20. Wahlperiode

Drucksache **20/9575**

HESSISCHER LANDTAG

18. 04. 2023

Einundfünfzigster Tätigkeitsbericht zum Datenschutz und Fünfter Bericht zur Informationsfreiheit

Hessischer Beauftragter für Datenschutz und Informationsfreiheit

vorgelegt zum 31. Dezember 2022
vom Hessischen Beauftragten für Datenschutz und
Informationsfreiheit Prof. Dr. Alexander Roßnagel
nach Art. 59 der Verordnung (EU) Nr. 2016/679 i. V. m.
§ 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und
§ 89 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

Eingegangen am 18. April 2023 · Ausgegeben am 18. April 2023
Gestaltung: Satzbüro Peters, Taunusstein · Herstellung: AC medienhaus, Wiesbaden · Landtagsinformationssystem: www.Hessischer-Landtag.de

Einundfünfzigster Tätigkeitsbericht zum Datenschutz
und
Fünfter Tätigkeitsbericht zur Informationsfreiheit

des

Hessischen Beauftragten für Datenschutz
und Informationsfreiheit

Professor Dr. Alexander Roßnagel

vorgelegt zum 31. Dezember 2022
gemäß Art. 59 der Verordnung (EU) Nr. 2016/679 i. V. m.
§ 15 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes
sowie § 89 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes

Beiträge zum Datenschutz und zur Informationsfreiheit
Herausgegeben vom Hessischen Beauftragten für Datenschutz und Informationsfreiheit
Prof. Dr. Alexander Roßnagel
Gustav-Stresemann-Ring 1, 65189 Wiesbaden
Postfach 31 63, 65021 Wiesbaden

Telefon: (06 11) 14 08-0
E-Mail: poststelle@datenschutz.hessen.de
Internet: www.datenschutz.hessen.de

Drucksache des Hessischen Landtags 20/9575

Technisch-organisatorische Betreuung: Frauke Börner (HBDI)
Gestaltung: Satzbüro Peters, www.satzbuero-peters.de
Herstellung: AC medienhaus GmbH, Ostring 13, 65205 Wiesbaden-Nordenstadt

Inhaltsvezeichnis

II Zweiter Teil
5. Tätigkeitsbericht zur Informationsfreiheit

Anhang zu II

Kernpunkte

1. Für den Datenschutz in Hessen waren im Berichtszeitraum keine schwerwiegenden Verstöße festzustellen – ganz im Gegensatz zur Entwicklung in Deutschland oder in der Welt. In Hessen wurde Datenschutz weitgehend akzeptiert und nicht grundsätzlich in Frage gestellt. Dennoch sind in vielen Bereichen die Anforderungen der Datenschutz-Grundverordnung (DS-GVO) noch immer nicht ausreichend umgesetzt, führen zu Beschwerden und erfordern das Eingreifen der Datenschutzaufsicht. Die meisten Verantwortlichen beseitigen datenschutzwidrige Zustände umgehend. Soweit dies nicht der Fall war, halfen förmliche Anordnungen, Durchsetzungsmaßnahmen und Sanktionen. Die Digitalisierung vieler Aufgaben und Tätigkeiten verursacht für die Verantwortlichen zusätzliche Pflichten, bringt zusätzliche Anforderungen mit sich und erfordert zusätzliche Aufmerksamkeit (Teil I Kap. 1).
2. Datenschutzrecht durchzusetzen, wird durch Techniksysteme, Dienstleistungen, Auftragnehmer und Geschäftsmodelle in Frage gestellt, die nicht den Anforderungen des Datenschutzes entsprechen, weil die Anbieter nicht in der Lage oder nicht willens sind, die europäischen Datenschutzanforderungen zu erfüllen. Verantwortliche in Hessen, die sie in Anspruch nehmen, sind im Regelfall nicht in der Lage, ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO zu entsprechen. Daher kommt es darauf an, soweit möglich technisch-organisatorische Alternativen zu den aus dem Drittland angebotenen Hardware, Software, Diensten und Plattformen zu nutzen und dadurch digitale Souveränität zu erringen (Teil I Kap. 2). Hierzu konnten im Berichtsjahr im Bereich der Videokonferenzen deutliche Erfolge erzielt werden (Teil I Kap. 3).
3. Für die Weiterentwicklung des Datenschutzes in Hessen gewinnt die Europäisierung mit Entscheidungen des Europäischen Gerichtshofs (EuGH) und des Europäischen Datenschutzausschusses (EDSA) (Teil I Kap. 1 und 4) sowie die Juridifizierung des Datenschutzrechts mit einem leichten Anstieg der Bußgeldbescheide (von 29 im Jahr 2021 auf 113 im Jahr 2022) und Gerichtsverfahren (von 34 im Jahr 2021 auf 35 im Jahr 2022) (Teil I Kap. 1 und 5) zunehmend an Bedeutung. Dies erfordert stärkere Einflussnahme auf die europäischen Entwicklungen durch engagierte Mitarbeit in Arbeitskreisen des EDSA und den Ausbau des Justiziariats zur Bewältigung der zusätzlichen Prozessverfahren.
4. Während in den beiden Vorjahren die Corona-Pandemie die Arbeit der Datenschutzaufsicht sehr stark prägte, änderte sich dies im Jahr 2022. Die Corona-Pandemie ebbte im Laufe des Jahres ab, neue Schutzmaß-

nahmen kamen nicht mehr dazu, sie wurden im Gegenteil nach und nach abgebaut. Damit reduzierten sich auch die mit ihnen verbundenen Datenschutzprobleme.

5. Nach wie vor war ein zentraler Schwerpunkt der Aufsichtstätigkeit die Bearbeitung von Beschwerden, Nachfragen und Beratungen zur Ausübung von Betroffenenrechten sowie zur Unterstützung von Verantwortlichen. Die Zahl der schriftlich zu bearbeitenden Vorgänge stabilisiert sich fünf Jahre nach dem Wirksamwerden der DS-GVO auf einem sehr hohen Niveau. Sie sank leicht von 8.404 auf 6.836. Durch die zunehmende Digitalisierung wird die Bearbeitung der Vorgänge aber qualitativ anspruchsvoller. Große Digitalisierungsprojekte, wie z. B. die Umsetzung des Onlinezugangsgesetzes oder das Hessische Schulportal schlagen in der Statistik nicht in dem Ausmaß zu Buche, wie sie meine Behörde tatsächlich beschäftigen (Teil I Kap. 19).
6. Meldungen von Datenschutzverstößen gemäß Art. 33 DS-GVO bilden mittlerweile einen Großteil der reaktiven Tätigkeit meiner Aufsichtsbehörde. Neue Formen von Cyberkriminalität wie Phishing- und Ransomware-Angriffe, das Ausnutzen von Sicherheitsschwachstellen und das Veröffentlichen personenbezogener Daten im Darknet nahmen im Berichtszeitraum leicht ab (von 2.016 im Jahr 2021 auf 1.754 im Jahr 2022), verursachten aber weiterhin neue Gefährdungen der betroffenen Personen und der Verantwortlichen (Teil 1 Kap. 17).
7. In den Verwaltungsbehörden des Landes und der Kommunen werden derzeit große und anspruchsvolle Digitalisierungsprojekte konzipiert, geplant und umgesetzt, die eine intensive Beteiligung und kritische Mitarbeit der Datenschutzaufsicht erfordern (Teil I Kap. 7).
8. Die Schulen und Hochschulen waren vor allem geprägt durch starke Entwicklungen zu mehr Digitalisierung von Unterricht und Prüfungen, Lehre und Lernen. Beim Einsatz von datenschutzgerechten Videokonferenzsystemen konnten große Fortschritte erzielt werden (Teil I Kap. 3). Im Schulbereich begleitete ich die Entwicklungen des Hessischen Schulportals und weiterer Digitalisierungsprojekte (Teil I Kap. 8).
9. Die Digitalisierung der Arbeit führt dazu, dass in Beschäftigtenverhältnissen die Arbeitgeber immer intensiver die Leistung und das Verhalten der Beschäftigten überwachen können. In diesem Bereich musste meine Behörde in mehreren Fällen korrigierend eingreifen (Teil I Kap. 11).
10. Die partielle Volkszählung 2022 wurde von mir intensiv begleitet und kontrolliert. Außer kleineren Nachlässigkeiten waren keine gravierenden Datenschutzverstöße festzustellen (Teil I Kap. 9).

11. Bei der Polizei, dem Landesamt für Verfassungsschutz und mehreren Staatsanwaltschaften stellten Datenschutzprüfungen keine gravierenden Verstöße gegen datenschutzrechtliche Vorgaben fest. Kritische Anmerkungen habe ich zur geplanten Novelle des HSOG im Gesetzgebungsverfahren sowie zur gesetzlichen Grundlage für eine umfassende Auswertung aller polizeilichen Datensammlungen in einem Verfassungsbeschwerdeverfahren vor dem Bundesverfassungsgericht vorgetragen (Teil I Kap. 6).
12. Hinsichtlich der Internetnutzung musste ich viele Verstöße durch Profilbildungen mit Hilfe von Cookies, durch die Geschäftsmodelle von Social Media und durch Werbemaßnahmen feststellen (Teil I Kap. 12).
13. Im Bereich der privaten Wirtschaft musste ich vielen Detailfragen zu Datenverarbeitungen bei Banken, Auskunfteien, Steuerberatern und unterschiedlichen Unternehmen nachgehen (Teil I Kap. 14).
14. Im Gesundheitsbereich waren im ersten Halbjahr 2022 noch einige Datenschutzverstöße im Kontext der Corona-Pandemie zu verfolgen. Stärker waren jedoch Probleme der Digitalisierung zu bearbeiten wie etwa zur Patientenakte, zum Upload medizinischer Bilder oder zur elektronischen Auskunftserteilung (Teil I Kap. 15).
15. Ein Schwerpunktthema im Berichtszeitraum war die Unterstützung der Forschung durch Datenschutz. In diesem Bereich waren Lösungen zu finden, die Forschungsprojekte im Allgemeininteresse ermöglichen, zugleich aber durch überzeugende Datenschutzmaßnahmen das Vertrauen der Patienten gewinnen (Teil I Kap. 16).
16. Obwohl die Informationsfreiheit in Hessen immer noch nur in der Landesverwaltung und wenigen Gemeinden und Landkreisen gilt, hatte ich als Informationsfreiheitsbeauftragter im Berichtsjahr viele interessante Fragen zur Informationsfreiheit zu beantworten und unterstützte viele Bürgerinnen und Bürger bei der Durchsetzung ihrer Ansprüche. Außerdem beteiligte ich mich an der rechtspolitischen Fortentwicklung der Informationsfreiheit und arbeitete in der Konferenz der Informationsfreiheitsbeauftragten (IFK) mit (Teil II). Beschwerden und Beratungen sanken leicht von 123 auf 110.

Vorwort

Dies ist der 51. Tätigkeitsbericht zum Datenschutz und der 5. Tätigkeitsbericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit. Mit diesen Berichten erfülle ich meine Informationspflichten nach Art. 59 Datenschutz-Grundverordnung (DS-GVO) sowie §§ 15 Abs. 3 und § 89 Abs. 4 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG).

Nach diesen Vorschriften habe ich jeweils zum Stichtag des 31. Dezember jedes Jahres dem Landtag und der Landesregierung einen Bericht über das Ergebnis meiner Tätigkeit in den Bereichen des Datenschutzes und der Informationsfreiheit vorzulegen und Verbesserungen des Datenschutzes anzuregen. Außerdem habe ich den Tätigkeitsbericht zum Datenschutz der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich zu machen.

Die Tätigkeitsberichte haben die Funktion, die aktuelle Praxis des Datenschutzes und der Informationsfreiheit in Hessen sowie die Möglichkeiten der Aufsichtsbehörde, auf diese zugunsten der Grundrechte und der Demokratie Einfluss zu nehmen, zu beschreiben und zu analysieren.

Der 51. Tätigkeitsbericht zum Datenschutz, der die Entwicklungen im Jahr 2022 umfasst, beschreibt Bedingungen und Ergebnisse der Aufsichtstätigkeit im Bereich des Datenschutzes. Das Grundrecht auf Datenschutz schützt die Selbstbestimmung des Individuums über seine Daten und ist zugleich eine Zielsetzung der gesellschaftlichen Ordnung und Entwicklung zum Schutz von Demokratie und Rechtsstaat. Die Datenschutzaufsicht hat die grundsätzliche Aufgabe, diese individuelle und gesellschaftliche Selbstbestimmung im Rahmen der Rechtsordnung gegenüber den Stellen, die die Verarbeitung personenbezogener Daten zur Steigerung ihrer Macht nutzen, zu verteidigen und Machtungleichgewichte, die durch die Datenverarbeitung entstehen, auszugleichen.

Diese Aufgabe wird jedoch immer schwieriger und verursacht neue Herausforderungen für die Hessische Datenschutzaufsicht. Die Digitalisierung aller Gesellschaftsbereiche führt zu einer intensiveren Verarbeitung personenbezogener Daten und die Geschäftsmodelle weltweiter Konzerne erschweren die Durchsetzung von Datenschutz, weil sie sich vielfach der Datenschutzaufsicht entziehen. Das Eindringen der Informationstechnik in den Alltag erfasst alltägliche Handlungen und führt zu einer „Explosion“ personenbezogener Daten. Dennoch ist es der Hessischen Datenschutzaufsicht gelungen, auch im Jahr 2022 an vielen Stellen und in vielen Verfahren Datenschutz durchzusetzen.

Für die Wahrnehmung der Grundrechte und die Teilnahme an der demokratischen Willensbildung ist in einer digitalen Gesellschaft neben dem Datenschutz der Zugang zu öffentlichen Informationen von besonderer Bedeutung. Diese Informationsfreiheit ist in Hessen erst seit 2018 im Gesetz vorgesehen. Ihre praktische Inanspruchnahme und Erfüllung muss sich in Hessen erst noch entwickeln. Der Informationszugang ist im Gesetz zu den Informationen der Landesverwaltung vorgesehen, für die Gemeinden und Landkreise aber nur, wenn sie die Anwendung des Anspruchs auf Informationszugang für ihre öffentlichen Stellen durch Satzung ausdrücklich festgelegt haben. Dies haben bisher nur wenige Gemeinden und Landkreise beschlossen. Hier werden in den nächsten Jahren weitere Diskussionen zu den Vor- und Nachteilen eines Informationsanspruchs zu führen sein. Für mich ist die weitere Entwicklung und Durchsetzung des Informationszugangs zu öffentlichen Stellen eine wichtige Aufgabe.

Prof. Dr. Alexander Roßnagel

I
Erster Teil
51. Tätigkeitsbericht zum Datenschutz

1. Neue Aufgaben und Rahmenbedingungen

Der vorliegende Tätigkeitsbericht beschreibt und analysiert den Datenschutz in Hessen im Jahr 5 seit dem Geltungsbeginn der Datenschutz-Grundverordnung am 25. Mai 2018. Viele Unsicherheiten, die der neue sehr abstrakte Rechtsrahmen für die Praxis des Datenschutzes gebracht hat, sind überwunden. Viele Streitfragen sind inzwischen geklärt, andere sind noch immer in der Diskussion, neue Fragestellungen kommen hinzu. Diese betreffen vor allem komplexe Herausforderungen großer Digitalisierungsprojekte in allen Bereichen der Gesellschaft. Die Europäisierung des Datenschutzes, aber auch die Zusammenarbeit der Aufsichtsbehörden in Deutschland schreiten voran und verändern zunehmend die Aufgaben und Handlungsmöglichkeiten der Datenschutzaufsicht.

Corona-Pandemie

In den beiden Vorjahren prägte die Corona-Pandemie die Arbeit der Datenschutzaufsicht sehr stark – sowohl durch immer wieder neue inhaltliche Herausforderungen (s. 50. Tätigkeitsbericht, Kap. 2) als auch durch ihre Auswirkungen auf den Arbeitsmodus der Aufsichtsbehörde (s. 50. Tätigkeitsbericht, Kap. 1). Dies änderte sich im Jahr 2022. Die Corona-Pandemie ebbte im Laufe des Jahres ab, neue Schutzmaßnahmen kamen keine mehr dazu, sie wurden im Gegenteil nach und nach abgebaut. Damit reduzierten sich auch die mit ihnen verbundenen Datenschutzprobleme. Solche waren weitgehend nur noch in der ersten Jahreshälfte zu bearbeiten. Beispiele waren die Datenverarbeitungen im Rahmen von Testverfahren (Kap. 15.4) und der postalische Versand von COVID-Impfzertifikaten (s. Kap. 15.6). In gleichem Maße konnten auch die behördeninternen Maßnahmen, um die Arbeitsfähigkeit der Aufsichtsbehörde aufrechtzuerhalten, nach und nach zurückgenommen werden. Der Pandemiemodus der Arbeit in der Dienststelle wich der Arbeit nach der neuen Dienstvereinbarung zum mobilen Arbeiten. Nach dieser können die Beschäftigten bis zu drei Tagen in der Woche ihre Arbeitsleistung im Homeoffice oder an anderen geeigneten Stellen erbringen. Mit dieser Dienstvereinbarung hat die Aufsichtsbehörde die guten Erfahrungen mit mobilem Arbeiten aus der Pandemiezeit in die Normalität des Arbeitslebens übertragen. Das Abebben der Pandemie erlaubte es auch, wieder externe Aufsichtstätigkeiten vor Ort wahrzunehmen.

Im Berichtszeitraum erhalten blieb jedoch die Aufgabe, die datenschutzrechtswidrigen Zustände, die zu Beginn der Corona-Pandemie und während des ersten Lockdowns im Frühjahr 2020 zur Bewältigung der damaligen Notsituation geduldet werden mussten, wieder an die datenschutzrechtlichen

Anforderungen anzupassen. Dies beanspruchte die Aufsichtsbehörde sehr. Doch konnte sie – insbesondere bei der Nutzung von Videokonferenzsystemen – die Verantwortlichen unterstützen, entscheidende Fortschritte zu erzielen (s. Kap. 3).

Digitalisierungsprojekte

Die Digitalisierung dringt in allen Gesellschaftsbereichen weiter voran. Dies führt zu großen Digitalisierungsprojekten in Wirtschaft und Verwaltung, die meist auf digitalen Plattformen aufsetzen und mit deren Hilfe eigene Anwendungen entwickeln. Für diese kommt es darauf an, dass datenschutzrechtliche Anforderungen von Anfang an berücksichtigt werden. Hierfür bietet es sich an, die professionelle Kompetenz der Aufsichtsbehörde in Form von Beratungen in Anspruch zu nehmen. Während z. B. die Corona-Pandemie vor allen viele kleinteilige Probleme des alltäglichen Lebens hervorgerufen hat, denen in der Bearbeitung des Einzelfalls nachzugehen war, stellen Digitalisierungsprojekte die Datenschutzaufsicht vor komplexere Herausforderungen: Hier geht es darum, die Bedingungen zu verändern, um Datenschutzanforderungen zu verwirklichen. Dies ist oft technisch-wirtschaftlich nicht mehr möglich, wenn in Digitalisierungsprojekten der Datenschutz erst nachträglich berücksichtigt wird. Ist die Konzeption schon fertiggestellt, sind Anwendungen bereits programmiert, die verfügbaren Mittel ausgegeben, das System eingeführt und die Arbeitsorganisation umgestellt, ist die Erfüllung datenschutzrechtlicher Anforderungen oft sehr teuer, extrem aufwändig oder sogar gar nicht mehr möglich. Die Aufsichtsbehörde muss daher versuchen, frühzeitig einzugreifen und die Probleme für den Datenschutz zu erkennen und – am besten mit den Beteiligten zusammen – durch Gestaltung der Systeme zu lösen.

Dieses Problem verstärkt sich, wenn die Digitalisierungsprojekte auf Plattformen internationaler Konzerne aufsetzen, die technische Systeme betreiben und Geschäftsmodelle verfolgen, die mit den datenschutzrechtlichen Anforderungen unvereinbar sind. Hier besteht das Problem, dass die Betreiber solcher Plattformen meist ihren Sitz in Irland haben, so dass ich nicht unmittelbar dafür zuständig bin, sie zu datenschutzkonformem Verhalten anzuhalten. Da sie ihre Plattformen meist über eine Cloud als Auftragsverarbeiter anbieten, sind für die datenschutzgerechte Nutzung der Plattformen die sie nutzenden Verantwortlichen in Hessen zuständig. Daher bin ich gezwungen, diese zu einem datenschutzgerechten Verhalten anzuhalten – und nicht die Plattformanbieter, die eigentlich für die Datenschutzwidrigkeit ihrer Plattformnutzung ursächlich sind. Jedoch sind die Verantwortlichen dafür verantwortlich, welche Techniksysteme sie nutzen. Das Ziel muss es daher sein, die Verantwortlichen in Hessen dazu zu bringen, Techniksysteme zu

nutzen, die ihnen ermöglichen, datenschutzrechtliche Anforderungen zu erfüllen (s. zur digitalen Souveränität Kap. 2).

Rechtsprechung des Europäischen Gerichtshofs

Das nationale Datenschutzrecht und die Tätigkeit der Aufsichtsbehörden werden immer stärker durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH) geprägt. Er hat inzwischen einige wichtige Entscheidungen zum Datenschutz und zur Auslegung der DS-GVO getroffen und durch sie bestehende Streitfragen geklärt. Aber jede Entscheidung konzentriert sich auf ihren Entscheidungsgegenstand und enthält doch auch immer über ihn hinausweisende Bemerkungen. Dadurch hinterlassen die Entscheidungen viele neue Fragen, über die gestritten wird und die Rechtsunsicherheit für Verantwortliche und Aufsichtsbehörden bewirken (s. 50. Tätigkeitsbericht, Kap. 1).

Im Berichtsjahr war vor allem die Entscheidung vom 20. September 2022 (C-793 und C-794/19, ZD 2022, 666) zur Vorratsdatenspeicherung in Deutschland bedeutsam (s. näher Roßnagel, Vorratsdatenspeicherung – was geht noch und was nicht mehr?, ZD 2022, 650 ff.). In seinem Urteil hat der EuGH in Übereinstimmung mit seiner inzwischen gefestigten (zur Vorratsdatenspeicherungs-Richtlinie EuGH vom 8. April 2014, C-288/12, MMR 2014, 412; zu den Regelungen in Schweden und Großbritannien EuGH vom 21. Dezember 2016, C-203 und 698/15, ZD 2017, 124; zu den Regelungen in Frankreich, Belgien und Großbritannien EuGH vom 6. Oktober 2020, C-511/18 u. a., ZD 2021, 520; zu den Regelungen in Estland EuGH vom 2. März 2021, C-746/18, ZD 2021, 517 und zu den Regelungen in Irland EuGH vom 5. April 2022, C-140/20, ZD 2022, 677) und weitergeführten Rechtsprechung (zur Vorratsdatenspeicherung in Bulgarien EuGH vom 17. November 2022, C-350/21) die permanente Pflicht der Anbieter elektronischer Kommunikationsdienste nach §§ 113a ff. TKG 2015, die Verkehrs- und Standortdaten nahezu aller Teilnehmer anlasslos und flächendeckend auf Vorrat zu speichern, als unionsrechtswidrig bewertet. Diese Entscheidung ist für die weitere Gesetzgebung und für die Interpretation bestehender Regelungen im Bereich der inneren Sicherheit von zentraler Bedeutung.

Regelungen, die eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen, erfassen die elektronischen Kommunikationen fast der gesamten Bevölkerung, ohne jede Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels. Sie betreffen somit auch „Personen, bei denen keinerlei Anhaltspunkt dafür besteht, dass ihr Verhalten in einem auch nur mittelbaren oder entfernten Zusammenhang mit dem Ziel der Bekämpfung schwerer Straftaten stehen könnte“, und

setzen „insbesondere keinen Zusammenhang zwischen den Daten, deren Vorratsspeicherung vorgesehen ist, und einer Bedrohung der öffentlichen Sicherheit voraus“. Sie beschränken die Vorratsdatenspeicherung „weder auf die Daten eines Zeitraums und/oder eines geografischen Gebiets und/oder eines Personenkreises, der in irgendeiner Weise in eine schwere Straftat verwickelt sein könnte, noch auf Personen, deren auf Vorrat gespeicherte Daten aus anderen Gründen zur Bekämpfung schwerer Kriminalität beitragen könnten“ (EuGH, ZD 2022, 666 Rn. 66.).

