berlinpass: Kein Datenschutz für Geringverdiener:innen (1. März)
- Bußgeldbescheid gegen Deutsche Wohnen SE: Beschwerde gegen Einstellung des Verfahrens eingelegt (3. März)
- Berlin Group (IWGDPT) veröffentlicht Arbeitspapiere zu Data Portability and Web Tracking (23. März)
- Berliner Beauftragte für Datenschutz und Informationsfreiheit veröffentlicht Jahresbericht 2020 (8. April)

- Berliner Datenschutzbeauftragte beteiligt sich an deutschlandweiter Prüfung internationaler Datentransfers von Unternehmen (1. Juni)
- Mängel auf allen Ebenen: Berliner Aufsichtsbehörde konfrontiert Webseiten-Betreibende mit rechtswidrigem Tracking (9. August)
- Datenschutz für Kinder: Neuer Workshop für Berliner Grundschulen (16. August)
- Berliner Schulgesetz: Reform stärkt den Datenschutz im Bildungsbereich (17. September)
- „Zeit der Umbrüche“: Amtszeit von Maja Smoltczyk als BlnBDI endet (19. Oktober)
- Kontaktdatenerfassung: Corona-Warn-App als datensparsame Alternative in Berliner Landesverordnung ermöglichen (19. November)
- TTDSG tritt in Kraft: Klare Regeln für Cookies und ähnliche Technologien (1. Dezember)

Alle Pressemitteilungen sind auf unserer Webseite abrufbar.[333]

Mit einer entsprechenden E-Mail an die Adresse presse@datenschutz-berlin.de ist eine Aufnahme in unseren Presseverteiler möglich.

[333] https://www.datenschutz-berlin.de/infothek-und-service/pressemitteilungen

19.7 Öffentlichkeitsarbeit

19.7.1 Veranstaltungen und Vorträge

Aufgrund der anhaltenden Corona-Pandemie fanden auch in diesem Jahr die meisten Veranstaltungen online im Rahmen von Videokonferenzen statt. Nach den Erfahrungen aus dem Vorjahr konnten geplante Podiumsdiskussionen, Kongresse, Workshops und Fachgespräche jetzt auch kurzfristig in Online-Formate umgewandelt oder als Hybrid-Veranstaltungen durchgeführt werden. So war es möglich, den regen Austausch der nationalen und internationalen Fachgremien, Arbeitsgruppen und Arbeitskreise zu gewährleisten.

Auch die Vortragstätigkeit verlagerte sich teils in den digitalen Raum. Einige Beispiele seien hier genannt:

- Online-Vortrag „Aktuelle Entwicklungen der Bußgeldpraxis deutscher Aufsichtsbehörden“ am 10. Juni bei einem Hamburger Verein
- Vortrag „Die DS-GVO in der Praxis aus Sicht der Berliner Beauftragten für Datenschutz und Informationsfreiheit“ am 16. September beim Datenschutztag eines Unternehmens in Berlin; Themen waren wichtige Problemfelder in der aufsichtsrechtlichen Praxis, z. B. bei der Erteilung von Auskünften nach Art. 15 DS-GVO, bei der Einholung von Einwilligungen für Tracking und beim Einsatz von Videokonferenzsystemen.
- Vortrag „Website-Tracking im aufsichtsbehördlichen Verfahren – rechtliche Gemengelage und technische Fallstricke“ bei der Datenschutzkonferenz (Hybridveranstaltung) eines Unternehmens am 20. September
- Vortrag „Einwilligungsverwaltung aus aufsichtsbehördlicher Perspektive“ beim ¬DatenTag der Stiftung Datenschutz am 3. November in Berlin; Die Veranstaltung unter dem Titel: „Das TTDSG und neue Wege zur Einwilligungsverwaltung“ informierte mit verschiedenen Beiträgen und Debatten zu einzelnen Aspekten rund um das neue Telekommunikations-Telemedien-Datenschutz-Gesetz (TTDSG).
- Podcast-Sendung vom 15. Dezember: „Cookies, Banner und das neue TTDSG“; Expertinnen der BlnBDI und der Landesbeauftragten für den Datenschutz Niedersachsen erklären die neuen Regelungen im „Datenfunk“-Podcast des Landes¬beauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz.