Selbst die Verpflichtungen der Mitgliedstaaten zur Sicherung der Grundrechte aus den Art. 3, 4 und 7 GRCh können „keine so schwerwiegenden Eingriffe rechtfertigen“ (EuGH, ZD 2022, 666 Rn. 123). Auch wenn sie das Ziel verfolgen, schwere Kriminalität zu bekämpfen und ernste Bedrohungen der öffentlichen Sicherheit zu verhüten, überschreiten sie „die Grenzen des absolut Notwendigen“ und können „nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden“. Verkehrs- und Standortdaten dürfen daher „nicht Gegenstand einer systematischen und kontinuierlichen Speicherung sein“ (EuGH, ZD 2022, 666 Rn. 74.). Selbst eine dem Gemeinwohl dienende Zielsetzung – wie die Bekämpfung der Kinderpornografie – „kann, so grundlegend sie auch sein mag, für sich genommen die Erforderlichkeit einer Maßnahme der allgemeinen und unterschiedslosen Vorratsdatenspeicherung von Verkehrs- und Standortdaten … nicht rechtfertigen“ (EuGH, ZD 2022, 666 Rn. 123f.).

Diese Feststellungen schließen jede klassische Vorratsdatenspeicherung aus. Sie lassen aber auch den Vorschlag der Kommission, die Betreiber elektronischer Kommunikation zu verpflichten, anlasslos, flächendeckend, ohne Ausnahme und zeitlich unbegrenzt elektronische Kommunikation danach zu untersuchen, ob Hinweise auf Kinderpornografie enthalten sind, und hierfür auch verschlüsselte Kommunikation zu entschlüsseln, als unvereinbar mit Unionsrecht erscheinen.

Für den EuGH dürfen jedoch die Sicherheitspflichten und die Sicherheitsinteressen der Mitgliedstaaten nicht unberücksichtigt bleiben. Sie rechtfertigen je nach Bedrohung der Sicherheit und der Schwere der Grundrechtseingriffe auf das jeweils absolut Notwendige beschränkte, gesetzlich geregelte und gegen Missbrauch abgesicherte Eingriffe in die Grundrechte aus Art. 7, 8 und 11 CRCh. So lässt er z. B. (zu weiteren Ausnahmen s. Roßnagel, ZD 2022, 650, 653 ff.) sehr enge Ausnahmen für die Speicherung von IP-Adressen zu: Für den EuGH entscheidend ist, dass bei einer Straftat im Internet und insbesondere im Fall von Kinderpornografie die IP-Adresse der einzige Anhaltspunkt sein kann, die Identität des Täters zu ermitteln. Aufgrund der Schwere des Grundrechtseingriffs darf dieser nur zum Schutz der „nationalen

Sicherheit“ oder zur „Bekämpfung schwerer Kriminalität und der Verhütung schwerer Bedrohungen der öffentlichen Sicherheit“ erfolgen. „Außerdem darf die Dauer der Speicherung das im Hinblick auf das verfolgte Ziel absolut Notwendige nicht überschreiten. Schließlich muss eine derartige Maßnahme strenge Voraussetzungen und Garantien hinsichtlich der Auswertung dieser Daten, insbesondere in Form einer Nachverfolgung, in Bezug auf die Online-Kommunikationen und -Aktivitäten der Betroffenen vorsehen“ (EuGH, ZD 2022, 666, Rn. 102). Die Speicherung von IP-Adressen könnte daher ausschließlich für die Quelle der Kommunikation bei strikter Einhaltung der Verhältnismäßigkeit und bei absoluter Notwendigkeit der jeweiligen Maßnahme unionsrechtlich vertretbar sein.

Europäische Gesetzesinitiativen

2022 war ein Jahr europäischer Gesetzesinitiativen zur Digitalisierung, die den Datenschutz zutiefst berühren können, auch wenn er nicht ihr Thema ist. Die fünf wichtigsten Initiativen sind die folgenden:

– Der Digital Market Act (DMA) vom 14. September 2022 (EU ABl. L 265 vom 12. Oktober 2022) ist als EU-Verordnung am 2. November 2022 in Kraft getreten und gilt in den Mitgliedstaaten ab dem 2. Mai 2023. Sie regelt wichtige Aspekte der europäischen Digitalwirtschaft und soll das Funktionieren eines fairen digitalen Binnenmarktes schützen. Deshalb enthält sie besondere Anforderungen an zentrale Plattformdienste, die als Torwächter durch ihre Monopolmacht, die auf großen Sammlungen personenbezogener Daten beruht, die Marktwirtschaft gefährden und Gewerbetreibende und Verbraucher unfair behandeln.
– Der Digital Services Act (DSA) vom 19. Oktober 2022 (EU-ABl. L 277 vom 27. Oktober 2022, 1) ist als EU-Verordnung (EU) 2022/2065 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG am 16. November 2022 in Kraft getreten und gilt in den Mitgliedstaaten in Teilen ab dem 16. November 2022, ansonsten ab dem 17. Februar 2024. Er aktualisiert den EU-Rechtsrahmen für den elektronischen Geschäftsverkehr, regelt Anforderungen an digitale Dienstleistungen neu und legt Sorgfaltspflichten für Anbieter von Vermittlungsdiensten, insbesondere Online-Plattformen wie soziale Medien und Marktplätze, fest.
– Der Artificial Intelligence Act (AIA) liegt als Entwurf der EU-Kommission vom 21. April 2021 vor (COM(2021) 206 final) vor. Das Rechtsetzungsverfahren zu dieser EU-Verordnung ist schon recht weit gediehen. Sie wird das Angebot und die Nutzung von IT-Systemen für künstliche Intelligenz regeln, um die Entwicklung eines Binnenmarkts für rechtskonforme, sichere und vertrauenswürdige KI-Anwendungen zu erleichtern. Sie

verbietet bestimmte Systeme mit unvertretbaren Risiken und fordert von Hochrisikosystemen eine hohe Transparenz, Risikovorsorge und Konformitätsbewertungen.

– Der Data Governance Act (DGA) vom 30. Mai 2022 (EU ABl. L 152 vom 3.6.2022, 1) ist zum 24. Juni 2022 als EU-Verordnung (EU) 2022/868 in Kraft getreten und gilt in den Mitgliedstaaten ab dem 24. September 2023. Sie ordnet die Infrastruktur einer künftigen Datenwirtschaft, indem sie die Datenbereitstellung durch öffentliche Stellen, einen Datenmarkt mit Datenmittlern und Datenaltruismus durch Datenspenden an Treuhänder regelt.
– Der Data Act (DA) beruht auf einem Entwurf einer Verordnung der EU-Kommission vom 23. Februar 2022 (COM(2022) 68 final) und wird derzeit im Gesetzgebungsprozess verhandelt. Sie wird Anforderungen an die europäische Datenwirtschaft enthalten und Pflichten zur Preisgabe von Daten sowie Rechte zum Zugang und zur Nutzung von Daten regeln.

Alle diese beschlossenen und künftigen Verordnungen berühren auch immer den Datenschutz, weil der weite Begriff von personenbezogenen Daten viele der Daten umfasst, deren Umgang durch sie geregelt wird. Sie alle bestimmen zwar, dass die DS-GVO auch für personenbezogene Daten in ihrem jeweiligen Anwendungsbereich gilt. Doch regeln sie auch die Bedingungen der Weitergabe, Veröffentlichung und Nutzung dieser Daten und haben damit Einfluss auf die Verwirklichungsbedingungen der Regelungen in der DS-GVO. Dies betrifft vor allem die Vorgaben zur Zulässigkeit der Datenverarbeitung, zu den Rechten der betroffenen Personen und zu den Pflichten der Verantwortlichen. Hierdurch ergeben sich viele rechtliche Fragen, die weder von der DS-GVO noch von den neuen Verordnungen beantwortet werden.

Auch die Datenschutzaufsicht ist von diesen Regelungen betroffen. Diese Verordnungen sehen zwar vor, dass die Aufsicht über die Verarbeitung personenbezogener Daten bei den unabhängigen Datenschutzaufsichtsbehörden verbleibt. Sie etablieren aber für ihre jeweiligen spezifischen Zielsetzungen weitere Aufsichtsregime mit jeweils eigenen Aufsichtsbehörden, deren Kompetenzen von denen der Datenschutzaufsichtsbehörden abgegrenzt werden müssen. Außerdem müssen alle diese Aufsichtsbehörden zusammenarbeiten. Auch durch diese Konkurrenz und Kooperation entstehen viele künftige Herausforderungen, auf die sich die Datenschutzaufsichtsbehörden einstellen müssen.

Alle diese neuen Regelungen fördern die Nutzung personenbezogener Daten. In besonderer Weise ist dies das Ziel des DGA und des DA, die einen Daten-Binnenmarkt initiieren und fördern wollen. Zu diesem Zweck verfolgt die EU-Kommission das Ziel, 13 europäische Datenräume zu initiieren. Für den ersten Datenraum, einen für Gesundheitsdaten, hat sie bereits eine

Verordnung für einen „Europäischen Raum für Gesundheitsdaten“ in den Gesetzgebungsprozess eingebracht. Auch viele nationale Gesetzesvorhaben sollen die Nutzung von personenbezogenen Daten fördern – wie etwa die im Koalitionsvertrag vorgesehenen Gesetzesinitiativen für ein Forschungsdatengesetz und ein Gesundheitsdatennutzungsgesetz. Als neue Herausforderungen der Datenschutzaufsicht entstehen vielfältige Fragen, wie sie die Zielsetzungen der umfassenden Datennutzung und des gebotenen Datenschutzes in Einklang bringen kann. Die datenschutzrechtlichen Ziele der Zweckbindung und der Datenminimierung scheinen auf den ersten Blick einer breiten Datennutzung entgegenzustehen. Vereinbaren wird die konträren Ziele wohl vor allem eine Technikgestaltung, die zur Anonymisierung personenbezogener Daten führt oder eine Datenauswertung an der Quelle der Daten ermöglicht oder die personenbezogenen Daten mit besonderen technisch-organisatorischen Garantien schützt (s. z. B. Kap. 16.1). Die damit verbundenen Fragen der Konzeption und Umsetzung solcher Techniksysteme datenschutzgerechter Datennutzung beschäftigte die Aufsichtsbehörden im Berichtszeitraum in starkem Maße.

Europäische Zusammenarbeit

Nicht nur die Unionsgesetzgebung und die Rechtsprechung des EuGH, sondern auch die Vorgaben der DS-GVO zur unionsweiten Zusammenarbeit der Aufsichtsbehörden führen zu einer immer weitergehenden Europäisierung des Datenschutzrechts (s. hierzu auch 50. Tätigkeitsbericht, Kap. 1).

Zum einen arbeiten die Aufsichtsbehörden im Europäischen Datenschutzausschuss (EDSA) zusammen. Dieser legt in Form von Empfehlungen, Leitlinien und Stellungnahmen abstrakt fest, wie Regelungen in der DS-GVO im Praxisvollzug zu verstehen sind und wie zwischen den Aufsichtsbehörden entstehende Streitfragen zu entscheiden sind. Damit trägt er entscheidend zur Rechtssicherheit im Datenschutzrecht der Union bei. Auch kann er in umstrittenen Fragen die nationale Aufsichtsbehörde überregeln und zu bestimmten Handlungen anweisen (s. Kap. 4.2). Wer darauf einwirken will, wie der Datenschutz künftig in der Union verstanden und praktiziert wird, muss sich aktiv in die Arbeit des EDSA und seiner Arbeitskreise einbringen.

Um einen einheitlichen Vollzug des Datenschutzes in der Union sicherzustellen, sieht die DS-GVO eine enge grenzüberschreitende Zusammenarbeit der Aufsichtsbehörden in den Mitgliedstaaten vor. Berührt ein Aufsichtsverfahren mehrere Mitgliedstaaten, sollen sich die Aufsichtsbehörden über die erforderlichen Maßnahmen einigen. Kommt keine Einigung zustande, entscheidet der EDSA in dem umstrittenen Aufsichtsverfahren abschließend. Diese von der DS-GVO verordnete Zusammenarbeit zwischen den Aufsichts-

behörden erweist sich vor allem deshalb als schwierig und aufwändig, weil ihr die notwendige kulturelle Grundlage fehlt. Alle Mitgliedstaaten haben unterschiedliche Datenschutztraditionen und unterschiedliche Verständnisse von Datenschutzaufsicht. Daher muss zwischen den Aufsichtsbehörden sehr oft über unterschiedliche Begriffsverständnisse, Vollzugspraktiken und Zielsetzungen in der Rechtsumsetzung verhandelt werden. Hinzu kommen die Sprachprobleme und die umständlichen Verfahren der Zusammenarbeit. Insgesamt setzt die DS-GVO einen Kulturwandel der Zusammenarbeit in allen Mitgliedstaaten voraus, den sie nicht selbst gewährleisten kann. Da aber in diesen Verfahren der Zusammenarbeit entschieden wird, wer Einfluss auf das künftige Verständnis des Datenschutzes in der Europäischen Union hat, ist eine intensive Beteiligung notwendig (s. Kap. 4.1). Dennoch ist es oft frustrierend, hilflos mitansehen zu müssen, wie die Datenschutzanforderungen, auf die sich alle Aufsichtsbehörden der Union geeinigt haben, für die weltweit agierenden Technologiekonzerne, für die es am wichtigsten wäre, praktisch nicht gelten, weil die zuständige Aufsichtsbehörde diese ihnen gegenüber nicht oder unzureichend durchsetzt.

Juridifizierung der Aufsichtstätigkeit

Die DS-GVO hat neue rechtliche Handlungsmöglichkeiten für betroffene Personen und die Aufsichtsbehörden geschaffen. Diese sind grundsätzlich zu begrüßen, führen aber zu einer stärkeren Juridifizierung der Aufsichtstätigkeit. Zum einen hat jede betroffene Person nach Art. 77 DS-GVO das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen die Verordnung verstößt. Ist sie mit der Bearbeitung ihrer Beschwerde nicht einverstanden, kann sie nach Art. 78 DS-GVO beim zuständigen Verwaltungsgericht eine Klage gegen den rechtsverbindlichen Abschluss des Beschwerdeverfahrens durch die Aufsichtsbehörde einlegen. Beide Rechte stärken den Grundrechtsschutz, weil sie der individuellen Rechtsdurchsetzung helfen und individuelle Selbstbestimmung gegenüber mächtigen Datenverarbeitern unterstützen können. Die Beschwerden sind für die Aufsichtsbehörden auch hilfreiche Mittel, um Erkenntnisse zur Praxis des Datenschutzes zu gewinnen. Zum anderen hat die DS-GVO in Art. 58 DS-GVO den Aufsichtsbehörden stärkere Befugnisse gegeben, Datenschutz in der Praxis durchzusetzen. Sie können gegenüber nicht öffentlichen Verantwortlichen Anordnungen zur Datenverarbeitung treffen und bei Verstoß gegen Datenschutzvorschriften empfindliche Bußgelder verhängen. Sowohl die neuen Rechte der betroffenen Personen als auch die größere Eingriffstiefe der neuen Befugnisse der Aufsicht in die Grundrechte von Unternehmen führen dazu, dass es zu einer steigenden Anzahl von Gerichtsprozessen kommt. Die Aussicht, dass ihre

Handlungen zunehmend gerichtlichen Überprüfungen unterzogen werden, prägt in immer stärkerer Weise den Aufgabenzuschnitt und den Charakter der Tätigkeiten der Aufsichtsbehörde. Diese werden förmlicher und umständlicher. Sie werden zunehmend geprägt von Fragen der Verfahrensrechte, der Aktenführung, der Darlegungslast, der Beweisführung und prozesstaktischen Überlegungen. Unvoreingenommene Beratungen und Hilfestellungen gegenüber den Verantwortlichen und den betroffenen Personen, die sehr schnell zum Prozessgegner werden können, werden schwieriger.

Die auf hohem Niveau sich einpendelnde Zahl der Beschwerden führt bei der Ressourcenausstattung der Aufsichtsbehörde zu dem Dilemma, dass die Aufsichtsbehörde der zunehmenden Arbeitslast nur gerecht werden kann, wenn sie Mittel der Arbeitsrationalisierung nutzt. Diese kann aber zur Unzufriedenheit bei den Personen führen, die Beschwerde eingelegt haben, und zu einem Anstieg der Klagen gegen die Aufsichtsbehörde. Diese wiederum erhöhen die Arbeitslast und gefährden das Ansehen der Aufsichtsbehörde als Treuhänder der Grundrechte der betroffenen Personen.

Durch die Juridifizierung der Aufsichtstätigkeit kommt der Rechtsprechung der nationalen Gerichte eine zunehmende Bedeutung für den Datenschutz zu (s. Kap. 5.1 und 5.2), ohne dass diese auf Datenschutzfragen spezialisiert sind. Dies kann eine einheitliche Anwendung der DS-GVO in der Europäischen Union erschweren (s. 50. Tätigkeitsbericht, Kap. 1). Daher ist es inhaltlich zu begrüßen, wenn ein Gericht wie das Verwaltungsgericht Wiesbaden umstrittene Auslegungsfragen nicht selbst entscheidet, sondern dem EuGH zur abschließenden Klärung vorlegt. Im Berichtszeitraum hat das Verwaltungsgericht Wiesbaden in sechs Verfahren vielfältige Rechtsfragen dem EuGH vorgelegt. Da ich dadurch jeweils zu einem Beteiligten der EuGH-Verfahren wurde, musste ich eine Anwaltskanzlei beauftragen und die Stellungnahmen vor dem EuGH zusammen mit den Anwälten in aufwändiger Arbeit erarbeiten.

Intensiv war im Berichtszeitraum auch die Teilnahme an einem Verfahren vor dem Bundesverfassungsgericht, dessen mündliche Verhandlung am 20. Dezember 2022 stattfand. Mit einer Verfassungsbeschwerde wandten sich mehrere Bürgerinnen und Bürger an das Gericht, weil sie in der potenziellen Verarbeitung ihrer Daten durch die Analyse-Software hessenData der hessischen Polizei eine Verletzung ihrer Grundrechte sahen. Ihrer Meinung nach war die Ermächtigungsnorm für diese Datennutzung in § 25a Hessisches Gesetz für Sicherheit und Ordnung (HSOG) verfassungswidrig (s. Kap. 6.1). Auch für dieses Verfahren waren die Arbeiten an meinem Schriftsatz aufwändig und die Vorbereitungen der mündlichen Verhandlung umfangreich.

Zusammenarbeit mit den Aufsichtsbehörden in Deutschland

Eine weitere wichtige Rahmenbedingung für die Wahrnehmung der Aufsichtsaufgaben besteht in der zunehmenden Notwendigkeit, die Aufsichtstätigkeit in Deutschland zu koordinieren. Die Hessische Aufsichtsbehörde ist Teil der deutschen Datenschutzaufsichtsstruktur. Die durch sie erfolgende Koordination ist zum einen notwendig, weil innerhalb der Union nur in Deutschland die Datenschutzaufsicht föderalistisch organisiert ist und Deutschland im EDSA nur eine Stimme hat. Die deutschen Aufsichtsbehörden müssen sich daher für die Willensbildung im EDSA auf jeweils eine Meinung verständigen.

Zum anderen ist eine Verständigung innerhalb Deutschlands in den Fragen notwendig, die Sachverhalte betreffen, die nicht nur Bedeutung für ein Bundesland haben. Dies ist im nicht öffentlichen Bereich der Datenverarbeitung regelmäßig der Fall und immer wieder in vielen Bereichen der Bund-Länder-Kooperation oder in der länderübergreifenden Zusammenarbeit. In den meisten Datenschutzfragen ist daher ein bundeseinheitlicher Vollzug von Datenschutzrecht gefragt. Für diesen arbeiten die Aufsichtsbehörden des Bundes und der Länder im Rahmen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) zunehmend enger zusammen. Das erfordert immer mehr Abstimmungen im Rahmen der Konferenz, in den fachlichen Arbeitskreisen der Konferenz und in einer steigenden Anzahl von Task Forces zu zeitlich befristeten gemeinsamen Aufgaben.

Vertreter meiner Behörde arbeiten in allen 25 Arbeitskreisen und in den meisten Task Forces der DSK mit. Ich habe den Vorsitz der Arbeitskreise „Organisation und Struktur“ und „Wissenschaft und Forschung“ inne sowie den Co-Vorsitz im Arbeitskreis „Auskunfteien“ und in der Task Force „Forschungsdaten“. Die Arbeitskreise tagen mindestens zwei Mal im Jahr und führen mehrfach Treffen in Unterarbeitskreisen durch. Die Task Forces beschäftigen sich mit dringenden oder arbeitskreisübergreifenden Fragen und tagen deutlich öfter.

Drittens müssen die Aufsichtsbehörden gemeinsame Konzepte und Strategien entwickeln, um sich gegenüber starken Datenverarbeitern durchsetzen zu können. Nur wenn sie gemeinsam auftreten und ihre Positionen gemeinsam durchfechten, haben sie Chancen, den Datenschutz in Deutschland voranzubringen. Die wichtigsten Entscheidungen fallen daher in den Gremien der DSK. Dementsprechend steigt im Rahmen der Aufsichtstätigkeit die Bedeutung der Mitarbeit in diesen Gremien und verändert damit zunehmend die Arbeitsaufgaben der Beschäftigten in der Aufsichtsbehörde.

Angesichts der Notwendigkeit zunehmender Kooperation hat die DSK einen Arbeitskreis „DSK 2.0“ gegründet, der die Verbindlichkeit der Zusammenarbeit

steigern und die Wahrnehmung einer einheitlichen Aufgabenerfüllung verbessern soll. Neben ihren halbjährlichen zweitägigen Konferenzen führt die DSK inzwischen zusätzlich mindestens drei eintägige Zwischenkonferenzen durch. Außerdem hat sie im Jahr 2021 einen wöchentlichen Jour fixe eingerichtet, um sich per Videokonferenz auch in alltäglichen Fragen gegenseitig zu informieren und sich abzustimmen. Weiterhin hat sie im Jahr 2022 ihre Geschäftsordnung – unter meiner Leitung – dahingehend weiterentwickelt, dass sie verbindliche Mehrheitsentscheidungen treffen kann. Ohne auf die Einstimmigkeit einer Entscheidung angewiesen zu sein, kann sie nun leichter eine einheitliche Anwendung des Datenschutzrechts erreichen. Um die Effektivität der DSK zu erhöhen, hat sie zum Ende des Berichtszeitraums ein Präsidium geschaffen, in dem der bisherige Vorsitzende, die nächstjährige Vorsitzende und die beiden Vertreter Deutschlands im EDSA die aktuelle Vorsitzende unterstützen. Weitere Maßnahmen zur Verbesserung und Stärkung der Zusammenarbeit in der DSK werden folgen.

2. Digitale Souveränität und Datenschutz

Die normative Eigenverpflichtung der Europäischen Union, das Grundrecht auf Privatsphäre und Schutz der personenbezogenen Daten gemäß Art. 7 und 8 Grundrechtecharta (GRCh) zu schützen, kann nur erfüllt werden, wenn die für die Digitalisierung gesellschaftlicher Beziehungen eingesetzten IT-Systeme diesen Schutz sicherstellen und ihn nicht konterkarieren. Nur wenn der für den Schutz Verantwortliche in der Lage ist, diesen Schutz bei seiner Datenverarbeitung zu gewährleisten, können diese Grundrechte umgesetzt werden.

Spätestens die politischen Ereignisse des Jahres 2022 rund um Putins Überfall auf die Ukraine haben gezeigt, wie wichtig es ist, Abhängigkeiten zu reduzieren und in bestimmten Bereichen eine hohe Unabhängigkeit zu wahren. Deutschland und Europa können auf globale Beziehungen, globale Kommunikation und globalen wirtschaftlichen Austausch nicht verzichten und wollen dies auch nicht. Dies darf aber nicht dazu führen, dass sie aufgrund von Abhängigkeiten die Verfolgung eigener Ziele und Werte aufgeben oder sich gar erpressbar machen. Dies gilt auch für die Digitalisierung. Daher ist in den Bereichen der Digitalisierung, in denen die Beschränkung von Abhängigkeiten sinnvoll und machbar erscheint, „digitale Souveränität" ein wichtiges politisches Ziel.

Digitale Souveränität als politisches Ziel

So verfolgt etwa die Datenstrategie der EU in expliziter Abgrenzung zu USA und China das Ziel, in der Digitalisierung der Wirtschaft und Verwaltung in Europa „unseren eigenen, europäischen Weg (zu) finden, indem wir den Austausch und die breite Nutzung von Daten kanalisieren und gleichzeitig hohe Datenschutz-, Sicherheits- und Ethik-Standards wahren" (EU-Kommission, Eine europäische Datenstrategie, vom 19. Februar 2021, COM(2020) 66 final, S. 4). Auch das Weißbuch der EU-Kommission zur Künstlichen Intelligenz fordert die EU auf, „geeint (zu) handeln und auf der Grundlage europäischer Werte ihren eigenen Weg zur Förderung der Entwicklung und Nutzung von KI fest(zu)legen" (EU-Kommission, Weißbuch zur Künstlichen Intelligenz – Ein europäisches Konzept für Exzellenz und Vertrauen, vom 19. Februar 2020, COM(2020) 65 final, S. 1). In Deutschland will die Bundesregierung mit ihrer Datenstrategie „einen Beitrag zur digitalen Souveränität Europas leisten" (Bundesregierung, Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum, vom 27. Januar 2021, S. 9). Auch für den Koalitionsvertrag vom 27. November 2021 ist digitale Souveränität ein

zentrales Ziel (SPD, Bündnis90/Die Grünen, FDP, Mehr Fortschritt wagen, Koalitionsvertrag, 2021, S. 15-20). In ihrem Forschungsrahmenprogramm zur IT-Sicherheit nennt die Bundesregierung 32 mal „technologische Souveränität" als Forschungsziel (BMBF, digital.sicher.souverän, Forschungsrahmenprogramm der Bundesregierung zur IT-Sicherheit, 2021; BMBF, souverän.digital.vernetzt, Forschungsprogramm Kommunikationssysteme, 2021). Strategische Bekenntnisse zur digitalen Souveränität als politischem Ziel finden sich auch in der Strategie des IT-Planungsrats (IT-Planungsrat, Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung, 2021) und in vielen Strategiepapieren der Bundesländer (s. z. B. für Hessen Hessische Ministerin für Digitale Strategie und Entwicklung, Digitales Hessen – wo Zukunft zu Hause ist, 2021, S. 9; dies., KI made in Hessen, 2022, S. 45, 50).

All diese politischen Strategien in Europa und Deutschland sehen digitale Souveränität als Ausdruck und Verpflichtung ihrer normativen Orientierung. Für sie ist digitale Souveränität aber nicht nur eine Frage der Sicherheit, der Wettbewerbsfähigkeit und der Innovationskraft, der Entwicklung der Demokratie, der politischen Selbstbestimmung und der Verantwortung für die sozialen Folgen der Digitalisierung, sondern auch eine Frage des Rechtsstaats und des Grundrechtsschutzes. Sie verweisen für die politischen Zielsetzungen der Digitalisierung – in bewusster Unterscheidung zu Strategien etwa in Nordamerika oder Asien – auf ihre Werteorientierung. Sie sehen den Schutz der Persönlichkeit, wie er etwa in den Grundrechten auf Privatheit und Datenschutz in Art. 7 und 8 GRCh zum Ausdruck kommt, als einen entscheidenden Orientierungspunkt und die DS-GVO als eine wichtige normative Grundlage für die Digitalisierung der Gesellschaft.

Um technologische Souveränität als Voraussetzung und Folge digitaler Selbstbehauptung zu erreichen, sind – wie die Stellungnahme der Hessischen Landesregierung zu meinem 50. Tätigkeitsbericht hervorhebt (LT-Drs. 20/9709, S. 2) – koordinierte Anstrengungen in vielen Politikbereichen wie der Wirtschafts- und Industrie-, Wettbewerbs-, Forschungs-, Bildungs-, Rechts- und Digitalpolitik in der EU und in Deutschland erforderlich. Sie erfordern, neben datenschutzrechtlichen Aspekten auch solche der Technik (Hard- und Software), der Digitalkompetenz, der IT-Sicherheit und der Kostenkontrolle zu berücksichtigen. In diesem Tätigkeitsbericht werde ich mich aber auf den datenschutzrechtlichen Aspekt digitaler Souveränität beschränken (s. hierzu auch Roßnagel, Digitale Souveränität im Datenschutzrecht, MultiMedia und Recht (MMR) 2023, 64 ff).

Digitale Selbstbehauptung für Grundrechte und Demokratie

Die EU gewährleistet allen Personen in ihrem Hoheitsgebiet Grundrechts- und Datenschutz. Zu dieser Gewährleistung steht sie auch dann, wenn die Daten dieser Menschen in Drittländern oder in der Union durch Techniksysteme und Dienstleister aus Drittländern verarbeitet werden. Daher müssen Datenschutzrecht und Grundrechtsschutz auch dann gelten und durchgesetzt werden, wenn die Hersteller von IT-Systemen und Diensteanbieter aus Drittländern von geringeren Anforderungen ausgehen, weil in ihrem Heimatland geringere Schutzanforderungen gelten. Will die Union ihr Schutzversprechen einhalten, muss sie darauf bestehen, dass jeder, der auf dem europäischen Markt auftritt, die hier geltenden Schutzanforderung erfüllt. Ein niedrigeres Schutzniveau in anderen Ländern darf nicht auf die Union übertragen werden. Aus diesem Grund darf auch die Auswahl von Techniken oder Dienstleistungen nicht dazu führen, dass es (faktisch) zu einem niedrigeren Schutzniveau kommt.

Zugleich ist die Durchsetzung des Grundrechts- und Datenschutzes gegenüber Herstellern und Anbietern aus Drittländern eine Maßnahme zur Selbstbehauptung europäischer Demokratie: Die Regeln des Zusammenlebens in der digitalen Welt sind demokratisch zu bestimmen. Sie dürfen nicht privater Marktmacht globaler Konzerne und den von ihnen gesetzten privaten Rechtsordnungen überlassen werden. Im Konfliktfall sind die demokratisch gesetzten Regeln durchzusetzen.

Durchsetzung von Datenschutzrecht

Meine Aufgabe, die in Art. 57 Buchst. a DS-GVO als erste genannt wird, Datenschutzrecht durchzusetzen, wird durch Techniksysteme, Dienstleistungen, Auftragnehmer und Geschäftsmodelle in Frage gestellt, die nicht den Anforderungen des Datenschutzes entsprechen. Drei Beispiele sollen zeigen, dass Verantwortliche, die solche Dienstleistungen, Techniksysteme oder Auftragnehmer in Anspruch nehmen, im Regelfall nicht in der Lage sind, ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO zu entsprechen. Sie müssten nachweisen, dass sie alle Anforderungen des Datenschutzes erfüllen, aber können dies nicht, weil sie nicht über die notwendigen Informationen verfügen oder die von ihnen in Anspruch genommenen Leistungen diese nicht erfüllen:

– Als Beispiel für Social Media soll Facebook dienen. Meta bietet im Rahmen seiner Dienstleistung „Facebook“ Verantwortlichen „Seiten“ an, die diese nutzen können, um der Öffentlichkeit Informationen bekanntzugeben. Dabei erhebt Meta personenbezogene Daten über die Nachfragenden, ohne die verantwortlichen Nutzenden zu informieren, welche Daten es für welche Zwecke erhebt und wie die Daten weiterverarbeitet werden,

ohne nachzuweisen, dass dieses Tracking und Profiling zulässig ist, und ohne mit den Nutzenden eine Vereinbarung zur gemeinsamen Verantwortung abzuschließen. Auch übertragen sie personenbezogene Daten ohne ausreichende zusätzliche Schutzmaßnahmen in die USA (s. näher Kap. 12.2). Andere Social Media-Angebote aus USA und China bieten vergleichbare grundsätzliche Probleme.

– Microsoft bietet seine Office-Programme künftig als MS 365 nur noch als cloudbasierte Dienstleistungen in einem Auftragsverhältnis an. Entsprechend seinem „Datenschutznachtrag“ vom 15. September 2022 für MS 365 will Microsoft diese Dienstleistungen erbringen, ohne dem Verantwortlichen zu ermöglichen, ihm als Auftragnehmer genauere Weisungen zu erteilen, ohne darüber zu informieren, welche Daten es in welcher Weise für eigene Zwecke verarbeitet, ohne über Änderungen bei Subauftragnehmern hinreichend präzise zu informieren und ohne Daten nach den Vorgaben der DS-GVO zu löschen oder zurückzugeben (s. auch Bundesregierung, BT-Drs. 20/4852, S. 44). Microsoft will außerdem auf Anforderung US-amerikanischen Behörden Daten herausgeben dürfen und Daten ohne ausreichende Schutzmaßnahmen in den USA verarbeiten. Andere cloudbasierte Dienstleistungen aus Drittländern verursachen vergleichbare Probleme.
– Als Beispiel für Probleme mit US-amerikanischen Anbietern von Videokonferenzsystemen (VKS) soll Webex von Cisco dienen. Cisco bietet Webex nicht im On-Premise-Betrieb an, sondern betreibt das VKS selbst. Dies verhindert, dass Verantwortliche selbst kontrollieren können, ob und wohin personenbezogene Daten abfließen. Im Betrieb des VKS verarbeitet Cisco personenbezogene Daten in den USA ohne ausreichende zusätzliche Schutzmaßnahmen. Zwar werden die Inhaltsdaten bei Videokonferenzen verschlüsselt, doch werden die Schlüssel nicht vom Verantwortlichen erzeugt, sondern von Cisco verteilt, so dass der Zugriff von US-amerikanischen Behörden auf die Schlüssel nicht ausgeschlossen ist (s. 50. Tätigkeitsbericht, Kap. 4.1). Ähnliche Probleme bieten auch andere VKS aus Drittländern.

Alle diese Anbieter haben ihre Hauptniederlassung in Irland. Für sie bin ich nicht zuständig. Aber ich muss in Hessen Datenschutz durchsetzen, auch wenn Verantwortliche in Hessen deren Angebote nutzen. Soweit Verantwortliche von solchen Techniksystemen oder Dienstleistungen abhängig sind, stehe ich vielfach vor dem Dilemma, entweder sie durch Anordnungen in ihrer Geschäftstätigkeit oder ihrer Aufgabenerfüllung zu behindern oder auf die Durchsetzung von Datenschutzanforderungen zu verzichten (s. 50. Tätigkeitsbericht, Kap. 3.1). Dieses Dilemma lässt sich nur vermeiden, wenn die Abhängigkeit von den Produkten solcher Anbieter überwunden wird.

Die Anbieter von Social-Media-, Cloud-, Videokonferenz- und anderen Techniksystemen aus Drittländern sind oft nicht bereit, ihre Systeme den datenschutzrechtlichen Anforderungen anzupassen. Aus praktischer Sicht sind daher jeweils technisch-organisatorische Alternativen zu den aus dem Drittland angebotenen Hardware, Software, Diensten und Plattformen erforderlich, um eine datenschutzgerechte Datenverarbeitung zu ermöglichen. Digitale Souveränität ist deshalb in vielen Fällen eine Voraussetzung zur Durchsetzung von datenschutzrechtlichen Anforderungen.

Die notwendigen Voraussetzungen für die erforderliche Vielfalt technischer und organisatorischer Alternativen in möglichst vielen Bereichen der Verarbeitung personenbezogener Daten zu fördern, ist vorrangig eine politische Aufgabe. Sie zu erfüllen, erfordert Maßnahmen in vielen Politikbereichen. Aber auch der Verantwortliche muss dazu beitragen, indem er seine IT-Systeme, die von ihm genutzten Dienstleistungen und seine Auftragnehmer so auswählt, dass er seine datenschutzrechtlichen Pflichten erfüllen kann.

Verantwortung der Verantwortlichen

Die Verantwortung des Verantwortlichen für die Voraussetzungen, um datenschutzrechtliche Anforderungen erfüllen zu können, hat der EuGH in seinem Urteil vom 16. Juli 2020 (C-311/18 – Schrems II) deutlich gemacht und am Beispiel des Transfers personenbezogener Daten in ein unsicheres Drittland (in diesem Fall die USA) herausgestellt (s. 50. Tätigkeitsbericht, Kap. 3.1). Die Ausführungen des Gerichts machen deutlich, dass die Auswahl der Techniksysteme und Dienstleistungen durch den Verantwortlichen unter seine Verantwortung fällt. Dies hat der EDSA in seinen „Empfehlungen zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten“ (Empfehlung 1/2020, Version 2 vom 18. Juni 2021) überzeugend herausgearbeitet. Der Verantwortliche muss prüfen, bevor er personenbezogene Daten in ein Drittland überträgt, ob dort die Daten einen vergleichbaren Schutz genießen wie in der EU. Wenn dies nicht der Fall ist, muss er zusätzliche Schutzmaßnahmen ergreifen oder die Datenübermittlung unterbinden.

Rechtsstaatliche Definition digitaler Souveränität

Die vom EuGH für den internationalen Datenverkehr ausformulierte Verantwortung für den Schutz des Grundrechts auf Datenschutz kann jedoch nicht nur für die im Schrems II-Urteil zu entscheidenden Vorlagefragen gelten, sondern ist über die Pflichten im internationalen Datentransfer hinaus auf alle datenschutzrechtlichen Pflichten zu erweitern. Der Verantwortliche hat grundsätzlich die Pflicht, durch die Auswahl der von ihm verwendeten Technik

und der in Anspruch genommenen Dienste seine datenschutzrechtlichen Handlungserfordernisse zu sichern. Er darf sich nicht selbst in Sachzwänge oder Abhängigkeiten bringen, die es ihm unmöglich machen, seiner Verantwortung gerecht zu werden. Umgekehrt kann er nicht geltend machen, dass bestimmte datenschutzrechtliche Pflichten für ihn deshalb nicht gelten, weil er wegen der von ihm verwendeten Techniken und der in Anspruch genommenen Dienste nicht in der Lage ist, sie zu erfüllen. Digitale Souveränität in einem rechtsstaatlichen Sinn besteht mit Blick auf das Datenschutzrecht, wenn der Verantwortliche Techniksysteme oder Dienstleistungen nutzt, die ihn in die Lage versetzen, datenschutzrechtliche Anforderungen zu erfüllen. Diese Definition zielt nicht auf protektionistische Bevorzugung europäischer Techniksysteme und Dienstleistungen, sondern allein auf die Durchsetzung des Rechts der Union und des Mitgliedstaats.

Digitale Souveränität ist kein Rechtsbegriff, sie steht nicht als solche in der DS-GVO. Sie ist aber ein Begriff, der für vielfältige datenschutzrechtliche Probleme, denen ein gleiches Strukturproblem zugrunde liegt, einen Lösungsweg bezeichnet. Dieses strukturelle Problem besteht darin, dass Anbieter aus Drittländern Techniksysteme oder Dienstleistungen anbieten und Geschäftsmodelle verfolgen, die mit den rechtlichen Vorgaben in der EU und Deutschland nicht vereinbar sind. Sie wollen entgegen gesetzlicher Regelungen daran festhalten und setzen dies aufgrund ihrer Marktmacht auch oft durch. Im Datenschutzrecht sind die Verantwortlichen aber auch dann zur Einhaltung der datenschutzrechtlichen Vorgaben verpflichtet, wenn sie diese Techniksysteme und Dienstleistungen nutzen. Sie müssen Techniksysteme und Dienste wählen, mit denen sie in der Lage sind, die sie betreffenden Anforderungen zu erfüllen. Dies gilt nicht nur für die Frage des internationalen Datentransfers in Drittländer, sondern etwa auch für

– die von Art. 25 Abs. 1 DS-GVO geforderte datenschutzgerechte Systemgestaltung, die die Voraussetzungen für eine Datenverarbeitung gewährleisten soll, die die Datenschutzprinzipien nach Art. 5 DS-GVO einhält. Diese Verpflichtung beinhaltet auch, die eingesetzten Hard- und Software-Systeme, Plattformen und Dienstleistungen so auszuwählen, dass eine datenschutzgerechte Datenverarbeitung möglich ist. Die Relativierung dieser Pflicht durch Berücksichtigung des Stands der Technik und der Implementierungskosten in Art. 25 Abs. 1 DS-GVO bedeutet, dass der Verantwortliche zwischen geeigneten technischen Alternativen, die dem Stand der Technik entsprechen, auswählen kann, nicht aber, dass er datenschutzrechtliche Anforderungen nicht erfüllen muss, wenn er keine technische Alternative für seinen Verarbeitungszweck findet, die datenschutzgerecht einsetzbar ist.

– die von Art. 25 Abs. 2 DS-GVO geforderten datenschutzfreundlichen Voreinstellungen. Er muss für seine Zwecke IT-Systeme, Dienste und Plattformen auswählen, die ihm z. B. ermöglichen, jedes Tracking auszuschalten und alle Vorgaben des § 25 TTDSG einzuhalten (s. zu diesen DSK, Orientierungshilfe Telemedien, Dezember 2021).
– die von Art. 26 DS-GVO geforderte Wahrnehmung gemeinsamer Verantwortung. Der Verantwortliche darf IT-Kooperationen mit gemeinsamer Verantwortung nur eingehen, wenn die Partner mit ihm Vereinbarungen nach Art. 26 Abs. 1 S. 2 DS-GVO treffen, in denen sie festlegen, wie eine datenschutzgerechte Datenverarbeitung erfolgt, wer welche Verpflichtungen insbesondere gegenüber betroffenen Personen erfüllt und wer welchen Informationspflichten nachkommt. Dies setzt weiter voraus, dass der Partner dem Verantwortlichen die hierfür notwendigen Informationen erteilt.
– den von Art. 28 DS-GVO geforderten Einbezug von Auftragsverarbeitern, die sicherstellen, dass sie alle Vorgaben des Datenschutzrechts erfüllen (können). Mit Blick auf die Verpflichtungen von Unternehmen aus dem Drittland, ihren Behörden Daten auch aus dem EWR zugänglich zu machen, dürfen Verantwortliche Auftragnehmern personenbezogene Daten nur dann anvertrauen, wenn diese nicht ausländischen staatlichen Stellen verpflichtet sind, die von ihnen die Herausgabe dieser Daten entgegen Art. 48 DS-GVO verlangen können, oder zusätzliche Schutzmaßnahmen eine Offenlegung personenbezogener Daten verhindern. Sie dürfen Auftragnehmern auch nur dann Daten übergeben, wenn diese sicherstellen, dass sie die Daten nicht für eigene Zwecke verwenden.
– die von Art. 32 DS-GVO geforderte ausreichende Datensicherheit. Diese kann gefährdet sein, wenn Unternehmen aus einem Drittland von den heimischen Behörden verpflichtet werden können, mit ihnen zusammenzuarbeiten und zu diesem Zweck in ihre Software oder Hardware Schwachstellen einzubauen, die es diesen Behörden ermöglichen, in IT-Systeme von Verantwortlichen aus dem EWR einzudringen.

Ob der Hersteller, Diensteanbieter, Plattformbetreiber oder Auftragsverarbeiter aus einem Drittland diese Anforderungen erfüllt, muss der Verantwortliche vor einem Vertragsschluss überprüfen. Kann oder will er sie nicht erfüllen, darf der Verantwortliche ihm keine personenbezogenen Daten anvertrauen.

Neue transatlantische Entwicklungen

Die Diskussion um digitale Souveränität wird durch die Bemühungen eines neuen „Trans-Atlantic Data Privacy Framework“ zwischen den USA und der EU belebt. Am 7. Oktober 2022 hat der US-Präsident eine „Executive Order

on Enhancing Safeguards for United States Signals Intelligence Activities“ (EO) erlassen, die es der Kommission ermöglichen soll, den Stellen in USA, die sich dem Framework unterwerfen, ein angemessenes Datenschutzniveau anzuerkennen. Durch diese neue Rechtskonstruktion könnte das Problem der Datenübermittlung in die USA auf eine neue Grundlage gestellt werden. Für die anderen zuvor dargestellten Aspekte der digitalen Souveränität würde sich durch das Framework und seine Anerkennung jedoch nichts ändern.

Die EO versucht, die beiden zentralen Kritikpunkte des EuGH in seinem Urteil zur Aufhebung des Vorgänger-Beschlusses zu „Privacy Shield“ (vom 16. Juli 2020, C-311/18 – Schrems II) zu adressieren: die unverhältnismäßigen Datenverarbeitungsbefugnisse der Nachrichtendienste und der fehlende Rechtsschutz für Europäerinnen und Europäer.

Für die Überwachungsmaßnahmen der USA haben nach der EO die Sicherheits- und Aufklärungsinteressen der USA weiterhin höchste Priorität. Die Maßnahmen der „signal intelligence“ sollen jedoch auf das Überwachungsziel zugeschnitten sein und „not disproportionately impact privacy and civil liberties“. Massenüberwachung des Internetverkehrs (wie nach den Programmen PRISM und Upstream) soll aber weiterhin möglich sein. Die Verwendung der so erhobenen Daten soll aber beschränkt werden, soweit das Überwachungsziel durch zugeschnittene Überwachungsmaßnahmen erreicht werden kann (Sec. 2 c). Die EO stellt allerdings ausdrücklich fest, dass sie in keiner Weise „any signals intelligence collection technique“ beschränkt, die durch bisherige Vorschriften erlaubt sind (Sec. 2 e). Die Befugnisse nach Section 702 des Foreign Intelligence Surveillance Act (FISA), die der EuGH als nicht mit den europäischen Grundrechten vereinbar erklärt hat, gelten somit weiter.

Hinsichtlich des Rechtsschutzes sieht die EO außerdem einen zweistufigen Beschwerdemechanismus vor, wenn eine Nicht-US-Person der Meinung ist, dass die Überwachungsmaßnahmen der US-Nachrichtendienste gegen geltendes US-Recht verstoßen. In der ersten Stufe kann eine von den USA anerkannte Organisation (z. B. eine europäische Datenschutzaufsichtsbehörde) für ein Individuum eine Überprüfung durch einen „Civil Liberties Protection Officer“ (CLPO) im „Office of the Director of National Intelligence“ anstoßen. In der zweiten Stufe kann ein „Data Protection Review Court“ beim Attorney General den Fall überprüfen. Als Ergebnis der jeweiligen Entscheidung in der ersten und in der zweiten Stufe darf dem Beschwerdeführer weder bestätigt noch verneint werden, dass er überwacht worden ist. Vielmehr darf ihm – unabhängig vom Ergebnis der Untersuchung – immer nur mitgeteilt werden, dass die Untersuchung entweder keine Grundrechtsverletzung identifizieren konnte oder zu einer angemessenen Abhilfe geführt hat (Sec. 3 c, d).

Auf der Grundlage der EO und weiterer US-Regelungen zur Framework hat die Kommission am 13. Dezember 2022 einen Entwurf eines Anerkennungsbeschlusses vorgelegt. In dem sich anschließenden Verfahren nach Art. 45 Abs. 3 DS-GVO hat die Kommission gemäß Art. 70 Abs. 1 Buchst. s DS-GVO dem EDSA alle erforderlichen Unterlagen einschließlich des Schriftwechsels mit der Regierung der USA vorzulegen und der EDSA hat in einer Stellungnahme die Angemessenheit des in den USA gebotenen Schutzniveaus zu beurteilen. Danach sind die Mitgliedstaaten im Rahmen des Komitologieverfahrens nach Art. 45 Abs. 3 und 93 Abs. 2 DS-GVO sowie Art. 5 VO (EU) 182/2011 zu beteiligen. Die Kommission erlässt den Angemessenheitsbeschluss als Durchführungsrechtsakt gemäß Art. 291 AEUV nach Art. 5 Abs. 3 der VO (EU) 182/2011 nicht, wenn die gewichtete Mehrheit im Ausschuss zum Entwurf eine ablehnende Stellungnahme abgibt. Sie muss in diesem Fall nachverhandeln und das neue Ergebnis erneut dem Ausschuss vorlegen oder von der weiteren Verfolgung des Entwurfs absehen. Nach diesem „Fahrplan" ist mit einer verbindlichen Entscheidung über die Angemessenheit des Datenschutzniveaus in dem spezifischen Bereich der USA, in dem die Vereinbarung gelten soll, wohl erst Mitte 2023 zu rechnen. In Kraft treten lassen will die Kommission den Beschluss aber erst, wenn die USA alle relevanten Bestimmungen in der vorgesehenen Weise umgesetzt haben. Dies dürfte frühestens im Herbst 2023 der Fall sein.