19.7.2 Veröffentlichungen

Ein weiterer Baustein unserer Öffentlichkeitsarbeit sind die Publikationen. Die Infothek[334] auf unserer Webseite enthält u. a. Gesetzestexte, Beschlüsse und Leitlinien sowie hauseigene Flyer, Broschüren und Ratgeber. Alle Informationsmaterialien stehen als Download zur Verfügung, einige können auch als gedruckte Ausgabe kostenfrei bestellt werden.
Neben dem Tätigkeitsbericht des vergangenen Berichtszeitraums ergänzten wir unsere Printpublikationen um einen neuaufgelegten Ratgeber:

- Anlässlich der Bundestagswahlen und der Wahl zum Abgeordnetenhaus von Berlin in diesem Jahr haben wir unseren Ratgeber **„Wahlwerbung durch politische Parteien“**, der erstmalig 2008 veröffentlicht wurde, grundlegend überarbeitet und neu aufgelegt. Der Ratgeber informiert über die rechtlichen Rahmenbedingungen im Zusammenhang mit unerwünschter Wahlwerbung – ob per Post, an der Haustür oder mittels Wahlkampf-App – und zeigt auf, dass und wie der Weitergabe der Meldedaten widersprochen werden kann.
- Ebenfalls neu aufgelegt haben wir unsere hauseigene Ausgabe der Datenschutz-Grundverordnung (DS-GVO). Nach über drei Jahren Erfahrung mit der DS-GVO haben wir die erste Auflage an die praktischen Anforderungen angepasst und damit mehr Übersichtlichkeit hergestellt. Die Erwägungsgründe sind nun als Ganzes vor den Artikeln abgedruckt und mit Verweisen auf die einschlägigen Normen versehen. An den jeweiligen Artikeln befinden sich wiederum Verweise auf die dazugehörigen Erwägungsgründe.

Auf unserer Webseite bieten wir zusätzlich zu den bereits oben beispielhaft genannten Materialien auch Orientierungshilfen und komprimierte Informationen zu Schwerpunktthemen wie der Corona-Pandemie an. So finden sich hier u. a. aktuelle Hinweise für Berliner Verantwortliche zum Einsatz von Videokonferenzdiensten, zum datenschutzkonformen Einsatz von digitalen Lernplattformen, ein Musterformular zur Kontaktnachverfolgung sowie FAQs zu den Themen Impfzertifikat und Teststellen. In unserer Rubrik „Themen A bis Z“ greifen wir von A wie Akkreditierung bis Z wie Zertifizierung verschiedene Themen auf, die wir ständig erweitern.

[334] https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen

19.7.3 Ausblick

Das im September 2020 neu geschaffene Referat „Gremien-, Presse- und Öffentlichkeitsarbeit“ hat sich im Laufe des Jahres personell zunehmend konsolidiert und die nötigen Strukturen und Grundlagen geschaffen, um die Öffentlichkeitsarbeit unserer Behörde weiter ausbauen zu können. Erfreulich ist, dass die einzelnen Arbeitsbereiche nun deutlich besser ineinandergreifen. Auch die interne Kommunikation konnte dadurch insgesamt verbessert werden, insbesondere auch durch den vom Referat umgesetzten umfassenden Relaunch des Intranets.

Im kommenden Jahr wird die seit Frühjahr vakante Stelle im Bereich Öffentlichkeitsarbeit nachbesetzt, sodass wir dann wieder mit voller Kraft an neuen Veranstaltungsformaten, Print-Publikationen und nicht zuletzt an der Umsetzung unserer digitalen Kommunikationsstrategie arbeiten können. Dazu gehört u. a. die Überarbeitung unserer Webseite sowie die Erweiterung unseres digitalen Informationsangebots.

Das zentrale Anliegen ist, den Austausch mit Politik und Medien und insbesondere mit Bürgerinnen und Bürgern weiter zu stärken und so das allgemeine Bewusstsein für den Datenschutz und Medienkompetenz zu fördern. Daher werden wir unsere Zusammenarbeit mit zivilgesellschaftlichen Akteur:innen, wissenschaftlichen Institutionen, Schulen und Bildungseinrichtungen weiter ausbauen. Die Einbindung von Multiplikator:innen, neuer digitaler Veranstaltungsformate und Medien sowie die Einführung verschiedener Schulungsangebote werden unsere Arbeit im kommenden Jahr maßgeblich prägen.