Ist der Angemessenheitsbeschluss der Kommission in Kraft getreten, hat dieser nach Art. 288 Abs. 4 AEUV für die Aufsichtsbehörden Bindungswirkung, soweit darin festgestellt wird, dass die USA ein angemessenes Schutzniveau gewährleisten und die Übermittlung personenbezogener Daten im Ergebnis genehmigt wird (EuGH vom 16. Juli 2020, C-311/18).

Der EuGH wird über diesen Beschluss entscheiden müssen. Er wird ihn am Maßstab der Art. 7, 8 und 47 GRCh sowie Art. 44 Satz 2 und Art. 45 Abs. 2 DS-GVO sowie seiner Schrems II-Entscheidung überprüfen. Entscheidend wird sein, ob die USA „wirksame und durchsetzbare Rechte" sowie „wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe für betroffene Personen" aus Europa bieten, eine wirksame unabhängige Aufsichtsbehörde auch in Bezug auf die US-Sicherheitsbehörden etablieren, die auch gegenüber den US-Nachrichtendiensten verbindliche Anordnungen treffen kann (EDSA, Statement 1/2022 v. 6.4.2022), und die Überwachungspraxis („Anwendung der Rechtsvorschriften") auf verhältnismäßige Maßnahmen beschränken. Hierzu wird der EuGH u. a. folgende Fragen entscheiden müssen:

Ist eine Executive Order des Präsidenten eine ausreichende Rechtsgrundlage? Hat sie mehr als behördeninterne Wirkung? Bietet sie ausreichende Rechtssicherheit, wenn sie jederzeit – z. B. durch einen republikanischen

Präsidenten – verändert oder widerrufen werden kann? Genügt es, von den Nachrichtendiensten zu fordern, ihre Überwachung „proportionately“ zu praktizieren, wenn die gesetzlichen Grundlagen für die Massenüberwachung ausdrücklich beibehalten werden? Gilt die Verhältnismäßigkeit auch für die automatisierte massenhafte Datenerhebung oder nur für die nachfolgende Nutzung der Daten? Ist „proportionality“ im Sinn des „absolut Notwendigen“ gemeint, wie dies der EuGH in vielen Entscheidungen fordert (s. Kap. 1)? Oder meint die EO „proportionality“ in einem nach US-Verständnis den Überwachungszielen angepassten Sinn? Ist der „Data Protection Review Court“ tatsächlich ein unabhängiges Gericht oder faktisch nur ein Ausschuss innerhalb der US-Regierungsbehörden? Ist seine Überprüfung der Entscheidungen des „Civil Liberties Protection Officer“ ein echtes Gerichtsverfahren im Sinn des Art. 47 GRCh? Inwieweit wird dies durch die Beschränkung auf eine Beschwerde und die Versagung einer Klagemöglichkeit, die fehlende Öffentlichkeit und den vorgestanzten Entscheidungstenor eingeschränkt?

Nach der Beantwortung dieser und weiterer Fragen ist nicht auszuschließen, dass der EuGH die Adäquanzentscheidung der Kommission – nach Safe Harbor und Privacy Shield – ein drittes Mal aufheben wird. Jedenfalls herrscht bis zur Entscheidung des EuGH eine sehr große Rechtsunsicherheit. Diese vermeidet, wer seine Investitionen und sonstigen Entscheidungen zu Digitalprojekten langfristig an der bisherigen Rechtsprechung des EuGH und der Zielsetzung digitaler Souveränität orientiert – zumal eine Entscheidung des EuGH, die den Angemessenheitsbeschluss bestätigen würde, nur einen von vielen Gründen für digitale Souveränität, nämlich den internationalen Transfer personenbezogener Daten, betreffen und nur für die USA gelten würde. Selbst wenn nur der internationale Datentransfer beachtet wird, ist zu berücksichtigen, dass sich Fragen der digitalen Souveränität in den letzten Jahren sehr auf die USA konzentriert haben. Ähnliche Fragen stellen sich aber auch in vielen anderen Drittstaaten, in die Daten transferiert werden.

Umsetzung digitaler Souveränität in Hessen

Daher ist es sinnvoll, sich auch langfristig an dem Ziel digitaler Souveränität zu orientieren. Aus diesem Grund haben die EU-Kommission, die Bundesregierung und die Landesregierungen dieses Ziel in ihre eingangs genannten Digitalisierungsstrategien für die öffentliche Verwaltung aufgenommen. In Umsetzung dieser Strategien wurden etwa auf Bundesebene inzwischen viele Projekte auf den Weg gebracht – wie die Souveräne Verwaltungs-Cloud, der Souveräne Arbeitsplatz, der Sovereign Tech Fund und das Zentrum für Digitale Souveränität (ZenDiS) der Öffentlichen Verwaltung. Dadurch hat der Bund „frühzeitig Entscheidungen getroffen und Maßnahmen umgesetzt,

die einen Einsatz dieser Produkte (= MS 365) für den Bund grundsätzlich entbehrlich machen“. Schon heute verzichtet die Bundesregierung beinahe vollständig auf den Einsatz von MS 365 (BT-Drs. 20/4852, S. 44f.)

Hessen ist an den Projekten zur Souveränen Verwaltungs-Cloud und zum Souveränen Arbeitsplatz beteiligt. Wechselmöglichkeiten zwischen IT-Lösungen im Kontext digitaler Souveränität werden u. a. im Projekt HessenSW 2025 erarbeitet. Ein gelungenes Beispiel der Umsetzung digitaler Souveränität ist auch das Schulportal Hessen (s. Kap. 8.2). Besondere Fortschritte konnten in Hessen unter Mitwirkung meiner Behörde im Bereich Videokonferenzen erzielt werden. Durch Technikauswahl und Technikgestaltung konnten datenschutzgerechte Systemlösungen entwickelt und zum Einsatz gebracht werden:

– In der hessischen Landesverwaltung wird für ca. 70.000 Beschäftigte seit dem Ende des Berichtszeitraums vom Hessischen Ministerium für Digitale Strategie und Entwicklung als „Hessen Connect 2.0“ eine Systemlösung Schritt für Schritt ausgerollt. Sie wird von T-Systems betrieben und integriert als Chat-System die Open Source-Lösung „Matrix/Elements“ und als VKS die Open Source-Lösung „Jitsi“ (s. Kap. 3.4).
– Hessische Schulen können seit dem Herbst 2022 als VKS die Open Source-Lösung BigBlueButton einsetzen. Das System wird durch das hessische Unternehmen German Edge Cloud betrieben. Das Hessische Kultusministerium bietet es aus Sicherheitsgründen integriert im Schulportal für alle 2.000 staatlichen und privaten Schulen in Hessen kostenlos an. Die Schulträger und Schulen können nun rechtsicher ein VKS für Schulzwecke einsetzen (s. Kap. 3.2).
– Für die hessischen Hochschulen konnte unter Moderation des Hessischen Ministeriums für Wissenschaft und Kunst geklärt werden, welche VKS durch entsprechende Technikgestaltung rechtsgemäß genutzt werden können. Eingesetzt werden künftig vor allem das deutsche Open Source-System BigBlueButton, aber auch eine sichere Technikgestaltung des US-amerikanischen VKS Zoom. Dieses VKS wird nach dem „Hessischen Modell“ unter Einschaltung eines hessischen Dienstleisters (im konkreten Fall Connect4Video) im Eigenbetrieb genutzt. Dieser ist auch in die Abrechnung zwischengeschaltet und kontrolliert externe Zugriffe auf Systeme. Die Hochschule verhindert durch ein Identitätsmanagementsystem, Pseudonymisierung, VPN und Verschlüsselung der Inhaltsdaten, dass personenbezogene Daten an Zoom gelangen (s. Kap. 3.3).
– Die Berücksichtigung des Datenschutzes und der digitalen Souveränität kommt auch im Baustein „Datenschutz“ im IT-Designprinzip BaSiS (Barrierefreie IT, Informationssicherheit und Datenschutz) zum Ausdruck, das die Ministerin für Digitale Strategie und Entwicklung gemeinsam mit der

Landesbeauftragten für barrierefreie IT, dem Hessischen Ministerium des Inneren und für den Sport und mir erarbeitet hat. Dieses Designprinzip soll künftig als landesweiter IT-Standard für die Projektumsetzung in allen Phasen der Digitalisierungsprojekte des Landes Hessen – auch bereits bei der Konzeption, der Ausschreibung und der Auswahl – verbindlich angewendet werden.

Diese Beispiele zeigen, dass es schon jetzt Bereiche der Digitalisierung gibt, in denen durch digitale Souveränität das grundsätzliche Problem des Vollzugs des Datenschutzes durch Techniksysteme und Dienstleistungen, die sich nicht an den rechtlichen Vorgaben der GRCh und der DS-GVO orientieren, gelöst oder zumindest gemindert werden kann.

3. Videokonferenzsysteme

Der Digitalisierungsschub durch die Corona-Pandemie hat vor allem zu einer verstärkten Nutzung von Videokonferenzsystemen (VKS) geführt. Dabei wurden durch den Zwang zu schnellen Lösungen viele Systeme ausgewählt, die den datenschutzrechtlichen Anforderungen nicht genügen. Dies gilt insbesondere für viele weit verbreitete VKS, die von US-amerikanischen Anbietern stammen. Diese übertragen personenbezogene Daten in die USA und bewirken dadurch für die betroffenen Personen einen Verlust in der Wahrnehmung ihrer Grundrechte (s. 50. Tätigkeitsbericht, Kap. 3.1). Sie verstoßen aber auch oft gegen andere Datenschutzvorgaben, weil sie ein mit der DS-GVO unvereinbares Geschäftsmodell verfolgen (s. 50. Tätigkeitsbericht, Kap. 4.1). VKS sind daher ein Technikbereich, in dem digitale Souveränität die Umsetzung von Datenschutzrecht unterstützt und erleichtert (s. Kap. 2). In diesem Bereich ist digitale Souveränität aber auch schon möglich. In diesem Kapitel werden drei erfolgreiche Digitalisierungsprojekte aus dem Berichtszeitraum vorgestellt, die ermöglichen, von der rechtswidrigen Nutzung von VKS auf rechtmäßig nutzbare Systeme zu wechseln. Sie sind ein Beispiel dafür, wie technologische Abhängigkeit vermieden, gesellschaftlicher Bedarf an Technologienutzung befriedigt und Problemlösungen durch datenschutzkonforme Systemgestaltung erreicht werden können. Sie zeigen, dass es richtig war, in den letzten zwei Jahren auf systemische Beratung und Gestaltung von Digitalisierungsprojekten statt auf Intervention im Einzelfall zu setzen und den Verantwortlichen die für diese Transformation notwendige Zeit einzuräumen. Bevor diese Projekte vorgestellt werden, ist jedoch zu klären, welche datenschutzrechtlichen Anforderungen für VKS gelten.

3.1
Datenschutzrechtliche Einordnung von Videokonferenzsystemen

Hinsichtlich der datenschutzrechtlichen Einordnung von VKS besteht große Unsicherheit. Dies beruht zum einen darauf, dass Videokonferenzen erst in der Corona-Pandemie einen rasanten Aufstieg genommen haben und daher erst seit kurzer Zeit breit genutzt werden. Zum anderen haben sich erst vor kurzem die Rechtsgrundlagen geändert: Seit dem 1. Dezember 2021 gelten neue Regeln im Telekommunikationsgesetz (TKG) und das neue Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG). Um die Unsicherheit, wie das Angebot und die Nutzung von Videokonferenzen datenschutzrechtlich einzuordnen sind, habe ich für die Datenschutzkonferenz diese Frage untersucht (s. näher Roßnagel, Videokonferenzen als Telekommunikationsdienste?, Neue Juristische Wochenschrift (NJW) 2023, Heft 7, 400 ff.).

Telekommunikation?

Videokonferenzdienste sind dann Telekommunikationsdienste, wenn sie die Definition für diesen Begriff erfüllen. Dann müssten sie nach § 3 Nr. 61 TKG „in der Regel gegen Entgelt über Telekommunikationsnetze erbrachte Dienste“ sein, die einer der drei in der Vorschrift genannten Dienstkategorien entsprechen. In Frage kommt nur die Einordnung als „interpersoneller Telekommunikationsdienst“. Ein solcher ist nach § 3 Nr. 24 TKG „ein gewöhnlich gegen Entgelt“ erbrachter Dienst, der einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze zwischen einer endlichen Zahl von Personen ermöglicht. Außerdem müssen die Empfänger von den Veranstaltern der Videokonferenz bestimmt sein.

Videokonferenzen bieten im Regelfall einen direkten interpersonellen und interaktiven visuellen und auditiven Informationsaustausch zwischen den Teilnehmern. Die Signale der Videokonferenzen werden über Telekommunikationsnetze übertragen. Um an einer Videokonferenz teilnehmen zu können, muss man dazu eingeladen sein. An einer Videokonferenz nimmt daher nur eine endliche Zahl von Personen teil.

Als interpersoneller Kommunikationsdienst muss der Dienst den direkten interpersonellen und interaktiven Informationsaustausch „ermöglichen“. Nicht die einzelne Videokonferenz ist ein interpersoneller Kommunikationsdienst, sondern der Dienst, der dem Veranstalter einer Videokonferenz ermöglicht, durch Ton- und Bildübertragung eine solche Konferenz durchzuführen. Zu diesem Videokonferenzdienst gehören als Leistungsmerkmale auch die Möglichkeiten, den Konferenzraum zu buchen, zur Konferenz einzuladen, die Konferenz zu steuern, Teilnehmer nachträglich dazuzunehmen, Teilnehmer auszusperren, Untergruppen zu bilden, einen Chatkanal zu betreiben, Mikrofone und Kameras zentral zu bedienen, die Konferenz aufzuzeichnen, Rechte einzuräumen (etwa Dokumente hochzuladen) und ähnliche Funktionen wahrzunehmen. Solche Videokonferenzdienste sind z. B. Zoom, Cisco Webex, Microsoft Teams, Google Meet, GoToMeeting, Skype, BigBlueButton, Jitsi, alfaview und viele weitere.

Ob sie als Dienste interpersoneller Telekommunikation anzusehen sind, hängt nach § 3 Nr. 24 und 61 TKG noch davon ab, ob sie „gewöhnlich“ oder „in der Regel gegen Entgelt“ erbracht werden. Die Definition setzt also ein gegenseitiges Leistungsverhältnis zwischen „Marktbeteiligten“ voraus. Der Videokonferenzdienst muss eine selbstständige Leistung sein, die darin besteht, dass der Anbieter dem Nachfrager die Möglichkeit eröffnet, Videokonferenzen mit von ihm bestimmten Teilnehmern durchzuführen. Dieses Leistungsverhältnis betrifft somit den Betreiber eines Videokonferenzdienstes als Anbieter und den Veranstalter von Videokonferenzen als Nachfrager.

Demgegenüber liegt jedoch kein interpersoneller Telekommunikationsdienst vor, wenn der Nachfrager den Dienst nutzt, um eine Videokonferenz durchzuführen. Soweit der Veranstalter Teilnehmer in die Videokonferenz einlädt, um aus eigenem Interesse mit ihnen zu kommunizieren, bietet er ihnen keine Möglichkeit an, selbst Konferenzen mit allen Nebenfunktionen zu veranstalten. Die Teilnehmer erbringen in diesem Fall auch kein Entgelt. Wenn aber kein Videokonferenzdienst auf einem Markt für solche Dienste angeboten wird und bezogen auf einen solchen Dienst kein gegenseitiges Leistungsverhältnis besteht, fehlt es an den begrifflichen Voraussetzungen des Angebots eines interpersonellen Telekommunikationsdienstes nach § 3 Nr. 24 TKG und eines Telekommunikationsdienstes nach § 3 Nr. 61 TKG. Wer Videokonferenzdienste nutzt, um Videokonferenzen zu veranstalten, ist kein Anbieter von Videokonferenzdiensten und daher auch kein Adressat des TKG. Ein solcher Nutzer ist vielmehr mit einer Person vergleichbar, die einen Telefonanschluss nutzt, um mit anderen Personen zu telefonieren. Diese Person wird auch nicht als Anbieter eines Telekommunikationsdienstes angesehen.

Die Konsequenzen dieser Differenzierung können an folgenden praktischen Beispielen verdeutlicht werden. Anbieter von Videokonferenzdiensten wie Zoom, Cisco, Microsoft, Google, Telekom u. a. bieten auf einem weltweiten Markt gegen Entgelt die Möglichkeit an, mit Hilfe ihrer Dienste Videokonferenzen durchzuführen. Diese Möglichkeit wird z. B. von Verwaltungsbehörden, Hochschulen, Schulen, Arztpraxen, Rechtsanwaltsbüros, Vereinen und Unternehmen nachgefragt und sie zahlen dafür ein Entgelt. Diese Anbieter erbringen somit interpersonelle Telekommunikationsdienste und unterfallen dem TKG.

Wenn dagegen die Hochschulen ihren bezahlten Videokonferenzdienst nutzen, um mit ihren Mitgliedern zu kommunizieren und damit ihren Aufgaben zu Lehre und Forschung nachzukommen, dann bieten sie ihnen keinen Dienst auf einem Markt an, für den die Teilnehmer ein Entgelt entrichten. Ebenso wenig entsteht ein Markt für Videokonferenzdienste, wenn Schulen ihren Lehrenden sowie Schülerinnen und Schülern die Teilnahme an virtuellen Unterrichtsstunden ermöglichen. Vergleichbar verlangen Verwaltungsbehörden keine Entgelte, wenn sie interne Besprechungen zwischen Verwaltungsbediensteten oder Sprechstunden mit Bürgerinnen und Bürgern per Videokonferenz durchführen. Auch Anwaltsbüros und Arztpraxen können ihre erworbenen Lizenzen für Videokonferenzen dafür nutzen, um mit Mandanten oder Patienten zu kommunizieren und auch aus der Ferne ihre Beratungsleistungen zu erbringen. Sie verlangen für die Teilnahme an der Videokonferenz kein Entgelt. Ebenso fordern Vereine, die ihre Vorstandssitzung in Form einer Videokonferenz durchführen, von den Vorstandsmitgliedern kein Entgelt für die Teilnahme. Schließlich verlangen Unternehmen von ihren Beschäftigten

kein Entgelt, wenn sie für interne Besprechungen Videokonferenzen nutzen. Das Gleiche gilt, wenn sie über Videokonferenzen mit ihren Partnern, Kunden oder Zulieferern Kontakt halten. In all diesen Fällen eröffnen die Veranstalter von Videokonferenzen keinen Markt, auf dem sie die Möglichkeit, Videokonferenzen durchzuführen, gegen Entgelt anbieten und erbringen, sondern nutzen diese. Sie sind daher keine Anbieter von Telekommunikationsdiensten.

Es ist daher festzuhalten, dass die Anbieter von Videokonferenzdiensten gegen Entgelt einen Telekommunikationsdienst erbringen und daher unter das Telekommunikationsrecht, also das TKG und die §§ 1 bis 18 und 27 bis 30 TTDSG fallen. Dagegen sind auf diejenigen, die Videokonferenzdienste nur nutzen, die DS-GVO und ergänzend die einschlägigen Regelungen zu Telemedien in §§ 1 und 2, 19 bis 26 und 28 TTDSG anzuwenden.

Fernmeldegeheimnis oder informationelle Selbstbestimmung?

Dieses Ergebnis passt auch zu den Regelungen des Fernmeldegeheimnisses im TTDSG. Nach § 3 Abs. 2 TTDSG sind „Anbieter von öffentlich zugänglichen Telekommunikationsdiensten“ sowie „Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten“ zur Wahrung des Fernmeldegeheimnisses verpflichtet. Danach gilt das Fernmeldegeheimnis für die Anbieter von Videokonferenzdiensten wie Zoom, Cisco, Microsoft u. a. Sie bieten auf dem Markt öffentlich Telekommunikationsdienste für jeden an und sie erbringen sie dauerhaft gegenüber Dritten, also geschäftsmäßig.

Dagegen sind Vereine, Hochschulen, Schulen, Verwaltungsbehörden, Arztpraxen und Anwaltsbüros sowie Unternehmen, die ihre Möglichkeit zur Durchführung von Videokonferenzen für eigene Zwecke zur Kommunikation mit Mitgliedern, Beschäftigten und Vertragspartnern nutzen, nicht zur Wahrung des Fernmeldegeheimnisses verpflichtet, weil sie keine Telekommunikationsdienste gegen Entgelt erbringen. Sie müssen jedoch das Grundrecht auf informationelle Selbstbestimmung aller betroffenen Personen schützen. Mit diesem Grundrecht sind in der Praxis weitgehend das gleiche Schutzniveau und die gleichen Anforderungen verbunden wie mit dem Fernmeldegeheimnis.

Datenschutzaufsicht

Der Begriff der Telekommunikation entscheidet auch über die zuständige Aufsichtsbehörde. Nach § 29 Abs. 1 TTDSG ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die zuständige Aufsichtsbehörde, soweit es sich um Telekommunikationsdienste handelt, also für Anbieter von Videokonferenzdiensten am Telekommunikationsmarkt wie z. B. Zoom, Cisco, Microsoft u. a. Nicht er, sondern die Datenschutzbeauftragten der Länder

sind jedoch für die Nutzung von diesen Videokonferenzdiensten zuständig, wenn sie zu eigenen Zwecken in der Regel oder gewöhnlich ohne Entgelt zur Kommunikation mit den Mitgliedern, Angehörigen, Beschäftigten, Kunden, Bewerben oder Lieferanten verwendet werden.

Anwendung der DS-GVO

Soweit Anbieter von Videokonferenzdiensten öffentlich zugängliche Telekommunikationsdienste in öffentlichen Kommunikationsnetzen erbringen, unterfallen sie nicht der DS-GVO, sondern nach Art. 95 DS-GVO der ePrivacy-Richtlinie 2002/58/EG und den nationalen Regelungen zu ihrer Umsetzung. Für sie gelten daher die Regelungen im TKG und die Datenschutzregelungen in §§ 1 bis 18 und 27 bis 30 TTDSG. Dieser Vorrang der ePrivacy-Richtlinie gilt jedoch nur, soweit die ePrivacy-Richtlinie die jeweiligen Rechtsfragen spezifisch regelt. Solche Regelungen enthält die ePrivacy-Richtlinie z. B. nicht für die Auftragsverarbeitung oder für den internationalen Transfer personenbezogener Daten. Daher gelten auch für Telekommunikationsdienste Art. 28 und 44 ff. DS-GVO.

Dagegen unterfällt die Nutzung von Videokonferenzdiensten insgesamt der DS-GVO. Der Veranstalter ist Verantwortlicher im Sinn des Art. 4 Nr. 7 DS-GVO und muss nach Art. 5 Abs. 2 und 24 DS-GVO sicherstellen, dass alle Grundsätze der Datenverarbeitung nach Art. 5 Abs. 1 DS-GVO und alle sonstigen Vorgaben der DS-GVO eingehalten werden. Ergänzend gelten die einschlägigen Regelungen für Telemediendienste in §§ 19 bis 26 TTDSG.

Ob der Anbieter von Videokonferenzdiensten als Auftragnehmer anzusehen ist, hängt davon ab, ob er seinem Vertragspartner ermöglicht, als Verantwortlicher eigene Videokonferenzen zu veranstalten, oder ob er selbst die Videokonferenz gegenüber den Teilnehmern als entgeltliche Dienstleistung erbringt. Soweit er den Verantwortlichen unterstützt, eigene Videokonferenzen zu veranstalten, muss dieser ihn als Auftragnehmer nach Art. 28 Abs. 1 DS-GVO sorgfältig auswählen. Er muss hinreichend Garantien dafür bieten, dass er geeignete technische und organisatorische Maßnahmen so durchführt, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Der Verantwortliche muss mit dem Anbieter von Videokonferenzdiensten einen Auftragsvertrag nach Art. 28 Abs. 3 DS-GVO abschließen. In diesem müssen die Bedingungen für die Einhaltung der DS-GVO vereinbart sein. Im Betrieb muss der Verantwortliche die Leistungserbringung des Auftragnehmers immer wieder danach überprüfen, ob er diese Datenschutzvorgaben auch tatsächlich einhält, und ihn nach Art. 29 DS-GVO entsprechend anweisen. Diese Vorgaben machen besondere Probleme, wenn der Anbieter

der Videokonferenzdienste der Rechtsordnung eines unsicheren Drittlands unterliegt (s. hierzu Kap. 2).