20 Statistik für den Jahresbericht

Im vierten Jahr der Datenschutz-Grundverordnung (DS-GVO) zeigt sich, dass sich sowohl die Anzahl der Eingaben als auch die der gemeldeten Datenpannen auf einem konstant hohen Niveau verstetigen. Dies wird besonders im Vergleich zur Anzahl der Fälle vor Geltung der DS-GVO deutlich. Im Vergleich zum Vorjahr ist ein Anstieg bei den förmlichen Beschwerden und Beratungen von Betroffenen sowie den gemeldeten Datenpannen zu verzeichnen.

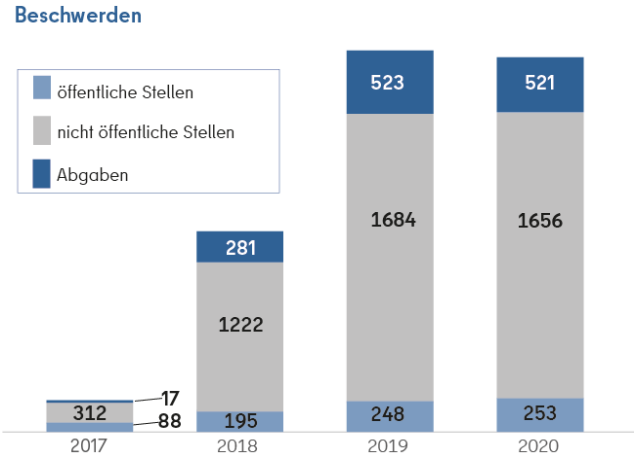
Die Darstellung des folgenden Kapitels orientiert sich an den einheitlichen Statistikkriterien, die die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) be-

schlossen hat. Zudem kommen wir damit unseren Berichtspflichten aus der DS-GVO und dem Bundesdatenschutzgesetz (BDSG) nach. Hierbei ist jedoch zu beachten, dass aufgrund der Corona-Pandemie und den dadurch erschwerten Arbeitsbedingungen noch nicht alle Vorgänge abschließend statistisch erfasst sind. Die hier angegebenen Zahlen stehen demnach unter Vorbehalt.

20.1 Beschwerden

Unsere Behörde erreichten in diesem Jahr insgesamt 5.671 Eingaben von Betroffenen, von denen 2.436 als förmliche Beschwerden im Sinne der DS-GVO zu behandeln waren.[335] Für den Großteil der Beschwerden eröffneten wir Verfahren in eigener Zuständigkeit. Alles in allem waren das in diesem Jahr 1.856 Verfahren. Davon richteten sich mehr als 80 % gegen private Stellen (1.589), der Rest gegen Behörden (267). In 580 Fällen lagen die Beschwerden nicht in unserem Zuständigkeitsbereich, bspw., weil der Verantwortliche seinen deutschen Hauptsitz in einem anderen Bundesland hatte. Diese Beschwerden haben wir an die jeweils zuständigen Aufsichtsbehörden in Deutschland abgegeben.

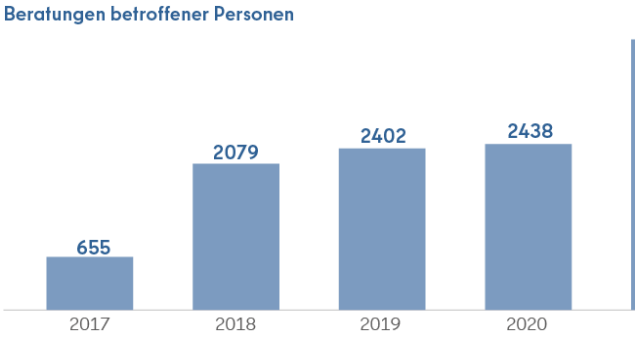
Auch in diesem Jahr blieb die Zahl der bei uns seit Geltung der DS-GVO eingereichten Beschwerden auf einem konstant hohen Niveau. Die nachfolgende Grafik gibt einen Überblick über die Anzahl der bei uns eingereichten Beschwerden von Betroffenen ggü. öffentlichen und nicht-öffentlichen Stellen sowie über Abgaben an andere deutsche Aufsichtsbehörden seit 2017.