3.2
Videokonferenzsystem für alle hessischen Schulen

Mehr als zweieinhalb Jahre nach den ersten Schulschließungen und der Einführung von Distanzunterricht, der von den Schulen oftmals mit dem Einsatz rechtlich bedenklicher VKS bewerkstelligt wurde, hat das Hessische Kultusministerium (HKM) eine ebenso leistungsfähige wie datenschutzkonforme Lösung umgesetzt. Damit können die hessischen Schulen jetzt auf ein digitales Instrument zurückgreifen, das auch über den pädagogischen Bereich hinaus zur Anwendung kommen könnte.

Es bestand ein dringender Handlungsbedarf für das Ministerium

In meinem 50. Tätigkeitsbericht (Kap. 5.2) hatte ich u. a. geschildert, dass das HKM im März 2020 an mich herangetreten war. Es erbat nach den ersten Schulschließungen und in Anbetracht der Eilbedürftigkeit in der Sache sowie wegen der mangelnden Kenntnisse vieler Schulleitungen rund um die Datenverarbeitung bei der Nutzung von VKS eine pragmatisch orientierte Freigabe der auf dem Markt angebotenen Anwendungen. Die Sicherstellung des schulischen Bildungs- und Erziehungsauftrages gepaart mit einer bisher unbekannten Situation rund um die pandemische Entwicklung hatten mich dann dazu bewogen, eine bis August 2020 befristete Duldung fast aller VKS-Systeme für den pädagogischen Bereich auf der Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. d und e DS-GVO auszusprechen.

Das von mir geforderte datenschutzkonforme, landesweite Angebot für die Schulen, welches das HKM zur Verfügung stellen sollte, konnte bis zum Beginn des Schuljahres 2020/21 nicht realisiert werden. Deshalb trat das Ministerium erneut an mich heran und bat um die Verlängerung der Duldungsphase. Dieser Bitte hatte ich entsprochen und die Duldung bis zum 31. Juli 2021 verlängert. Allerdings waren an die Verlängerung Bedingungen geknüpft (zu den Einzelheiten s. https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/hbdi-duldet-temporaeren-einsatz-von-videokonferenzsysteme-in-schulen).

Europaweite Ausschreibung wird vom Gericht gekippt

Mittlerweile hatte das Ministerium im Frühjahr 2021 im Zuge einer europaweiten Ausschreibung einen Anbieter ausgewählt, der allen 2.000 hessischen Schulen die Nutzung eines VKS ermöglichen sollte. Gegen das Ergebnis

des Auswahlverfahrens ging ein unterlegener Mitbewerber durch die Initiierung eines Vergabenachprüfungsverfahrens vor. Zunächst stellte die Vergabekammer Mängel im Rahmen der Ausschreibung fest und forderte eine Neuausschreibung. Hiergegen legte das HKM Beschwerde beim OLG Frankfurt ein. Das Gericht bestätigte aber per Beschluss Ende Dezember 2021 die Entscheidung der Vergabekammer. Damit musste das Ministerium einen neuen Ausschreibungsprozess in Gang setzen, der den ursprünglich festgesetzten Zeitplan obsolet machte. Auch auf die neue Situation habe ich mit viel Pragmatismus reagiert. Zwar habe ich die Duldung für die Nutzung nicht datenschutzkonformer VKS nicht erneut verlängert, doch im Rahmen meines Handlungsermessens keine repressiven Maßnahmen gegen Schulen eingeleitet, die z. B. die bedenklichen, insbesondere US-amerikanischen Systeme, weiter nutzten (s. auch: https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/duldung-fuer-die-nutzung-insbesondere-us-amerikanischer-anwendungen-laeuft-aus).

Im Frühsommer 2022 ist ein neuer VKS-Dienstleister bestimmt

Die zweite Ausschreibung des Ministeriums stand schließlich unter günstigeren Vorzeichen. Die Wahl fiel auf den deutschen Anbieter German Edge Cloud (GEC), der seinen Sitz in Eschborn bei Frankfurt am Main hat. Das Unternehmen ist bereits für den Betrieb des Schulportals Hessen (SPH) mitverantwortlich und stellt ein VKS mit dem Open-Source-Webkonferenzdienst BigBlueButton (BBB) zur Verfügung.

Im Frühherbst begann die Integration in das Schulportal des Landes, über welches das System u. a. aus Gründen der IT-Sicherheit zugänglich ist. Von Ende September 2022 an stand den hessischen Schulen das neue Angebot schrittweise und nach Bedarf zur Verfügung. Nach Abstimmung mit mir konnten die Schulen zunächst mit den bestehenden VKS weiterarbeiten. Mit Ablauf des ersten Schulhalbjahres 2022/23 endete der Zeitpunkt für die Nutzung von nicht-datenschutzkonformen VKS. Meine Mitarbeiter befanden sich am Ende des Berichtszeitraums noch in der Prüfungsphase. Vor allem Aspekte der IT-Sicherheit, des Zugangs sowie der Einbindung der VKS-Anwendung in das SPH bedürfen einer weiteren Untersuchung. Zudem standen mir noch nicht alle erforderlichen Dokumentationen zur Verfügung. Die bisherigen Prüfungen lassen aber erwarten, dass das VKS den zentralen datenschutzrechtlichen Anforderungen entspricht.

Umgang der Nutzung bedarf einer Festlegung

Ohne Zweifel ist die Beschaffung des landeseinheitlichen VKS für die Schulen für die Durchführung von Distanzunterricht vorgesehen. Das geht über die

Corona-Pandemie hinaus. Man denke nur an Schlechtwetterereignisse, die für Schüler den Weg zur Schule unmöglich machen. Die kurzfristige Nutzung des VKS ist eine probate Alternative zu einem drohenden Unterrichtsausfall. Doch ergeben sich noch weitere Nutzungsmöglichkeiten. Klassen- oder Schulkonferenzen oder sogar Elternabende könnten per VKS in einem erforderlichen Fall ebenfalls durchgeführt werden, soweit damit im Zusammenhang stehende datenschutzrechtliche Fragestellungen geklärt sind. Allerdings bedarf es hinsichtlich der Nutzung noch konkreter Festlegungen durch das Ministerium zu der Fragestellung, wie weit der Umfang einer pädagogischen Nutzung reicht. Zudem wird zu diskutieren sein, ob und in welcher Form die klassische Schulverwaltung das digitale Instrument wird nutzen können.

Datenschutzrechtlicher Mehrwert im Zeichen digitaler Souveränität

Die Einführung eines ebenso performanten wie datenschutzkonformen VKS für alle hessischen Schulen wird von mir sehr begrüßt. Auch wenn der Prozess bis zur Auswahl eines Anbieters und der konkreten Umsetzung anspruchsvoll und teilweise mühsam war, so hat sich der Aufwand meines Erachtens für alle Beteiligten gelohnt. So wird den hessischen Schulen jetzt ein System angeboten, das in eine geschützte IT-Infrastruktur, das SPH, eingebettet ist. Die Umsetzung des Datenschutzes wird durch die Verwendung des Open-Source-Produkts BBB und das Hosting in einem deutschen Rechenzentrum erleichtert. Eine Übermittlung personenbezogener Daten in ein Drittland ohne das Schutzniveau der DS-GVO und der Zugriff Dritter auf diese Daten ohne ausreichenden Rechtsschutz für die Betroffenen ist damit ausgeschlossen. Die Vorgaben des EuGH aus dem Schrems-II-Urteil sind damit hinreichend umgesetzt.

Zudem wird mit dem bundesweit einmaligen Projekt auch dem Aspekt der digitalen Souveränität Rechnung getragen. Die Realisierung nationaler wie europäischer digitaler Datenverarbeitungsprojekte unter dem Schutzschirm der DS-GVO können insbesondere im Bildungsbereich eine adäquate Alternative zu den Angeboten der großen, internationalen Konzerne sein und besser als diese bisher die Einhaltung des gebotenen Grundrechtsschutzes gewährleisten.

3.3
„Hessisches Modell“ für Videokonferenzen in Hochschulen

In meinem 50. Tätigkeitsbericht (Kap. 4.2) habe ich berichtet, vor welche Herausforderungen die Corona-Pandemie die hessischen Hochschulen gestellt hat. Das Leben der Studierenden und Lehrenden hat sich erheblich

verändert. Seitdem werden verstärkt VKS eingesetzt, um Lehrveranstaltungen durchzuführen. Bei der Auswahl der VKS wurde oftmals nicht der Datenschutz in den Vordergrund gestellt, sondern auf am Markt etablierte Anbieter zurückgegriffen, die einen hohen Komfort und eine stabile Verbindung versprachen. Unter anderem ist an den Hochschulen das VKS Zoom verbreitet. Um jedoch auch die Aspekte des Datenschutzes bei der VKS-Nutzung im erforderlichen Umfang zu beachten, haben die Hochschulen und ich unter Moderation des Hessischen Ministeriums für Wissenschaft und Kunst (HMWK) nach geeigneten Lösungen gesucht. Hierbei hat die Universität Kassel mit meiner Unterstützung ein „Hessisches Modell" entwickelt, mit dem das VKS Zoom von den Hochschulen konfiguriert und betrieben werden kann, ohne gegen die Datenschutzvorgaben des Europäischen Gerichtshofs zu verstoßen.

Hintergrund ist die Entscheidung des Europäischen Gerichtshofs vom 16. Juli 2020 (sog. Schrems II-Urteil) (s. ausführlich 50. Tätigkeitsbericht, Kap. 3.1). Danach dürfen personenbezogene Daten in die USA nur dann übertragen werden, soweit ausgeschlossen ist, dass US-Behörden auf diese zugreifen können. Das jedoch kann ein US-amerikanischer Diensteanbieter nicht garantieren, insbesondere dann nicht, wenn er – wie der VKS-Dienstleister Zoom – die Übertragung von Daten in die USA vorsieht. Daher habe ich die im April 2020 ausgesprochene pandemiebedingte Duldung solcher Systeme zum 31. Juli 2021 beendet und in der Folge die hessischen Hochschulen dazu aufgefordert, die Nutzung von VKS US-amerikanischer Anbieter datenschutzgerecht zu gestalten oder zu datenschutzkonformen Systemen zu wechseln.

An hessischen Hochschulen kann das VKS Zoom demnach nur dann für Lehrveranstaltungen genutzt werden, wenn die Hochschulen geeignete Maßnahmen ergreifen, um den Abfluss personenbezogener Daten an Stellen in den USA zu begrenzen und einen Zugriff auf diese durch US-Behörden zu vermeiden.

Anforderungen für eine datenschutzkonforme Anwendung

Setzen die hessischen Hochschulen dieses hier beschriebene „Hessische Modell" in der praktischen Nutzung von Zoom um, bewerte ich das verbleibende Risiko für die Teilnehmenden an Zoom-Videokonferenzen bei den bestehenden Wahlmöglichkeiten mit den datenschutzrechtlichen Vorgaben als vereinbar. Die dem „Hessischen Modell" zugrundeliegenden Anforderungen sind im Folgenden beschrieben.

1. Installation, Konfiguration und Betrieb durch geeigneten Auftragsverarbeiter

   Die Hochschule nutzt einen zwischengeschalteten Auftragsverarbeiter mit Sitz und Standort der Datenverarbeitung in der EU oder dem EWR,

der hier den On-Premise-Betrieb der Zoom-Audio-Video-Konnektoren anbietet. Die verantwortliche Hochschule schließt mit einem solchen Betreiber einen Auftragsverarbeitungsvertrag gemäß Art. 28 Abs. 3 S. 1 DS-GVO ab und kommt ihren dahingehenden Sorgfaltspflichten als für den Datenschutz verantwortliche Stelle nach. Der Auftragsverarbeiter schließt mit dem Anbieter Zoom die Standardvertragsklauseln der EU-Kommission in der jeweils gültigen Fassung ab.

Der Auftragnehmer stellt der verantwortlichen Hochschule das VKS Zoom zur Verfügung und ist deren unmittelbarer Abrechnungspartner. Hierdurch kann die Übermittlung von Abrechnungsdaten an den Anbieter Zoom minimiert oder anonymisiert erfolgen.

Der Auftragsverarbeiter setzt insbesondere solche technischen Maßnahmen um, die geeignet sein können, ein Risiko aus dem Zugriff auf Inhaltsdaten durch den Anbieter Zoom selbst weniger wahrscheinlich werden zu lassen (z. B. durch ein regelmäßiges, prozessgesteuertes Monitoring zum Erkennen und Unterbinden unerwünschten Verbindungsaufbaus).

2. Pseudonymisierung, technische und organisatorische Maßnahmen

   Art und Umfang der personenbezogenen Daten, die trotz des Betriebs der Konnektoren durch den Auftragsverarbeiter weiterhin an Zoom übermittelt werden (Verbindungs-, Telemetrie- und Diagnosedaten), werden in dem Umfang, wie es durch technische und organisatorische Maßnahmen möglich ist, eingeschränkt.

   Die verantwortliche Hochschule verwaltet die Benutzeridentitäten für die Teilnahme an Videokonferenzen in einem von ihr lokal betriebenen Identitätsmanagement (IDM). Sie schränkt die Übermittlung personenbezogener Daten durch das IDM an den Anbieter Zoom in einem Umfang ein, der einen Personenbezug nicht möglich macht. Dazu gehört u. a., dass das IDM eine Übermittlung von Klarnamen an Zoom ausschließt. Durch organisatorische Maßnahmen muss sichergestellt sein, dass nicht etwa Veranstaltungsleiter die Angabe von Klarnamen erzwingen, wenn diese z. B. eine Anwesenheitskontrolle im Rahmen von Seminarformaten durchführen.

   Maßgeblich gehört hierzu auch die Deaktivierung von Funktionalitäten, die nur durch die Übermittlung personenbezogener Daten an den Anbieter Zoom nutzbar sind. Dazu gehören z. B. die Aufzeichnung und Speicherung der Konferenz in der Cloud, die Nutzung der Chat-Funktion oder die Teilnahme mittels Browser.

3. Ende-zu-Ende-Verschlüsselung

   Die Ende-zu-Ende-Verschlüsselung des Zoom-Clients muss vom Verantwortlichen zwingend aktiviert werden. Dabei werden die Schlüssel

im Zoom-Client der Hochschulen und nicht zentral von Zoom erstellt und verteilt. Die Sicherheit der zugrundeliegenden kryptografischen Verfahren ist durch eine externe Zertifizierung nachgewiesen.

4. Virtual Private Network (VPN)

   Die verantwortliche Hochschule bietet den Hochschulangehörigen einen VPN-Zugang an, der geeignet ist, die Übermittlung personenbeziehbarer IP-Adressen an Zoom zu unterbinden. Sie stellt sicher, dass ein solcher VPN-Zugang durch alle interessierten Teilnehmenden für den betrachteten Anwendungsfall genutzt werden kann. Dies schließt insbesondere die Bereitstellung ausreichender technischer Kapazitäten ein.

   Dass ein personenbezogenes Datum des Hosts einer Veranstaltung (Name des Veranstaltungsleiters) übermittelt wird, kann dagegen nicht unterbunden werden. Sofern eine Übermittlung dieses Datums vom Host nicht gewünscht wird, kann er auf ein alternatives datenschutzkonformes VKS ausweichen, das die Hochschule anbietet.

5. Beschränkung hinsichtlich der Nutzung

   Die verantwortliche Hochschule setzt das VKS Zoom im Rahmen der Durchführung von Lehrveranstaltungen ein. Sie schließt grundsätzlich Anwendungsfälle aus, bei denen eine Verarbeitung sensiblerer, personenbezogener Daten erfolgt, z. B. für Zwecke der hochschulinternen Selbstverwaltung, von studentischen Interessenvertretungen, Personalvertretungen oder auch für die Durchführung von Bewerbungsverfahren. Hierfür hält die verantwortliche Hochschule ein alternatives datenschutzkonformes VKS bereit.

6. Ausreichende Information der Teilnehmenden

   Soweit die genannten Sicherheitsmaßnahmen ein Mitwirken der an dem VKS Teilnehmenden erfordern oder ihnen eine Wahlmöglichkeit eröffnen, muss die Hochschule die Teilnehmenden ausreichend darüber informieren, durch welche Maßnahmen sie ihre informationelle Selbstbestimmung schützen können. Diese Information muss sowohl zusammenhängend leicht auffindbar als auch bei den einzelnen Nutzungsschritten in der Anwendung des VKS in dem jeweils erforderlichen Umfang angeboten werden.

Zusammenfassung

Zusammenfassend lässt sich festhalten, dass die Hochschulen die datenschutzrechtlichen Defizite des US-amerikanischen Anbieters Zoom ausgleichen und einen datenschutzgerechten Betrieb des VKS gewährleisten können. Sie stellen beim „Hessischen Modell“ deshalb sicher, dass sie

– einen von Zoom unabhängigen Auftragsverarbeiter mit Sitz in der EU oder im EWR beauftragen, das Videokonferenzsystem auf Servern in der EU oder im EWR zu betreiben und mit ihnen abzurechnen,
– eine Ende-zu-Ende-Verschlüsselung aller Inhaltsdaten zur Verfügung stellen,
– den Abfluss personenbezogener Daten von Teilnehmenden in die USA und den Zugriff auf solche Daten aus den USA heraus verhindern,
– die Nutzung von Zoom auf Lehrveranstaltungen beschränken,
– ein alternatives datenschutzkonformes VKS für andere Zwecke oder für Lehrpersonen, die nicht mit Zoom arbeiten wollen, anbieten,
– die Lehrenden und Studierenden über weiterführende, unterstützende Maßnahmen zum Schutz der informationellen Selbstbestimmung ausführlich informieren.

3.4
Videokonferenzsystem in der hessischen Landesverwaltung

Im Berichtszeitraum konnten mit der europaweiten Ausschreibung für den Aufbau und den Betrieb eines VKS und der nachfolgenden Zuschlagserteilung zwei wesentliche Meilensteine auf dem Weg zu einem neuen und datenschutzkonformen VKS für die hessische Landesverwaltung erreicht werden. Ich berate dieses Großprojekt nicht erst seit dem aktuellen Berichtszeitraum. Auch für die Zukunft gehe ich von einer Fortsetzung der erfolgreichen Zusammenarbeit mit der Hessischen Ministerin für Digitale Strategie und Entwicklung (HMinD) aus.

Hintergrund

Auch in der Landesverwaltung wurde zu Beginn der Corona-Pandemie bei der Suche nach tauglichen VKS Datenschutzfragen erst einmal zurückgestellt. Ich habe dies im ersten Jahr der Pandemie angesichts des dringenden Bedarfs nach einer kurzfristigen Bereitstellung von VKS für vertretbar gehalten. Gleichzeitig äußerte ich die Prognose, dass die großflächige Nutzung von VKS keine kurzzeitige Erscheinung bleiben werde und in vielen Bereichen mit einem dauerhaften Einsatz zu rechnen sei (50. Tätigkeitsbericht, Kap. 4.2). Daher war es notwendig, nach datenschutzkonformen Alternativen zu suchen.

Die Rahmenbedingungen für die Einführung eines neuen VKS haben sich seit Beginn der Pandemie verändert. So ist aufgrund der Vielzahl vorhandener Angebote seit einiger Zeit eine Situation gegeben, in der Verantwortliche im Sinne des Art 4 Nr. 7 DS-GVO die Möglichkeit haben, ein VKS so

auszuwählen, zu gestalten und zu nutzen, dass sie ihre nach der DS-GVO bestehenden Pflichten erfüllen können. Verantwortliche sind folglich in der Lage, im Bereich von VKS mit Blick auf den Datenschutz digital souverän zu agieren. Dementsprechend habe ich Verantwortliche dazu aufgerufen, ihre digitale Souveränität zu nutzen und sich auf den Weg hin zu einem datenschutzrechtskonformen VKS zu machen.

Abhängig von den Zwecken und den Rahmenbedingungen des Einsatzes eines VKS kann es sich bei der Konzeption, der Umsetzung und der Einführung um ein Projekt erheblicher Größe und Laufzeit handeln. Hierbei ist es unerlässlich, dass datenschutzrechtliche Anforderungen von Beginn an, durchgängig und umfassend berücksichtigt und umgesetzt werden. Gerade der frühen Projektphase kommt hier eine besondere Bedeutung zu. Denn in dieser werden in der Regel richtungsweisende Entscheidungen getroffen und somit das Fundament für alle weiteren Projektphasen sowie den Einsatz des VKS gelegt.

Das Beratungsangebot meiner Behörde

Meine Behörde unterstützt öffentliche Stellen in Hessen im Rahmen von IT-Projekten. Die angebotenen Beratungsleistungen können sich hierbei auf unterschiedliche datenschutzrechtliche Fragestellungen und Themenfelder in verschiedenen Projektphasen beziehen sowie in Art und Umfang stark variieren. Die konkrete Ausgestaltung ist von den Spezifika des jeweiligen Projekts und dessen Beratungsbedarf abhängig. Trotz beratender Unterstützung durch meine Behörde bleibt die Umsetzung datenschutzrechtlicher Anforderungen Aufgabe der Verantwortlichen. Gleiches gilt in besonderem Maße für Entscheidungen im Rahmen des Projekts sowie für die Abnahme von Dokumenten, Meilensteinen oder anderen Projektergebnissen. Es ist daher unerlässlich, dass projektseitig in ausreichendem Maße datenschutzrechtliche Expertise eingeplant und bereitgestellt wird. Die Beratung durch meine Behörde ersetzt dies nicht – zumal eine Beratung immer nur im Rahmen der vorhandenen Ressourcen meiner Behörde erfolgen kann.

Das Projekt HessenConnect 2.0

Das zentrale VKS der hessischen Landesverwaltung HessenConnect 1.0 wurde bereits vor der Corona-Pandemie eingeführt. Während der Pandemie stieg seine Bedeutung für die Zusammenarbeit innerhalb der und zwischen den Dienststellen der hessischen Landesverwaltung sprunghaft an. So wurde das VKS in meiner Behörde beispielsweise erst nach dem Ausbruch der Pandemie an jedem Arbeitsplatz zur Verfügung gestellt. Binnen kürzester

Zeit ist es anschließend zu einem unverzichtbaren Bestandteil des Kommunikationsportfolios meiner Mitarbeiterinnen und Mitarbeiter geworden.

Bereits seit längerem steht fest, dass HessenConnect 1.0 durch ein neues VKS ersetzt werden muss. Hierzu wurde von Seiten der HMinD noch vor dem Berichtszeitraum ein mehrjähriges Projekt initiiert, in das ich bereits frühzeitig eingebunden wurde. Seitdem beraten Mitarbeitende meiner Behörde mit juristischem und technischem Schwerpunkt das Projekt HessenConnect 2.0. Dadurch konnte ich schon im Rahmen der Erstellung der für die Ausschreibung vergaberechtlich notwendigen Leistungsbeschreibung datenschutzrechtlichen Anforderungen angemessenes Gewicht verleihen.

Mit der Ausschreibung unter Berücksichtigung datenschutzrechtlicher Vorgaben wurde aus meiner Sicht ein erster wesentlicher Meilenstein erreicht. Es zeigte sich, dass die Integration des Datenschutzes in Ausschreibungsverfahren ein wesentlicher Erfolgsfaktor für nachfolgende Projektphasen ist. Dabei hatte die explizite Aufnahme datenschutzrechtlicher Anforderungen keineswegs abschreckende Wirkung auf mögliche Anbietende. Vielmehr leistete sie einen wesentlichen Beitrag dazu, dass Anbietende den Vorschriften des Datenschutzrechts die notwendige Bedeutung beimaßen und dies in ihren Angeboten entsprechend berücksichtigten.

Mit dem Abschluss der Ausschreibung und der Zuschlagserteilung wurde im Berichtszeitraum ein zweiter, wesentlicher Meilenstein erreicht. HessenConnect 2.0 soll auf Basis einer integrierten und auf Open Source-Software basierenden Lösung (Matrix/Elements als Messenger-Dienst und Jitsi als VKS) umgesetzt und betrieben werden. Ich sehe hierin eine vielversprechende Grundlage für die bereits im Berichtszeitraum begonnenen Folgephasen des Projekts.