[335] Siehe Art. 77 DS-GVO

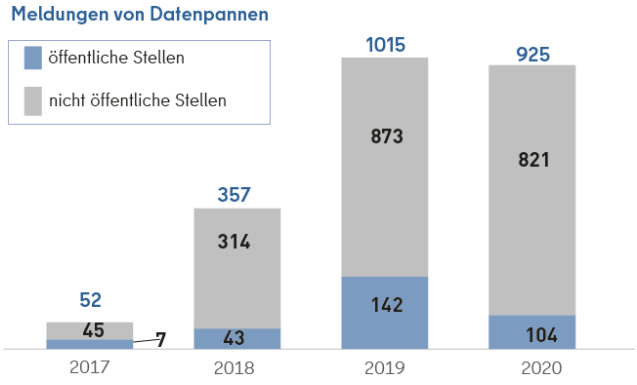
20.2 Beratungen

Mit dem Begriff Beratungen werden alle schriftlichen datenschutzrechtlichen Auskünfte ggü. Verantwortlichen, betroffenen Personen und der öffentlichen Verwaltung beschrieben. Der Schwerpunkt lag hierbei in der Beratung betroffener Personen, also Bürger:innen, mit 3.235 Fällen. Hier gab es im Berichtszeitraum einen sehr starken Anstieg im Vergleich zum Vorjahr. Daneben berieten wir in 472 Fällen Verantwortliche. Hinzu kommt eine Vielzahl telefonischer Auskünfte, die nicht statistisch erfasst werden.



20.3 Datenpannen

In diesem Jahr haben Verantwortliche bei uns deutlich mehr Datenpannen gemeldet als im Vorjahr. Im Berichtszeitraum gab es insgesamt 1.163 Meldungen von Verantwortlichen, was einen neuen Maximal-Wert ggü. den Jahren zuvor darstellt. Von den Meldungen entfielen 1.026 auf den nicht-öffentlichen Bereich, d. h. vor allem auf private Unternehmen. Öffentliche Stellen meldeten uns 137 Datenpannen.



Auch wenn wegen der Vielfalt von Datenpannen keine quantifizierten Aussagen zu bestimmten Arten getroffen werden können, so lassen sich folgende exemplarische Aussagen treffen:

Nicht alle Datenpannen können auf unmittelbares menschliches Versagen zurückgeführt werden. Oft

sind nicht ergriffene Sicherheitsmaßnahmen eine weitere Ursache.

Beispielsweise sind unverschlüsselte mobile Datenträger bei Verlust problematisch. Häufig werden in Einrichtungen zur Kinderbetreuung Film- und Fotoaufnahmen auf nicht verschlüsselten Medien gespeichert, sodass bei Verlust von USB-Sticks, SD-Karten, Kameras oder Rechnern die Aufnahmen von Kindern in den Besitz Unbefugter gelangen. Bereits im Jahresbericht 2019[336] wurde diese Problematik thematisiert.

Schwachstellen von Software sind eine weitere, mittelbare Ursache für Datenpannen. Zwei daraus resultierende Angriffswege sind auch in diesem Berichtszeitraum markant gewesen.

Zum einen waren dies weit verbreitete Schwachstellen in E-Mail-Server-Software, die durch Kriminelle zur Übernahme dieser Server ausgenutzt wurden, wodurch auf Informationen zugegriffen werden konnte, die auf den Servern gespeichert vorlagen.

Zum anderen waren dies sog. Ransomware-Angriffe, die bereits andernorts in diesem Tätigkeitsbericht näher behandelt wurden.[337]

20.4 Abhilfemaßnahmen

Wenn wir einen Verstoß gegen die DS-GVO durch Verantwortliche feststellen, können wir verschiedene Abhilfemaßnahmen ergreifen.[338] In diesem Jahr haben wir zwei Warnungen und 212 Verwarnungen ausgesprochen. Von der Möglichkeit, Zertifizierungen zu widerrufen wurde im Berichtszeitraum kein Gebrauch gemacht. In einem Fall wurde eine Anordnung erlassen. In 61 Fällen haben wir Geldbußen in Höhe von insgesamt 133.350,00 Euro verhängt. Zum Ende des Berichtszeitraums waren die entsprechenden Verfahren jedoch noch nicht alle rechtskräftig abgeschlossen. Zudem wurden 36 Zwangsgeldbescheide erlassen. In 3 Fällen haben wir einen Strafantrag gestellt. Über das Jahr verteilt wurden 25 Bußgeldverfahren eingestellt.

Zusätzlich zu den hier genannten Fällen wurde eine größere Anzahl weiterer Verfahren eröffnet, in denen noch kein Bescheid ergangen ist.

---

[336] JB 2019, 15.2
[337] Siehe 5.4
[338] Siehe Art. 58 Abs. 2 DS-GVO

Abhilfemaßnahmen 2021	
Warnungen	2
Verwarnungen	212
Anweisungen und Anordnungen	1
Widerruf von Zertifizierungen	0
Geldbußen	61

20.5 Förmliche Begleitung bei Rechtssetzungsvorhaben

Unsere Behörde hat nach dem Berliner Datenschutzgesetz (BlnDSG) u. a. die Aufgabe, das Abgeordnetenhaus, den Senat und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen datenschutzrechtlich zu beraten.[339] Dazu gehören sowohl schriftliche Stellungnahmen als auch Besprechungen mit Fraktionen und Abgeordneten sowie förmliche Anhörungen im Abgeordnetenhaus und in dessen Ausschüssen.

Im Berichtszeitraum haben wir bei mehreren Gesetzgebungsvorhaben beraten, wie z. B. bei Änderungen des Schulgesetzes (SchulG)[340] oder des BlnDSG[341]. Des Weiteren gaben wir u. a. Stellungnahmen zur Novellierung des Zweckentfremdungsverbot-Gesetzes (ZwVbG)[342] und dem Lobbyregistergesetz (BerlLG) ab.[343]

Hinzu kamen mehrere Beratungen bei Rechtsetzungsvorhaben, die die Schaffung und Änderung von Rechtsverordnungen und Verwaltungsvorschriften zum Gegenstand hatten. Als Beispiel sei hier die Änderung der Verordnung über sachliche Zuständigkeiten für die Verfolgung und Ahndung von Ordnungswidrigkeiten (ZustVO-OWiG) u. a. aufgrund des Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG) genannt.[344] Bei Projekten der Bundesgesetzgebung nahmen wir zudem gemeinsam mit den anderen Aufsichtsbehörden des Bundes und der Länder Stellung.

[339] § 11 Abs. 1 Satz 1 Nr. 3 BlnDSG
[340] Siehe 1.2.1
[341] Siehe 18.1
[342] Siehe 9.3
[343] Siehe 17.2.1
[344] Zum TTDSG siehe 14.2

20.6 Europäische Verfahren

Die DS-GVO sieht vor, dass die europäischen Aufsichtsbehörden bei grenzüberschreitenden Fällen zusammenarbeiten.[345] Im Rahmen des Kooperationsverfahrens wird dazu eine federführende Aufsichtsbehörde bestimmt, die die Ermittlungen in dem jeweiligen Fall führt.[346] Weitere Aufsichtsbehörden können sich als betroffene Behörden melden, wenn der Verantwortliche eine Niederlassung in ihrem Land hat oder die Verarbeitung erhebliche Auswirkungen auf betroffene Personen in dem jeweiligen Land hat. Dabei kooperieren die jeweiligen Aufsichtsbehörden eng miteinander.[347]

Nach Abschluss der Ermittlungen legt die federführende Aufsichtsbehörde den betroffenen Aufsichtsbehörden einen Beschlussentwurf zur Stellungnahme vor.[348]

Insgesamt veröffentlichte unsere Behörde in diesem Jahr 13 Beschlussentwürfe und 14 endgültige Beschlüsse. Zur Abstimmung und Kooperation nutzen die europäischen Aufsichtsbehörden das elektronische Binnenmarkt-Informationssystem (IMI).

Die nachfolgende Tabelle gibt einen Überblick über die Beteiligung unserer Behörde an den wichtigsten dieser europäischen Verfahren.

Europäische Verfahren	
Art. 56-Verfahren (betroffen)	253
Art. 56-Verfahren (federführend)	41
Art. 60ff-Verfahren	27

[345] Siehe 16.2 und JB 2018, 1.1
[346] Siehe Art. 56 Abs. 1 DS-GVO
[347] Siehe Art. 60 Abs. 1 bis 3 Satz 1 und Art. 61, 62 DS-GVO
[348] Siehe Art. 60 Abs. 3 Satz 2 DS-GVO