Die beiden Meilensteine unterstreichen, dass Verantwortlichen bei VKS unterschiedliche datenschutzrechtskonforme Alternativen zur Verfügung stehen. Sie sind somit nicht gezwungen, auf datenschutzrechtlich problematische Lösungen zurückzugreifen. Hierzu ist jedoch erforderlich, dass Verantwortliche ihrer Rolle gerecht werden und die Erfüllung der datenschutzrechtlichen Anforderungen explizit und nachdrücklich einfordern. Nur auf dieser Basis können sie ihre digitale Souveränität in datenschutzrechtlicher Hinsicht auch tatsächlich nutzen.

Ich begrüße ausdrücklich, dass die hessische Landesverwaltung ihre Möglichkeiten ausgeschöpft hat, um gemeinsam eine zukunftsfähige und datenschutzrechtskonforme VKS-Lösung zu finden. Der bisherige Projektverlauf stellt für mich ein besonders positives Beispiel für eine kooperative, lösungsorientierte und erfolgreiche Zusammenarbeit im Rahmen der datenschutzrechtlichen Beratung von IT-Projekten durch meine Behörde dar.

Ausblick

Zukünftig wird die im aktuellen Berichtszeitraum begonnene Umsetzung des VKS HessenConnect 2.0 weiter fortschreiten. Meine Mitarbeitenden werden dem Projekt auch in den nächsten Phasen tatkräftig beratend zur Seite stehen und die bisher erfolgreiche Zusammenarbeit fortsetzen, sofern dies seitens der Projektverantwortlichen gewünscht ist.

Ich gehe davon aus, dass die hessische Landesregierung und insbesondere die HMinD ihre Anstrengungen unvermindert fortsetzen, um den Mitarbeiterinnen und Mitarbeitern der hessischen Landesverwaltung am Ende des Projekts ein datenschutzrechtskonformes und datenschutzfreundliches VKS bereitzustellen. Mit den bisher erreichten Meilensteinen wurde jedenfalls eine vielversprechende Grundlage hierfür gelegt.

4. Europa, Internationales

Die DS-GVO hat zu einer starken Europäisierung des Datenschutzrechts, aber auch des Datenschutzvollzugs geführt. Mit dem EDSA ist eine europäische Datenschutzinstitution entstanden, die auf den Vollzug in allen Mitgliedstaaten durch Empfehlungen, Leitlinien und verbindliche Entscheidungen starken Einfluss ausübt. Diese Beschlüsse werden in Unter-Gremien des EDSA vorbereitet. Zugleich zwingt die DS-GVO zu einer intensiven Zusammenarbeit zwischen den Aufsichtsbehörden der Mitgliedstaaten, die für alle zu einer erheblichen Mehrarbeit führt. Im EDSA, in seinen Unter-Gremien und in der täglichen Zusammenarbeit der Aufsichtsbehörden wird entschieden, wie der europäische Datenschutz zu verstehen ist und gelebt wird. Daher ist Mitarbeit der deutschen Aufsichtsbehörden im europäischen Datenschutzverbund unabdingbar (Kap. 4.1). Dass diese Mitarbeit ermöglicht, Einfluss auszuüben und sogar die Entscheidungen anderer Aufsichtsbehörden zu korrigieren, zeigen beispielhaft zwei Verfahren zur Festsetzung von Geldbußen gegen Meta Ireland (Kap. 4.2).

4.1
Zusammenarbeit mit anderen Aufsichtsbehörden in Europa und in Deutschland

Mit Inkrafttreten der DS-GVO haben sich zahlreiche Neuerungen für die Zusammenarbeit der Aufsichtsbehörden in Deutschland und Europa ergeben. Art. 60 Abs. 1 S. 1 DS-GVO verpflichtet die europäischen Datenschutzaufsichtsbehörden, in Fällen grenzüberschreitender Datenverarbeitungen im Bemühen, einen Konsens zu erzielen, eng zu kooperieren. Um den kommunikativen und organisatorischen Mehraufwand zu bewältigen, der sich aus der Intensivierung der Zusammenarbeit ergibt, habe ich im Jahr 2019 die Stabsstelle Europa und Internationales eingerichtet, die als Bindeglied zwischen der Hessischen Datenschutzaufsichtsbehörde und verschiedenen Stellen außerhalb Hessens in Deutschland, Europa und der Welt fungiert.

Verfahren der Kooperation und Kohärenz nach Kapitel VII DS-GVO

Alle bei mir eingehenden Beschwerden, Anfragen und Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO werden in den Fachreferaten zunächst daraufhin überprüft, ob eine grenzüberschreitende Verarbeitung vorliegt, die die Pflicht zur Zusammenarbeit mit anderen europäischen Aufsichtsbehörden auslöst (s. hierzu auch 47., 48., 49. und 50. Tätigkeitsbericht, Kap. 2.1, 3.2, 4.2.2 und 5). Eine grenzüberschreitende Verarbeitung liegt gemäß Art. 4 Nr. 23 DS-GVO vor, wenn der

Verantwortliche oder der Auftragsverarbeiter in mehreren Mitgliedstaaten niedergelassen ist und die Verarbeitung in mehreren dieser Niederlassungen erfolgt oder wenn es nur eine einzelne Niederlassung in der EU oder dem EWR gibt, aber die Verarbeitung erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Nach dem mit der DS-GVO eingeführten Konzept des sog. „One-Stop-Shop" ist bei grenzüberschreitenden Datenverarbeitungen eine Aufsichtsbehörde – grundsätzlich die Aufsichtsbehörde am Ort der Hauptniederlassung des Verantwortlichen oder des Auftragsverarbeiters (Art. 56 Abs. 1 DS-GVO) – als federführende Aufsichtsbehörde einziger Ansprechpartner des Verantwortlichen oder des Auftragsverarbeiters (Art. 56 Abs. 6 DS-GVO). Dies bringt für ein Unternehmen die Erleichterung, sich wegen ein und derselben Datenverarbeitung nur mit einer Aufsichtsbehörde auseinandersetzen zu müssen. Dies bedeutet aber für die Aufsichtsbehörden einen Mehraufwand, weil die federführende Aufsichtsbehörde nicht alleine entscheidet. Vielmehr wirken neben der federführenden Aufsichtsbehörde auch alle weiteren betroffenen Aufsichtsbehörden an der Entscheidungsfindung mit. „Betroffen" („concerned") sind nach Art. 4 Nr. 22 DS-GVO alle Aufsichtsbehörden, in deren Hoheitsgebiet der Verantwortliche oder der Auftragsverarbeiter niedergelassen ist, individuell betroffene Personen („data subjects") ihren Wohnsitz haben oder bei denen eine Beschwerde eingereicht wurde.

Die Zusammenarbeit, Abstimmung und Kommunikation in grenzüberschreitenden Verwaltungsverfahren erfolgt elektronisch über das sog. „IMI-System" (Internal Market Information System, deutsch: Binnenmarkt-Informationssystem). Die Arbeitssprache im IMI-System ist Englisch.

Beschwerden, Meldungen nach Art. 33 DS-GVO und sonstige Anfragen mit grenzüberschreitendem Bezug, die bei den europäischen Datenschutzbehörden eingehen, werden in einem ersten Schritt in einem Verfahren nach Art. 56 DS-GVO zur Feststellung der federführenden und betroffenen Aufsichtsbehörden in das IMI-System eingestellt. Dabei ist der Sachverhalt für die anderen Aufsichtsbehörden aufzubereiten, in englischer Sprache zusammengefasst zu schildern und die mutmaßlich federführende Aufsichtsbehörde sowie die mutmaßlich betroffenen Aufsichtsbehörden anzugeben. Alle Aufsichtsbehörden haben dann Gelegenheit, den Fall zu prüfen und sich als federführende oder betroffene Aufsichtsbehörde zu melden.

Wird im Art. 56-Verfahren festgestellt, dass die europäische Federführung bei mir liegt, da z. B. der Verantwortliche in Hessen niedergelassen ist, leitet die Stabsstelle Europa und Internationales die über das IMI-System eingegangene Beschwerde, Anfrage oder Meldung nach Art. 33 DS-GVO

an mein jeweiliges Fachreferat weiter, das dann nach eingehender Prüfung des Sachverhalts den Kontakt zum Verantwortlichen aufnimmt.

Für den Fall, dass die Federführung für eine bei mir eingegangene Beschwerde, Anfrage oder Meldung nach Art. 33 DS-GVO bei einer anderen europäischen Aufsichtsbehörde liegt, übermittelt die Stabsstelle Europa und Internationales diese über das IMI-System zur Bearbeitung an die jeweils federführend zuständige Behörde. Hierzu müssen die Eingabe sowie alle weiteren zur Bearbeitung notwendigen Unterlagen und sachdienlichen Informationen ins Englische übersetzt werden. Als betroffene Aufsichtsbehörde wirke ich in diesen Verfahren an der Entscheidungsfindung mit und bleibe im sog. One-Stop-Shop Ansprechpartner für die Eingebende oder den Eingebenden und informiere in regelmäßigen Abständen über den Stand der Bearbeitung.

Die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden arbeiten im Kooperationsverfahren eng zusammen und versuchen, einen Konsens zu erzielen (Art. 60 Abs. 1 DS-GVO). Die federführende Aufsichtsbehörde prüft gem. Art. 60 Abs. 3 S. 2 DS-GVO den Fall und legt den betroffenen Aufsichtsbehörden nach Abschluss der Ermittlungen einen Beschlussentwurf vor. Gegen diesen Beschlussentwurf können die betroffenen Aufsichtsbehörden nach Art. 60 Abs. 4 DS-GVO Einspruch einlegen. Bei unlösbaren Meinungsverschiedenheiten wird die Angelegenheit dem EDSA im Kohärenzverfahren nach Art. 63 DS-GVO zur verbindlichen Entscheidung vorgelegt.

Fallzahlen und Prüfungsaufwand

Die Zahl der über das IMI-System gemeldeten Beschwerden, Anfragen und Art. 33-Meldungen ging im Berichtszeitraum zurück und hat sich wieder dem Level aus dem Jahr 2019 angenähert. Die Zahl der Verfahren der gegenseitigen Amtshilfe ist im Berichtszeitraum dagegen weiter deutlich angestiegen.

Europäisches Verfahren	Anzahl 2019	Anzahl 2020	Anzahl 2021	Anzahl 2022
Art. 56-Verfahren gesamt	633	812	1419	645
Art. 56-Verfahren mit Betroffenheit	17	32	47	11
Art. 56-Verfahren mit Federführung	4	7	16	2
Art. 61-Verfahren (Amtshilfe)	65	26	92	155

Tabelle 1: Europäische Verfahren

Im Berichtszeitraum waren von der Stabsstelle Europa und Internationales insgesamt 645 im IMI-System eingetragene Art. 56-Verfahren auf eine mögliche Betroffenheit oder Federführung zu prüfen. In elf dieser Verfahren hat die Stabsstelle Europa und Internationales mich als „betroffen“ gemeldet, befasste sich in der Folge inhaltlich mit der Angelegenheit und wirkte an der Entscheidungsfindung mit. In zwei Verfahren habe ich die Bearbeitung der Beschwerde als federführende Aufsichtsbehörde übernommen.

Der im Berichtsjahr gegenüber dem Vorjahr zu verzeichnende Rückgang der Art. 56-Verfahren erklärt sich u. a. dadurch, dass mittlerweile für eine Vielzahl von Verantwortlichen und Auftragsverarbeitern und eine Vielzahl spezifischer Datenverarbeitungskonstellationen bereits Fallregister (sog. „Case Register“) in IMI angelegt sind, auf die aufbauend neue Vorgänge direkt – etwa als neues Art. 61-Verfahren – in IMI eingestellt werden können, ohne dass ein neues Art. 56-Verfahren zur Klärung der Federführung und Betroffenheit erforderlich wird. Der Rückgang der Art. 56-Verfahren geht also mit einem Anstieg der Art. 61-Verfahren einher. Es ist daher zu erwarten, dass die Zahl der Verfahren der gegenseitigen Amtshilfe nach Art. 61 DS-GVO in Zukunft weiter zunimmt.

Genehmigung von Binding Corporate Rules

Neben den über das IMI-System zu bearbeitenden grenzüberschreitenden Verwaltungsverfahren lag auch im zurückliegenden Berichtsjahr ein weiterer Schwerpunkt der Tätigkeit der Stabsstelle Europa und Internationales in der Prüfung und Genehmigung von Binding Corporate Rules (deutsch: verbindliche interne Datenschutzvorschriften, englisch kurz: BCR) nach Art. 47 DS-GVO, die sich – nicht zuletzt seit dem sog. Schrems II-Urteils des EuGH vom 16. Juli 2020 (Rs. C-311/18) und der Unwirksamkeit des EU-US Privacy Shields – als Transferinstrument für Datenübermittlungen in Drittländer wachsender Beliebtheit erfreuen.

BCR sind komplexe Vertragswerke mit Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein multinationaler Konzern verpflichtet, um personenbezogene Daten innerhalb der Unternehmensgruppe in sog. „Drittländer“ (d. h. Länder außerhalb des Europäischen Wirtschaftsraumes) zu übermitteln, die an und für sich kein angemessenes Datenschutzniveau bieten.

BCR werden in einem europaweiten Kooperationsverfahren von Aufsichtsbehörden mehrerer Mitgliedstaaten gemeinsam geprüft. Auch hierbei agiert eine Aufsichtsbehörde als Federführung, als sog. „BCR Lead“, und koordiniert das Verfahren. Eine oder zwei weitere Aufsichtsbehörden werden unterstützend als sog. „Co-Prüfer“ tätig. Zudem müssen seit Inkrafttreten

der DS-GVO und in Abkehr vom vorherigen sog. Mutual Recognition-Verfahren alle europäischen Aufsichtsbehörden gemäß dem in Art. 63 DS-GVO festgelegten Konsistenzmechanismus einbezogen werden und Gelegenheit zur Prüfung und Kommentierung der BCR erhalten, bevor der EDSA eine Stellungnahme hierzu abgibt.

Erst wenn diese Stellungnahme positiv ausfällt, also im EDSA eine Mehrheit der Mitgliedstaaten für die Genehmigung der BCR stimmt, kann die federführende Behörde einen Genehmigungsbescheid erlassen, der dann auch für die übrigen Aufsichtsbehörden bindend ist. Alle europäischen Aufsichtsbehörden werden damit stärker in die Verantwortung und Pflicht genommen. Das Ziel der Verfahrensneuerung ist eine stärkere Vereinheitlichung der BCR, womit aber auch ein neuer und erhöhter Prüfungsaufwand für die Aufsichtsbehörden einhergeht.

Da Hessen häufig Standort von großen global agierenden Unternehmensgruppen ist, bin ich sehr häufig in BCR-Genehmigungsverfahren als Federführung innerhalb Deutschlands beteiligt oder gar europaweit als BCR Lead federführend zuständig. Im Berichtsjahr war ich in vier BCR-Genehmigungsverfahren als europaweiter BCR Lead federführend zuständig. Zudem habe ich in fünf weiteren Verfahren die Co-Prüfung und in weiteren sechs Verfahren die innerdeutsche Federführung übernommen. Besonders erfreulich war, dass im Berichtszeitraum das Genehmigungsverfahren für die BCR für Verantwortliche (sog. Controller-BCR) von Fresenius SE & Co. KGaA und Fresenius Kabi AG mit einer positiven Stellungnahme des EDSA und meinem finalen Genehmigungsbescheid zum Abschluss gebracht werden konnte.

Mitarbeit in Gremien des EDSA

Neben den Aufgaben in grenzüberschreitenden Verwaltungsverfahren und bei der Prüfung von BCR arbeitet die Stabsstelle Europa und Internationales auf nationaler und europäischer Ebene weiter in verschiedenen Arbeitsgremien der DSK und Arbeitsgruppen des EDSA mit.

Auf europäischer Ebene hat die Stabsstelle die Vertretung Deutschlands in der International Transfers Subgroup fortgeführt. Die International Transfers Subgroup befasst sich mit internationalen Datenübermittlungen und sämtlichen Themen und Fragen, die sich auf diesem Gebiet stellen. Neben der Teilnahme an regelmäßigen Sitzungen der Subgroup und BCR-Sessions engagiert sich die Stabsstelle Europa und Internationales in diversen Drafting Teams und Task Forces und berichtet gemeinsam mit Kolleginnen und Kollegen des LDA Bayern und des BfDI den deutschen Aufsichtsbehörden stetig über die Arbeit der Subgroup und die Entwicklungen auf dem Gebiet des europäischen und internationalen Datenschutzrechts. Die Rückmeldungen

aus den deutschen Aufsichtsbehörden bringe ich als Ländervertreter dann wiederum in die Diskussionen auf europäischer Ebene ein. So gelingt es z. B., Einfluss auf vom EDSA zu verabschiedende Leitlinien und Empfehlungen zu nehmen, die dann für die spätere aufsichtsbehördliche Tätigkeit maßgeblich und richtungsweisend werden.

Neben den Informationen aus der International Transfers Subgroup sichtet die Stabsstelle Europa und Internationales aber auch sämtliche Posteingänge aus den übrigen Subgroups des EDSA (z. B. Arbeitspapiere und -ergebnisse, Tagesordnungen und Protokolle), die die Stabsstelle zum Teil per E-Mail, aber auch elektronisch über die Web-Plattform Confluence erreichen und an mein jeweils zuständiges Fachreferat – sei es zur bloßen Information und Kenntnis oder gegebenenfalls weiteren Veranlassung – weitergeleitet werden müssen. Dies versetzt die Fachreferate in die Lage, sich aktiv und gestaltend in die Arbeiten auf europäischer Ebene einzubringen und z. B. durch Mitarbeit in ad-hoc-Gruppen oder frühzeitige Kommentierung von Papieren, die sich noch im Entwurfsstadium befinden, Einfluss auf den europäischen Meinungsbildungsprozess zu nehmen.

Unterstützung der DSK in Fragen des europäischen Datenschutzes

Auch auf nationaler Ebene wurde die Mitarbeit in Arbeitsgremien der DSK zur Unterstützung in Fragen des europäischen Datenschutzes fortgeführt. So übernimmt die Stabsstelle weiterhin die Leitung des bundesweiten Arbeitskreises Organisation und Struktur, der die Arbeit der DSK in wichtigen organisatorischen Fragestellungen unterstützt und Konzepte und Prozesse zur besseren Verzahnung der Arbeit auf deutscher und europäischer Ebene entwickelt. Ein weiterer Themenkreis, mit dem sich der Arbeitskreis intensiv beschäftigt, sind Fragen, die sich aus der europäischen Zusammenarbeit nach Kapitel VII der DS-GVO ergeben, einschließlich der konkreten Abwicklung dieser Verfahren im IMI-System. Neben der Organisation regelmäßiger Arbeitskreissitzungen hat die Stabsstelle Europa und Internationales hier stetig die Entwicklungen auf nationaler und europäischer Ebene zu beobachten und zu bewerten, um den Kolleginnen und Kollegen der anderen deutschen Aufsichtsbehörden berichten zu können. Daneben nimmt die Stabsstelle Europa und Internationales für mich weiterhin auch an den Sitzungen des Arbeitskreises Internationaler Datenverkehr teil, der Fragen der grenzüberschreitenden Datenübermittlung im Blick hat.

4.2
Einflussnahme auf Entscheidungen anderer Aufsichtsbehörden

Im Berichtszeitraum wurden in Kooperations- und Kohärenzverfahren nach Kapitel VII DS-GVO eine Reihe substanzieller Maßnahmen und beachtlich hohe Geldbußen gegen globale IT-Konzerne auf den Weg gebracht, auf die ich durch die Mitarbeit in EDSA-Gremien Einfluss nehmen konnte. Exemplarisch seien hier zwei Verfahren gegen Meta Platforms Ireland Limited (kurz im Folgenden: Meta Ireland, ehemals Facebook Ireland Limited) genannt, in denen sich die EWR-Aufsichtsbehörden mit Grundpfeilern des EU-Datenschutzrechts, nämlich mit der Rechtmäßigkeit der Verarbeitung nach Art. 6 DS-GVO und Fragen der Geldbußenbemessung bei festgestellten Datenschutzverstößen, zu befassen hatten.

Offenlegung von Kinderdaten in Instagram

In einem Verfahren gegen Meta Ireland, das die Verarbeitung personenbezogener Daten von Kindern durch den Dienst Instagram betraf, hat die federführend zuständige irische Datenschutzaufsichtsbehörde (Data Protection Commission; kurz: DPC) nach Intervention der anderen EWR-Aufsichtsbehörden eine Geldbuße in Rekordhöhe von 405 Millionen Euro nebst einer Reihe weiterer Abhilfemaßnahmen nach Art. 58 Abs. 2 DS-GVO verhängt. Bei der verhängten Geldbuße handelt es sich um die zweithöchste Geldbuße seit Anwendbarkeit der DS-GVO.

Hintergrund der Maßnahme war eine durch die DPC von Amts wegen durchgeführte Untersuchung der durch den Dienst Instagram praktizierten Offenlegung personenbezogener Daten von Kindern. Das soziale Netzwerk hatte es Nutzern im Alter von 13 bis 17 Jahren erlaubt, die Funktion Instagram Business-Konto zu nutzen. Mit einem Wechsel von einem Privat- zu einem Business-Konto wurden die Kontaktinformationen der betroffenen Kinder (E-Mail-Adressen und Telefonnummern) öffentlich zugänglich. Zudem waren auch persönliche Instagram-Konten von Kindern nach standardmäßiger Voreinstellung „öffentlich“.

Im Rahmen der Untersuchungen wurde Meta Ireland angehört und stützte die Veröffentlichung der Kontaktinformationen von Kindern, welche die Funktion Instagram Business-Konto nutzen, als Rechtsgrundlagen alternativ auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO („Vertragserfüllung“) oder Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO („berechtigtes Interesse“). Die DPC hatte diese Praxis zunächst nicht beanstandet und den anderen betroffenen Aufsichtsbehörden im EWR (auch mir) einen Beschlussentwurf vorgelegt, in dem sie befand, dass sich Instagram auf die genannten Rechtsgrundlagen für die Verarbeitung der Kontaktinformationen der Kinder berufen könne.

Gegen diesen Beschlussentwurf der DPC legten eine Reihe betroffener Aufsichtsbehörden – darunter auch einige deutsche Aufsichtsbehörden – Einspruch ein. Beanstandet wurden nicht nur die Schlussfolgerungen der DPC hinsichtlich der Rechtsgrundlage für die Verarbeitung, sondern auch die in ihrer Höhe als unzulänglich erachtete Festsetzung der Geldbuße. Für die deutschen Aufsichtsbehörden wurde der Einspruch vom Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) koordiniert, der nach § 19 Abs. 2 BDSG aufgrund einer Niederlassung von Meta in Hamburg innerdeutsch federführend zuständig ist.

Die DPC schloss sich den Einsprüchen der EWR-Aufsichtsbehörden nicht an und leitete stattdessen nach Art. 65 Abs. 1 Buchst. a DS-GVO ein Streitbeilegungsverfahren beim EDSA ein.

Der EDSA stellte daraufhin am 2. September 2022 durch verbindlichen Beschluss fest, dass es für die DPC keinen Grund zu der Annahme gab, dass die Verarbeitung durch Instagram für die Erfüllung eines Vertrags erforderlich war und sich Meta Ireland folglich nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO als Rechtsgrundlage für diese Verarbeitung stützen konnte. Auch in Bezug auf das berechtigte Interesse als alternative Rechtsgrundlage für die Verarbeitung stellte der EDSA fest, dass die Veröffentlichung der E-Mail-Adressen oder Telefonnummern von Kindern die Anforderungen nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO nicht erfüllte. Die Verarbeitung war weder notwendig, noch war sie, falls sie für notwendig erachtet worden wäre, durch überwiegende berechtigte Interessen von Meta gedeckt. Der EDSA kam daher zu dem Schluss, dass Meta Ireland die personenbezogenen Daten von Kindern ohne Rechtsgrundlage unrechtmäßig verarbeitet hatte, und wies die DPC an, den Beschlussentwurf zu ändern und darin einen Verstoß gegen Art. 6 Abs. 1 DS-GVO festzustellen. Zudem wies der EDSA die DPC an, die geplante Geldbuße gemäß Art. 83 Abs. 1 und 2 DS-GVO zu überprüfen und eine wirksame, verhältnismäßige und abschreckende Geldbuße zu verhängen. Dem ist die DPC mit der Feststellung eines Datenschutzverstoßes und der nun verhängten Geldbuße in Höhe von 405 Millionen Euro nachgekommen.

Unzureichende Einwilligung in Facebook und Instagram

In einem weiteren Verfahren gegen Meta Ireland im Zusammenhang mit der Bereitstellung der Facebook- und Instagram-Dienste hat die DPC – ebenfalls nach Intervention der EWR-Aufsichtsbehörden und Beschluss des EDSA im Streitbeilegungsverfahren – Geldbußen in Höhe von 210 Millionen Euro für Verstöße gegen die DS-GVO im Zusammenhang mit dem Facebook-Dienst und in Höhe von 180 Millionen Euro für Verstöße im Zusammenhang mit dem Instagram-Dienst verhängt.

Anlass der Verfahren waren eine Beschwerde einer betroffenen Person aus Österreich (in Bezug auf Facebook) und eine Beschwerde einer betroffenen Person aus Belgien (in Bezug auf Instagram), die bereits am 25. Mai 2018, d. h. am Tag des Inkrafttretens der DS-GVO, eingereicht worden waren.

Im Vorfeld des 25. Mai 2018 und des DS-GVO-Inkrafttretens hatte Meta Ireland die Nutzungsbedingungen für seine Facebook- und Instagram-Dienste geändert. Nutzer wurden darüber informiert, dass sich die Rechtsgrundlage, auf die beide Dienste die Verarbeitung personenbezogener Daten von Nutzenden stützten, geändert habe. Bislang hatte sich Meta Ireland für die Verarbeitung personenbezogener Daten von Nutzenden der Facebook- und Instagram-Dienste auf deren Einwilligung gestützt. Nun versuchte Meta Ireland, sich für die meisten Verarbeitungen im Zusammenhang mit den Facebook- und Instagram-Diensten (einschließlich verhaltensorientierter Werbung) auf die Rechtsgrundlage der „Vertragserfüllung" aus Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO zu stützen. Wollten bestehende (und neue) Nutzende nach Inkrafttreten der DS-GVO (weiterhin) Zugang zu den Diensten von Facebook und Instagram haben, wurden sie aufgefordert, ihr Einverständnis mit den aktualisierten Nutzungsbedingungen zu erklären.

Meta Ireland vertrat in einer Anhörung die Ansicht, dass mit der Annahme der aktualisierten Nutzungsbedingungen ein Vertrag zwischen Meta Ireland und den Nutzern zustande kommt und die Verarbeitung von Nutzerdaten im Zusammenhang mit der Bereitstellung ihrer Facebook- und Instagram-Dienste für die Erfüllung dieses Vertrags erforderlich sei, wozu auch die Bereitstellung von personalisierten Diensten und verhaltensorientierter Werbung gehöre, so dass diese Verarbeitungen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO rechtmäßig seien.

Die Beschwerdeführer machten dagegen geltend, dass sich Meta Ireland entgegen ihrer Behauptung immer noch auf die Einwilligung als Rechtsgrundlage für die Verarbeitung der Nutzerdaten stütze und diese erzwinge. Indem Meta Ireland den Zugang zu seinen Diensten von der Zustimmung der Nutzenden zu den aktualisierten Nutzungsbedingungen abhängig mache, zwinge es sie faktisch dazu, der Verarbeitung ihrer personenbezogenen Daten für verhaltensbezogene Werbung und andere personalisierte Dienste zuzustimmen. Dies stelle einen Verstoß gegen die DS-GVO dar.

Nach umfassenden Untersuchungen legte die DPC den betroffenen EWR-Behörden (darunter mir) zwei Beschlussentwürfe vor, in denen die DPC eine Reihe von Feststellungen gegen Meta Ireland traf. Insbesondere stellte die DPC fest, dass Meta Ireland gegen die Transparenzverpflichtungen aus Art. 5 Abs. 1 Buchst. a DS-GVO und Art. 12 und Art. 13 Abs. 1 Buchst. c DS-GVO verstoßen habe, indem die Nutzer nicht ausreichend darüber in-

formiert wurden, welche Verarbeitungen ihrer personenbezogenen Daten zu welchem Zweck und auf Basis welcher Rechtsgrundlage durchgeführt wurden. Die von den Beschwerdeführern geltend gemachte „erzwungene Einwilligung“ sah die DPC allerdings nicht als gegeben, da sich Meta Ireland nicht auf die Einwilligung der Nutzenden als rechtmäßige Grundlage für die Verarbeitung ihrer personenbezogenen Daten berufen habe, und vertrat den Standpunkt, dass sich Meta Ireland rechtmäßig auf die Rechtsgrundlage der Vertragserfüllung für die Verarbeitung der personenbezogenen Nutzerdaten im Zusammenhang mit der Erbringung seiner personalisierten Dienste (einschließlich personalisierter Werbung) berufen konnte.

Die betroffenen Aufsichtsbehörden stimmten nach Prüfung der vorgelegten Beschlussentwürfe dem DPC zwar in der Feststellung des Verstoßes gegen Transparenzverpflichtungen zu, erachteten aber die als Reaktion auf den Verstoß vorgeschlagene Geldbuße in ihrer Höhe für zu gering. Zudem machten viele betroffene Aufsichtsbehörden – auch deutsche Aufsichtsbehörden unter Federführung des HmbBfDI – Einwände in Bezug auf die Rechtsgrundlage der Vertragserfüllung geltend, die die DPC als rechtmäßig bewertet hatte. Die Zurverfügungstellung verhaltensbezogener Werbung im Zusammenhang mit den Facebook- und Instagram-Diensten sei nicht für die Erfüllung vertraglicher Verpflichtungen von Meta gegenüber den Nutzern von Facebook und Instagram erforderlich.

Die DPC schloss sich auch in diesen Verfahren den von den betroffenen Aufsichtsbehörden erhobenen Einsprüchen nicht an und legte, da kein Konsens erzielt werden konnte, beide Verfahren dem EDSA zur Entscheidung im Streitbeilegungsverfahren nach Art. 65 Abs. 1 Buchst. a DS-GVO vor.

In seinem verbindlichen Beschluss vom 5. Dezember 2022 schloss sich der EDSA vielen der von den betroffenen Aufsichtsbehörden vorgebrachten Einsprüchen an und bestätigte den Verstoß von Meta Ireland gegen Transparenzverpflichtungen. Der EDSA wies die DPC zudem an, die Geldbuße zu erhöhen. Auch in der Frage der Rechtsgrundlage folgte der EDSA den Einsprüchen und kam zu dem Schluss, dass sich Meta Ireland grundsätzlich nicht rechtmäßig auf die Rechtsgrundlage der „Vertragserfüllung“ für die Verarbeitung personenbezogener Daten zum Zweck der verhaltensbezogenen Werbung berufen kann.

Dem EDSA-Beschluss ist die DPC mit der nun erfolgten Feststellung der Datenschutzverstöße und der Erhöhung der Geldbußen nachgekommen.

5. Gerichts- und Bußgeldverfahren

Die DS-GVO führt zu einer zunehmenden Juridifizierung der Aufsichtstätigkeit (s. Kap. 1). Die Zahl der Gerichtsverfahren und der Bußgeldverfahren nimmt zu und diese Entwicklung hat auch verstärkt Auswirkungen auf die Arbeit der Aufsichtsbehörde. In der Bearbeitung von Beschwerden ist immer auch damit zu rechnen, dass der Beschwerdeführer oder der Verantwortliche je nach Ausgang des Verfahrens zum Prozessgegner der Aufsichtsbehörde wird. Dies führt zu einer Formalisierung der Aufsichtstätigkeit und einer zunehmenden Notwendigkeit, Verfahrensschritte zu dokumentieren – mit der entsprechenden Mehrarbeit in den Beschwerdeverfahren.

5.1
Vor Gericht und auf hoher See – Entwicklung der Gerichtsverfahren im Jahr 2022

Der Trend der letzten Berichtsjahre setzte sich im Jahr 2022 fort. Die Zahl der Gerichtsverfahren stieg weiter deutlich an. Viele Verfahren gingen in die zweite Instanz, so dass ich auch mehrfach Beteiligter an Berufungsverfahren vor dem Hessischen Verwaltungsgerichtshof (VGH) in Kassel bin. Zu verhandeln war auch über Verfassungsbeschwerden gegen § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) und das Analysesystem hessenDATA vor dem Bundesverfassungsgericht (BVerfG). Stellungnahmen waren in zwei weiteren Verfahren vor dem BVerfG und in drei Verfahren vor den EuGH abzugeben.

Im Berichtsjahr waren insgesamt 35 Gerichtsverfahren neu zu verzeichnen. Diese verteilen sich auf verschiedene Instanzen und Gerichte. Davon sind 18 am Verwaltungsgericht (VG) Wiesbaden, zehn Verfahren beim Hessischen Verwaltungsgerichtshof (VGH), drei Vorlageverfahren vor dem EuGH sowie drei Verfahren beim BVerfG, in denen ich zur Abgabe einer Stellungnahme aufgefordert war.

Gerichtsverfahren	Anzahl
Klagen gemäß Art. 78 Abs. 1 DS-GVO	13
Klagen gemäß Art. 78 Abs. 2 DS-GVO	4
EuGH-Vorabentscheidungsverfahren	3
Verfahren vor dem VGH in 2. Instanz	11
Verfahren vor dem BVerfG	3
Eilverfahren	1
Gesamt	**35**

Zu den Gerichtsverfahren aus dem Berichtsjahr kamen noch nicht abgeschlossene Verfahren aus den vorherigen Berichtsjahren. Die Zahl belief sich damit insgesamt auf 45 offene Gerichtsverfahren zum Ende des Berichtsjahres.

Der thematische Schwerpunkt der erstinstanzlichen Verfahren lag vor allem im Beschäftigtendatenschutz, in den Betroffenenrechten (Auskunft nach Art. 15 DS-GVO, Berichtigung nach Art. 16 DS-GVO, Löschung von Daten nach Art. 17 DS-GVO), bei Untätigkeitsklagen nach Art. 78 Abs. 2 DS-GVO, in der Datenübermittlung an den Auftragsverarbeiter, in der Offenlegung von Daten gegenüber einem Finanzdienstleister, in der Datenverarbeitung mittels privater Mobilgeräte im Rahmen einer Vertragsbeziehung und in der Videoüberwachung.

Der Blick über die Verwaltungsstreitverfahren offenbart, dass im Falle der Klageabweisung in erster Instanz, öfter als im vergangenen Jahr, die Zulassung der Berufung beantragt wurde.

Untätigkeitsklagen

Einen Schwerpunkt bei den Klageverfahren nehmen die Untätigkeitsklagen nach Art. 78 Abs. 2 Alt. 2 DS-GVO ein. Aufgrund der sehr hohen Zahl an Beschwerden in einzelnen Fachreferaten kam es immer wieder zu Verzögerungen in der Bearbeitung von einzelnen Beschwerden. Meine Mitarbeiterinnen und Mitarbeiter zeigten einen hohen Einsatz zur Bewältigung der Beschwerden. In einzelnen Fällen konnte dennoch die Dreimonatsfrist im Sinn des Art. 78 Abs. 2 Alt. 2 DS-GVO nicht eingehalten werden. Grundsätzlich besteht eine Pflicht zur Unterrichtung über den Verfahrensstand in dreimonatigen Abständen. Erfolgt diese Unterrichtung nicht, so kann mit dem Ablauf der drei Monate das Klagerecht wegen Untätigkeit auf dem Gerichtsweg geltend gemacht werden. Die Dreimonatsfrist ist eine starre Frist, die nicht verkürzt oder verlängert werden kann. Damit bleibt es mir auch verwehrt, mich unter Berufung auf sachliche Erwägungen, wie z. B. hohe Komplexität

des Falles, auf eine Verlängerung der Frist zu berufen. Es ist stark von der Personaldecke in bestimmten Referaten abhängig, wie hoch das Risiko der Untätigkeitsklage ist. In Art. 52 Abs. 4 DS-GVO wird auch aus diesem Grund ausdrücklich geregelt, dass jeder Mitgliedstaat sicherzustellen hat, dass jede Aufsichtsbehörde unter anderem mit den personellen Ressourcen ausgestattet ist, die sie benötigt, um ihre Aufgaben und Befugnisse wahrnehmen zu können. Ich hoffe, mit den zugewiesenen neuen Stellen im Jahr 2023 hier eine Verbesserung verzeichnen zu können.

Aus den Verwaltungsgerichtsverfahren möchte ich zwei Fälle herausgreifen.

GPS-Tracking in der Logistikbranche

Im Fall einer Anordnung nach Art. 58 Abs. 2 DS-GVO wegen rechtswidrigen Einsatzes eines Softwaretools zur Erhebung und Speicherung von Standortdaten der Fahrzeuge eines Logistikunternehmens wurden die Anordnungen meiner Behörde durch das VG Wiesbaden bestätigt und die Anfechtungsklage abgewiesen (Urteil vom 17. Januar 2022, Az.: 6 K 1164/21.WI). Die Klägerin hatte GPS-Systeme in Fahrzeuge ihrer Firmenflotte eingebaut. Die verwendete Software ermöglichte die Bestimmung des Live-Standortes von Fahrzeugen per GPS und die Speicherung der Standortdaten und maß den Benzinverbrauch. Zwar hatte die Klägerin nur die Fahrzeuge tracken lassen, aber so war auch der jeweilige Nutzer (Fahrer) über die Zuordnung zu dem zugeteilten Fahrzeug identifizierbar (vgl. VG Lüneburg, Teilurteil vom 19. März 2019 – 4 A 12719, juris Rn. 29). Die Klägerin wandte sich gegen vier Anordnungen meiner Behörde – aber ohne Erfolg. Das Gericht kam zu dem Ergebnis, dass eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten nicht einschlägig sei, so dass die Verarbeitung nicht rechtmäßig gewesen ist (Art. 5 Abs. 1 Buchst. a DS-GVO). Weder habe eine Einwilligung gem. Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO vorgelegen, noch sei die Verarbeitung wegen einer rechtlichen Verpflichtung gem. Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO erforderlich gewesen, noch war sie zur Wahrung des berechtigten Interesses der Klägerin gem. Art. 6 Abs. 1 UAbs.1 Buchst. f DS-GVO erforderlich. Der Verzicht auf Speicherung der Daten wurde im Sinn des Art. 58 Abs. 2 Buchst. d DS-GVO rechtmäßig angeordnet. Die Anordnung gem. Art. 58 Abs. 2 Buchst. g DS-GVO, die bislang für Zwecke des GPS-Tracking erhobenen Daten innerhalb von zwei Woche ab Bestandskraft des Bescheides zu löschen und die Löschung zu bestätigen, hielt stand. Die Anordnung der umfassenden Information der die Fahrzeuge führenden Fahrer nach Art. 58 Abs. 2 Buchst. c DS-GVO wurde ebenfalls gerichtlich bestätigt. Das Gericht hat zudem die Anordnung der

Vorlage eines aktualisierten Verarbeitungsverzeichnisses nach Art. 58 Abs. 1 Buchst. a DS-GVO für rechtmäßig erachtet.

Ärztliche Abrechnungsstelle – datenschutzkonform abgerechnet?

Das VG Wiesbaden stellte in einem weiteren Verfahren klar, dass das Verwaltungsstreitverfahren kein Ort für die Vorbereitung von Schadenersatzansprüchen nach Art. 82 DS-GVO ist (Urteil vom 19. September 2022, Az. 6 K 685/22.WI). Der Kläger hatte bei mir darüber Beschwerde eingereicht, dass eine privatärztliche Abrechnungsstelle eine unvollständige Auskunft erteilt habe. Die Prüfung ergab, dass keine Daten zu der Rechnung mehr gespeichert waren, weil die Einwilligung des Klägers gefehlt hatte. Dieser hatte die umgehende Löschung erbeten und die Rechnung war umgehend gelöscht worden. Darüber hinaus hatte der Kläger zudem ein Auskunftsverlangen an die privatärztliche Abrechnungsstelle gerichtet. Ich hatte nach Prüfung der Sachlage mit Bescheid dem Kläger mitgeteilt, dass kein Verstoß vorliege. Hiergegen erhob er eine statthafte Verpflichtungsklage. Diese erachtete das VG Wiesbaden jedoch für unzulässig, da die Klagebefugnis nach § 42 Abs. 2 VwGO fehlte, weil der Kläger keine Verletzung eines subjektiven Rechts vortragen konnte. Es fehlte auch an einer Rechtsgrundlage, auf die er eine reine Feststellungsbefugnis ohne Rechtsfolgen für den Verantwortlichen stützen könnte. Das Gericht stellte fest, dass es keine Aufgabe der Aufsichtsbehörde ist, zivilrechtliche Schadenersatzprozesse nach Art. 82 DS-GVO zu erleichtern und über den Umweg der Amtsermittlung Beweise für den Betroffenen zu sichern. Die Entscheidung ist nicht rechtskräftig. Der Kläger hat den Antrag auf Zulassung der Berufung gestellt.

Mündliche Verhandlung vor dem Bundesverfassungsgericht

Höhepunkt unter den Gerichtsverfahren im Berichtsjahr war meine Beteiligung als sachverständige Auskunftsperson in der mündlichen Verhandlung des BVerfG über Verfassungsbeschwerden zur automatisierte Datenauswertung durch die Polizei in Hessen und Hamburg (Az.: 1 BvR 1547/19) am 20. Dezember 2022. § 25a HSOG ermöglicht es der Hessischen Polizei, alle bei ihr gespeicherten Daten u. a. zur vorbeugenden Bekämpfung von schweren Straftaten zu analysieren. Seit 2018 kommt hierfür in Hessen die Analyse-Software Gotham der US-Firma Palantir zum Einsatz. Das auf hessische Verhältnisse angepasste Analyse-Tool wird in Hessen unter der Bezeichnung hessenDATA geführt (s. hierzu auch Kap. 6.1).

Auf die umfangreichen Fragen des Gerichts in der mündlichen Verhandlung habe ich sowohl Antworten zu der von meinen Mitarbeiterinnen und Mitarbeitern festgestellten Praxis des Einsatzes von hessenDATA gegeben

als auch datenschutzrechtliche Bewertungen abgegeben. Hinsichtlich der Praxis habe ich auf die problematische Reichweite des Analyse-Werkzeugs hingewiesen. Es greift u. a. auf alle Daten von Funkzellenabfragen zu, durch die alle Personen, die sich mit einem Mobilfunkgerät zu einer bestimmten Zeit in einem bestimmten räumlichen Bereich aufgehalten haben, erfasst werden. Es wertet auch alle Daten des polizeilichen Dokumentationssystems aus, auch wenn sie nichts mit schwerwiegenden Straftaten zu tun haben. In diesem Dokumentationssystem werden alle Vorkommnisse, mit denen die Polizei zu tun hat, dokumentiert, von Ermittlungen zu Straftaten, über Zeugenaussagen, Verkehrsunfällen, Verlustanzeigen bis hin zu Nachbarstreitigkeiten und unbelegten Verdächtigungen. Dadurch besteht das Risiko, dass viele Personen in polizeiliche Ermittlungen einbezogen werden, die dort nicht hingehören. Zugriff auf diese Analyse-Software haben in Hessen über 2.000 Kriminalbeamte, die mit ihr im Jahr 2021 über 14.000 Ermittlungen durchgeführt haben.

Verfassungsrechtlich problematisch ist unter anderem, dass die gefahrenabwehrrechtliche Vorschrift des § 25a HSOG sehr wenig bestimmt ist. Wenn der Anwendungsbereich so weit formuliert ist, ist es schwer, in der Praxis Grenzen einzuziehen. Aufgrund ihrer Eingriffstiefe darf die Analyse-Software nicht zum Standardmittel für die polizeiliche Arbeit werden, sondern ist für sehr schwerwiegende Fälle vorzubehalten.

In dem Verfahren habe ich auch auf ein weiteres Problem im Zusammenhang mit dem Thema der Zweckbindung hingewiesen. Bei der Analyse der bei der Polizei gespeicherten Daten mit hessenDATA werden große Mengen an Daten von „Unbeteiligten“ einbezogen, die davon nichts erfahren und die keine Chance haben, ihre Lebensführung so einzurichten, dass sie nicht erfasst werden. Mit hessenDATA werden alle Daten bei der Polizei Bestandteile eines einheitlichen großen Datenpools zur Analyse für weitreichende künftige Ermittlungszwecke.

Zum Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 und den Folgen für die hessische Praxis werde ich im nächsten Tätigkeitsbericht nähere Ausführungen machen

5.2
Überblick über die geführten Bußgeldverfahren

Im Jahr 2022 waren die Verstöße der verantwortlichen Stellen aus den unterschiedlichen Branchen und Bereichen erneut vielfältig. Schwerpunkte bildeten im Berichtsjahr die Verfahren gegen Corona-Testzentren sowie Mitarbeiterexzesse im öffentlichen und nichtöffentlichen Bereich.

Bußgeldverfahren in Zahlen

Im Berichtszeitraum habe ich insgesamt 53 neue Bußgeldverfahren eingeleitet. Während die Zahl der neu anhängigen Verfahren im Vergleich zum Vorjahr zurückging, stieg die Zahl der sanktionierten Verstöße an. Es wurden insgesamt 113 Geldbußen erlassen, die sich sowohl gegen natürliche Personen als auch gegen Unternehmen aus verschiedenen Bereichen richteten. Die Gesamtsumme der festgesetzten Geldbußen lag im Berichtszeitraum bei 44.350 Euro.

Im Berichtszeitraum waren die Auswirkungen der Pandemie weiterhin spürbar. Ein Schwerpunkt der Bearbeitung in der Bußgeldstelle lag in der Ahndung von Verstößen durch Betreiber von Corona-Testzentren. Darüber hinaus wurden Fälle des Mitarbeiterexzesses sowohl im öffentlichen als auch im nichtöffentlichen Bereich weiterhin konsequent verfolgt.

Verstöße durch Betreiber von Testzentren

Durch die anhaltende Corona-Pandemie waren im Berichtsjahr der Gesundheitsbereich und insbesondere die Betreiber von Corona-Testzentren mehr in den Fokus gerückt. Hier musste ich nach dem Abschluss von vorausgegangenen Aufsichtsverfahren mehrere Verfahren wegen Ordnungswidrigkeiten einleiten (s. auch Kap. 15.3). Dies erfolgte vorwiegend wegen Verstößen gegen die Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 DS-GVO), die Rechtmäßigkeit (Art. 6 DS-GVO) und die Sicherheit (Art. 32 DS-GVO) der Verarbeitung. Mehrere Verfahren konnten bereits rechtskräftig abgeschlossen werden.

In einem Fall richtete sich das Bußgeldverfahren gegen ein Unternehmen, das mehrere Testcenter überwiegend im Rhein-Main-Gebiet betreibt. Gegenstand des Verfahrens war der Versand einer E-Mail im offenen Verteiler an ca. 100 Personen, wobei keine sensiblen Daten betroffen waren. Obwohl die Verantwortliche noch am selben Tag von einem E-Mail-Empfänger auf den Vorfall hingewiesen worden war, sah diese keinerlei Veranlassung, weitere Maßnahmen einzuleiten. Durch die unrechtmäßige Offenlegung der zahlreichen E-Mail-Adressen verstieß das Unternehmen gegen Art. 6 Abs. 1 DS-GVO. Darüber hinaus verletzte es die Dokumentationspflicht bei einer Datenschutzverletzung gem. Art. 33 Abs. 5 in Verbindung mit Art. 33 Abs. 1 DS-GVO.

Aufgrund der vorgenommenen Schätzung des Vorjahresumsatzes des Unternehmens und unter Berücksichtigung der Zumessungskriterien aus Art. 83 Abs. 2 DS-GVO wurden Geldbußen in Höhe von 10.000 Euro für den ersten und 6.400 Euro für den zweiten Verstoß festgesetzt. Wesentlich

für die Entscheidung war unter anderem die konstruktive Zusammenarbeit mit der Aufsichtsbehörde und die zum Ausdruck gebrachte Einsicht des Unternehmens. Darüber hinaus wurden die Bestellung eines Datenschutzbeauftragten im Nachgang des Vorfalls und die Tatsache, dass zum ersten Mal datenschutzrechtliche Verstöße gegen das Unternehmen bekannt wurden, im Rahmen der Geldbußenzumessung mildernd berücksichtigt. Somit waren die einzelnen Geldbußen in der gewählten Höhe im Gesamtergebnis entsprechend den Anforderungen der DS-GVO wirksam, verhältnismäßig und abschreckend. Das Unternehmen, das im Rahmen des Ordnungswidrigkeitenverfahrens anwaltlich vertreten wurde, akzeptierte die Entscheidung und legte keinen Einspruch ein.

In einem weiteren hessischen Testzentrum führte Unachtsamkeit zu einem Fehler: Eine Beschäftigte nahm aus mangelnder Sorgfalt ein Klebeetikett aus dem Müll, schrieb handschriftlich die E-Mail-Adresse des Testzentrums darauf und klebte den Zettel von außen sichtbar an die Plexiglasscheibe im Testzentrum. Unglücklicherweise waren die personenbezogenen Daten einer Kundin, wie Name, Geburtstag, Datum und Uhrzeit des letzten Tests sowie Test-ID, auf dem Etikett aufgedruckt. Der Zettel wurde erst am Folgetag von der Scheibe entfernt. Die Daten waren somit für eine Dauer von ca. 24 Stunden für Dritte einsehbar. Das Testzentrum wandte im Laufe des Verfahrens ein, dass die involvierte Mitarbeiterin nicht wahrgenommen habe, dass sich auf dem Etikettenbogen noch Kundendaten befunden haben. Sie habe den Zettel für ein leeres Klebeetikett gehalten und ihn daher mit der E-Mail-Adresse des Testzentrums an die Scheibe gehängt.

Durch die Offenbarung der genannten Informationen machte der Verantwortliche die Daten seiner Kundin einem unbegrenzten Adressatenkreis zugänglich und verstieß damit gegen mehrere Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 83 Abs. 5 Buchst. a in Verbindung mit Art. 5 Abs. 1 Buchst. a und f sowie Art. 6 Abs. 1 DS-GVO. Die Handlung wurde mit einer Geldbuße in Höhe von 1.800 Euro sanktioniert. Auch in diesem Fall zeigte sich der Betreiber des Testzentrums einsichtig und zahlte die Geldbuße.

Mitarbeiterexzesse

Im Bereich der Polizei habe ich im Berichtsjahr acht Verfahren mit einem Bußgeldbescheid abgeschlossen. Die zugrundeliegenden Handlungen von Beschäftigten der Polizei bezogen sich auf verschiedenste Sachverhalte, fanden jedoch alle aus privaten Motiven statt. Dabei wurden unter anderem Datenabfragen über Ex-Partnerinnen und Ex-Partner, Nachbarn, Familienangehörige, Bekannte, Kolleginnen und Kollegen sowie Führungskräfte aus polizeilichen und der Polizei zur Verfügung stehenden Systemen insbesondere

aus Neugier, elterlicher Sorge oder Liebeskummer vorgenommen. Dagegen habe ich gemäß § 170 Abs. 2 StPO in Verbindung mit § 46 Abs. 1 OWiG ein Verfahren aus rechtlichen sowie ein weiteres Verfahren aus tatsächlichen Gründen eingestellt.

In einem Verfahren gegen einen Polizeibeamten wurde ein Bescheid mit Geldbußen in Höhe von insgesamt 7.380 Euro zuzüglich Auslagen erlassen. Der Polizeibeamte hatte verschiedene polizeiliche oder der Polizei zur Verfügung stehende Datenbanken für Abfragen zu eigenen Zwecken genutzt. Außergewöhnlich war das Ausmaß der unzulässigen Datenabfragen: Der Polizeibeamte hatte über drei Jahre hinweg mehrere hundert Abfragen getätigt. Die Entscheidung ist nicht rechtskräftig.

In einem anderen Fall fragte ein Polizeibeamter eine Kollegin mehrmals in EWO ab. Zugunsten dieser Kollegin war eine Auskunftssperre im Melderegister gemäß § 51 BMG eingetragen. Durch die Eingabe verschiedener Abfrageparameter im System wurden dem Beamten jedoch über 300 Treffer angezeigt und somit umfangreiche Daten Dritter beauskunftet. Gegen den Polizisten habe ich eine Geldbuße in Höhe von 800 Euro verhängt. Der Bußgeldbescheid ist bereits rechtskräftig.

Mehrere EWO-Abfragen über die neue Lebensgefährtin ihres Ex-Mannes durch eine Beschäftigte der Polizei waren Gegenstand eines weiteren Bußgeldverfahrens. Unter anderem wollte die Polizistin durch die Abfragen in Erfahrung bringen, wo sich ihr Ex-Ehemann mit ihren gemeinsamen Kindern aufhält. Das Verfahren endete mit einem Bescheid zu einem Bußgeld über 300 Euro, der nicht angegriffen und bezahlt wurde.

Neben den oben beschriebenen Vorgängen verfolgte ich im Berichtsjahr auch mehrere Fälle des Mitarbeiterexzesses im nicht öffentlichen Bereich. In einem Verfahren war es aufgrund der konkreten Anhaltspunkte für eine Straftat im Sinn des § 42 BDSG geboten, einen Strafantrag bei der zuständigen Staatsanwaltschaft zu stellen. Auslöser des Verfahrens war eine Meldung von Verletzungen des Schutzes personenbezogener Daten eines Unternehmens, durch die ich über einen datenschutzrechtlichen Verstoß eines ehemaligen Mitarbeiters informiert wurde. Der ausgeschiedene Mitarbeiter bewarb in einer E-Mail seine Tätigkeit für ein neues Unternehmen, das im Wettbewerb zu seinem früheren Arbeitgeber steht. Dabei verwendete er 145 E-Mail-Adressen aus dem Kundenbestand seines ehemaligen Arbeitgebers. Die Unternehmensleitung ging davon aus, dass der Beschäftigte den Zugang zu den betroffenen E-Mail-Adressen, die im Unternehmen nicht allgemein zugänglich sind, missbraucht, diese auf einem externen Speicher gespeichert und anschließend für eigene Zwecke verwendet hatte.

Da der Mitarbeiter personenbezogene Daten aus dem Geschäftsbereich seines ehemaligen Arbeitgebers zum Zwecke der Kundenakquise für seinen neuen Arbeitgeber oder sich selbst entwendet hatte, bestanden unter anderem Anhaltspunkte dafür, dass der Mitarbeiter in Bereicherungsabsicht gehandelt hatte. Es bestand daher der Verdacht eines Verstoßes gegen § 42 Abs. 2 BDSG. Gemäß § 42 Abs. 3 BDSG ist die Tat nur auf Antrag verfolgbar.

Die zuständige Staatsanwaltschaft sah im Ermittlungsverfahren gemäß § 153 Abs. 1 StPO aufgrund der geringen Schuld des Täters und des mangelnden öffentlichen Interesses von der Verfolgung ab und gab das Verfahren zur Verfolgung eventueller Ordnungswidrigkeiten in eigener Zuständigkeit an meine Behörde ab. Das eingeleitete Bußgeldverfahren ist noch nicht abgeschlossen.

Verstöße durch Adresshändlerin

Bei einer anlasslosen Prüfung einer professionellen Adresshändlerin in Form einer kleinen Kapitalgesellschaft wurden mehrere datenschutzrechtliche Probleme festgestellt. Zum einen waren die Datenschutzhinweise der Betroffenen nicht an die Anforderungen der DS-GVO angepasst und somit veraltet. Zum anderen war das auf der Website eingebettete Kontaktformular unverschlüsselt. Es lagen somit Verstöße gegen Art. 13 DS-GVO sowie Art. 5 Abs. 1 Buchst. f in Verbindung mit Art. 32 DS-GVO vor.

Während das Unternehmen die Datenschutzhinweise rund vier Wochen nach Einschaltung meiner Behörde an die aktuellen Regelungen angepasst hatte, waren im Aufsichtsverfahren für die Durchsetzung der Rechtsordnung in Bezug auf die TLS-Verschlüsselung des Kontaktformulars gemäß den Vorgaben des Art. 32 DS-GVO mehrere Zwangsgeldandrohungen und eine Festsetzung des Zwangsgeldes in Höhe von 2.500 Euro notwendig. Parallel hatte ich ein Verfahren wegen Ordnungswidrigkeiten eingeleitet. Erst als die Vollstreckung des festgesetzten Zwangsgeldes unmittelbar bevorstand, sah sich das Unternehmen veranlasst, die notwendigen Schritte in die Wege zu leiten, um Übermittlungen des Kontaktformulars zu verschlüsseln.

Das Verfahren wegen Ordnungswidrigkeiten habe ich mit einem Bußgeldbescheid über insgesamt 7.800 Euro abgeschlossen. Obwohl die Verstöße eindeutig belegt werden konnten, legte das Unternehmen gegen den Bescheid erst deutlich nach Ablauf der Frist Einspruch ein und stellte einen Antrag auf Wiedereinsetzung in den vorigen Stand. Begründet wurde dies damit, dass die Geschäftsführerin urlaubsbedingt ortsabwesend war und der von ihr beauftragte Vertreter sie nicht rechtzeitig über den zugegangenen Bußgeldbescheid informiert hatte. Der Vertreter soll ihr die gesamte Post übergeben haben, lediglich der mittels Postzustellungsurkunde im gelben Umschlag zugestellte Bußgeldbescheid soll dem Vertreter hinter den Bei-

fahrersitz des Autos gerutscht sein. Dies sei erst mehrere Wochen später festgestellt worden.

Ich verwarf den Antrag auf Wiedereinsetzung in den vorigen Stand als unbegründet und den Einspruch folglich als unzulässig. Aus meiner Sicht konnte ein Verschulden der Geschäftsführerin an der Fristversäumung nicht ausgeräumt werden. Der Vertreter wurde von der Geschäftsführerin weder entsprechend angewiesen oder geschult noch erhielt er konkrete Anweisungen, wie mit behördlichen oder gerichtlichen fristauslösenden Zustellungen zu verfahren war.

Gegen den Verwerfungsbescheid stellte die Geschäftsführerin Antrag auf gerichtliche Entscheidung gemäß § 69 Abs. 1 S. 1 und S. 2 in Verbindung mit § 62 OWiG. Meine Behörde half dem Antrag nicht ab und legte den Fall dem Amtsgericht Wiesbaden zur Entscheidung vor. Das Amtsgericht schloss sich meiner Rechtsauffassung an und bestätigte meinen Verwerfungsbescheid vollumfänglich als rechtmäßig. Nach 62 Abs. 2 S. 3 OWiG ist diese Entscheidung des Gerichts unanfechtbar. Die Betroffene legte dennoch dagegen Beschwerde ein. Diese wurde dem Landgericht Wiesbaden vorgelegt und von diesem als unzulässig abgewiesen.

Das Bußgeldverfahren ist damit rechtskräftig abgeschlossen. Die Geldbuße wird im Rahmen der Zwangsvollstreckung gegen das Unternehmen beigetrieben.

5.3
EU-Leitlinien für die Berechnung von Geldbußen

Um die Praxis zur Berechnung von Geldbußen in der EU und im EWR zu vereinheitlichen, arbeitet der EDSA an Leitlinien für die Berechnung von Geldbußen. Hierzu hat der EDSA einen ersten Entwurf vorgelegt und ein Konsultationsverfahren durchgeführt. Diese Leitlinien werden große Bedeutung für die künftige Verhängung von Geldbußen haben.

Im Berichtsjahr hat der EDSA am 12. Mai 2022 den lang erwarteten Vorschlag für Leitlinien zur Berechnung von Geldbußen unter der DS-GVO (Guidelines 04/2022 on the calculation of adminstrative fines under the GDPR) angenommen und veröffentlicht (https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf). Vom 16. Mai bis 27. Juni 2022 wurde dann eine öffentliche Konsultation zu dem Entwurf durchgeführt. Das Feedback auf die öffentliche Konsultation wurde auf der Homepage des EDSA veröffentlicht.

Die Leitlinien ergänzen die zuvor erlassenen Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinn der DS-GVO (WP 253), die sich auf die Umstände für die Verhängung einer Geldbuße konzentrieren. Ziel der neuen Leitlinien zur Berechnung von Geldbußen ist es, eine europaweite Harmonisierung ihrer Festsetzung anzustreben. Harmonisierte Ausgangspunkte sollen eine gemeinsame Ausrichtung sein, auf deren Basis die Berechnung von Geldbußen im Einzelfall erfolgen kann. Damit kommt der EDSA seinem gesetzlichen Auftrag aus Art. 70 Abs. 1 Buchst. k DS-GVO nach, nach dem er einheitliche Leitlinien für die Aufsichtsbehörden in Bezug auf die Anwendung von Maßnahmen nach Art. 58 Abs. 1, 2 und 3 DS-GVO und die Festsetzung von Geldbußen nach Art. 83 DS-GVO zu erlassen hat. Diese Leitlinien gehen den nationalen Leitlinien der DSK vor. Sie betreffen sowohl grenzüberschreitende als auch nicht grenzüberschreitende Fälle.

Die Bewertung des Einzelfalls entfällt aber nicht. Entsprechend Art. 83 Abs. 1 DS-GVO ist sicherzustellen, dass jede einzelne Geldbuße wirksam, verhältnismäßig und abschreckend ist.

Die erarbeitete Berechnungsmethode der Höhe der Geldbuße teilt sich in fünf Schritte auf, die sich an Art. 83 DS-GVO „entlanghangeln“:

Schritt 1

In einem ersten Schritt sind die Verarbeitungsvorgänge des Einzelfalls zu ermitteln und die Anwendung von Art. 83 Abs. 3 DS-GVO zu bewerten (Kap. 3 der Leitlinie). Es ist wichtig, zunächst zu prüfen, auf welchem Verhalten (tatsächliche Umstände des Verhaltens) und welchen Verstößen (abstrakte rechtliche Beschreibungen dessen, was sanktionierbar ist) der Sachverhalt beruht. Zunächst ist zu klären, ob der Fall aus einem sanktionsfähigen Verhalten besteht oder ob es sich um getrennte sanktionsfähige Verhaltensweisen handelt. Geben die Verhaltensweisen Anlass zu einer Einordnung von einem Verstoß und liegt keine Übereinstimmung vor, so ist das Anlass, für jede Zuwiderhandlung eine Geldbuße bis zur gesetzlichen Höchstgrenze der Zuwiderhandlung zu verhängen. Geben das sanktionsfähige Handeln oder die getrennt sanktionsfähigen Verhaltensweisen Anlass zur Ahndung von mehr als einem Verstoß, dann ist zu prüfen, ob sich die Verstöße einander ausschließen oder ob die Verstöße nebeneinander gelten. Hier kommt es also auf die Beurteilung nach den Grundsätzen der Spezialität, der Subsidiarität und der Konsumtion an.

Schritt 2

Darauf folgt die Festsetzung des Ausgangspunkts für die weitere Berechnung der Höhe des Bußgeldes (Kap. 4 der Leitlinie). Der EDSA ist der Auffassung, dass die Berechnung der Geldbuße von einem harmonisierten Ausgangspunkt beginnen sollte. Der Ausgangspunkt wird durch drei Elemente definiert:

a. die Einstufung des Verstoßes gem. Art. 83 Abs. 4 bis 6 DS-GVO,
b. die Schwere des Verstoßes gem. Art. 83 Abs. 2 Buchst. a, b und g DS-GVO,
c. der Umsatz des Unternehmens als ein wichtiges Element im Hinblick auf die Verhängung einer wirksamen, abschreckenden und verhältnismäßigen Geldbuße im Sinn des Art. 83 Abs. 1 DS-GVO.

Schritt 3

In einem dritten Schritt werden die strafverschärfenden und -mildernden Umstände im Zusammenhang mit dem früheren oder gegenwärtigen Verhalten des Verantwortlichen und die entsprechende Erhöhung oder Verringerung der Geldbuße berücksichtigt (Kap. 5 der Leitlinie). Nach der Bewertung der Art, Schwere und der Dauer des Verstoßes sowie ihres vorsätzlichen oder fahrlässigen Charakters und der Kategorien betroffener Daten in Schritt 2 sind nun die erschwerenden oder mildernden Faktoren gemäß Art. 83 Abs. 2 DS-GVO zu berücksichtigen.

Schritt 4

Im vierten Schritt werden die maßgeblichen gesetzlichen Höchstbeträge für die Verarbeitungsvorgänge ermittelt. Die in früheren oder nächsten Schritten vorgenommenen Berechnungen dürfen diesen Höchstbetrag nicht überschreiten (Kap. 6 der Leitlinie). Die DS-GVO folgt mit diesen Höchstbeträgen der allgemeinen Tradition des Unionsrechts zu Sanktionen. Die Beträge in Art. 83 Abs. 4 bis 6 DS-GVO stellen gesetzliche Höchstbeträge dar und verbieten es somit den Aufsichtsbehörden, Geldbußen zu verhängen, die im Endergebnis die geltenden Höchstbeträge überschreiten. Die Höchstbeträge unterscheiden sich in statische Höchstbeträge und dynamische Höchstbeträge. Nach Art. 83 Abs. 4 DS-GVO können Geldbußen bis zu einer Höhe von bis zu 10 Millionen Euro wegen Verletzung der in Art 83 Abs. 4 DS-GVO genannten Verpflichtungen verhängt werden. Dahingegen sieht Art. 83 Abs. 5 und 6 DS-GVO bei Verstößen gegen die dort genannten Verpflichtungen Geldbußen bis zu einer Höhe von 20 Millionen Euro vor. Im Fall eines Unternehmens kann sich die Spanne der Geldbuße in Richtung eines umsatzbasierten Höchstbetrages verschieben. Dieser umsatzbasierte Höchstbetrag ist dynamisch und individualisiert auf das jeweilige Unternehmen

ausgerichtet, um die Grundsätze der Wirksamkeit, Verhältnismäßigkeit und Abschreckung aus Art. 83 Abs. 1 DS-GVO zu erhalten. In diesem Kontext ist es wichtig zu verstehen, wie der Begriff „Unternehmen“ im Sinn des Art. 83 DS-GVO zu verstehen ist. Erwägungsgrund 150 DS-GVO orientiert sich am Begriff des Unternehmens nach Art. 101 und 102 AEUV. Demnach wird ein sog. funktionaler Unternehmensbegriff zugrunde gelegt, der dem deutschen Ordnungswidrigkeitenrecht fremd ist. Dieses baut auf das sog. Rechtsträgerprinzip auf. Nachdem das Landgericht Bonn, in seiner Entscheidung vom 11. November 2020 (Az.: 29 OWi 430 Js-OWi 366/20-1/20) zugunsten des europäischen Ansatzes entschieden hatte, hat das KG Berlin am 6. Dezember 2021 (Az.:3 Ws 250/21 – 161 AR 84/21) dem EuGH in Sachen Deutsche Wohnen diese Frage zur Entscheidung vorgelegt. Eine Entscheidung des EuGH (C-807/21) wird hierzu mit großer Spannung erwartet.

Schritt 5

Im fünften und letzten Schritt ist zu prüfen, ob der berechnete Endbetrag den Anforderungen an Wirksamkeit, Verhältnismäßigkeit und Abschreckung aus Art. 83 Abs. 1 DS-GVO entspricht. Die Geldbuße kann in diesem Schritt ggf. im Hinblick auf Art. 83 Ab. 1 DS-GVO entsprechend angepasst werden, ohne jedoch den maßgeblichen gesetzlichen Höchstbetrag zu überschreiten (Kap. 7 der Leitlinie). Alles was über diesen Maximalbetrag hinausgeht, wird gekappt.

In den fünf Schritten ist jederzeit zu berücksichtigen, dass die Berechnung einer Geldbuße keine bloße mathematische Übung ist. Vielmehr sind die Umstände des konkreten Einzelfalls die bestimmenden Faktoren, die zum Endbetrag führen.

Wenn auch die Leitlinien aufgrund ihrer Struktur den Anschein erwecken könnten, die Berechnung der Geldbußen sei rein mathematisch, soll die Berechnung von Geldbußen keine mathematische Übung sein. Daher schlagen grundsätzlich auch Ansätze, Bußgeldrechner zu programmieren, im Ergebnis fehl.

Ausblick

Im nächsten Schritt ist es nun am EDSA und der zuständigen Arbeitsgruppe, die Rückmeldungen aus der Konsultationsphase in die Leitlinien aufzunehmen. Diese Arbeit wurde bereits aufgenommen. Hessen ist neben dem Bund und Berlin an dieser Arbeitsgruppe beteiligt.

Ob die Bußgeldleitlinien des EDSA zu wesentlich höheren Geldbußen führen, bleibt abzuwarten. Denn es findet Art. 83 Abs. 1 DS-GVO als Korrektiv Anwendung, nach dem die Geldbuße wirksam, verhältnismäßig und abschreckend sein soll. Richtig ist sicherlich, dass die Geldbußen schon heute deutlich höher sind, als sie es unter dem BDSG waren, und dadurch bei den Amts- und Landgerichten zu Irritationen führen. Weil die nationale gerichtliche Bußgeldpraxis diese hohen Beträge nicht kennt, reagieren die Gerichte zunächst einmal eher zurüchaltend. Dabei ergibt sich bereits aus den Geldbußenrahmen, dass die Geldbußen auf andere Höhen ausgelegt sind. Auch hier wird sich zunächst erst einmal eine Praxis entwickeln müssen. Das bedingt aber auch, dass Geldbußenverfahren vor den Gerichten landen.

6. Polizei, Verfassungsschutz und Justiz

Polizei, Verfassungsschutz und Justizbehörden haben weitreichende Befugnisse zur Verarbeitung personenbezogener Daten, die zu tiefen Eingriffen in die informationelle Selbstbestimmung der betroffenen Personen führen können. Diese Befugnisse sind jedoch gerade deswegen immer an bestimmte gesetzliche Voraussetzungen gekoppelt. Zum Schutz des Grundrechts auf informationelle Selbstbestimmung ist es daher wichtig, dass diese Befugnisse, ihre Voraussetzungen und ihre Grenzen verhältnismäßig sind und hinsichtlich ihrer Einhaltung überwacht werden. Die Verhältnismäßigkeit der gesetzlichen Befugnisse war im Berichtszeitraum Gegenstand von Verfassungsbeschwerden gegen die Befugnis in § 25a HSOG, die vorhandenen Daten in Polizeisammlungen mit Hilfe von Analyse-Software auszuwerten (Kap. 6.1), und von parlamentarischen Anhörungen zur Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (Kap. 6.2). Die Einhaltung der Voraussetzungen und Grenzen dieser Befugnisse war Gegenstand von Prüfungen beim Landesamt für Verfassungsschutz (Kap. 6.3), bei Polizeibehörden (Kap. 6.4) und bei Staatsanwaltschaften (Kap. 6.5). Schwierige Abgrenzungen der Befugnisse nach Versammlungsrecht und Strafverfolgungsrecht zeigten sich bei „Spaziergängen" von Corona-Leugnern (Kap. 6.6).

6.1 HessenDATA vor dem Bundesverfassungsgericht

Aufgrund mehrerer Verfassungsbeschwerden prüfte das BVerfG u. a. die Verfassungsmäßigkeit des § 25a des Hessischen Sicherheits- und Ordnungsgesetzes (HSOG), der die automatisierte Datenauswertung durch die Polizei in Hessen erlaubt. In diesem Verfahren hat mich das Gericht um eine schriftliche Stellungnahme gebeten und zur mündlichen Verhandlung am 20. Dezember 2022 (s. hierzu Kap. 5.1) geladen.

Im Verfahren um die Verfassungsmäßigkeit der automatisierten Datenauswertung durch die Polizei in Hessen und Hamburg (Aktenzeichen: 1 BvR 1547/19, 1 BvR 2634/20) legte ich dem BVerfG eine Stellungnahme zu meinen Erfahrungen mit der Anwendung des § 25a HSOG und meiner verfassungsrechtlichen Bewertung vor. Diese Vorschrift ermöglicht es der Hessischen Polizei, die bei ihr gespeicherten personenbezogenen Daten auch zur vorbeugenden Bekämpfung von schweren Straftaten zu analysieren. In Hessen kommt hierfür seit 2018 die Analyse-Software Gotham der US-Firma Palantir zum Einsatz. Das auf hessische Verhältnisse angepasste Analyse-Tool trägt die Bezeichnung hessenDATA.

§ 25a HSOG

(1) Die Polizeibehörden können in begründeten Einzelfällen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten zur vorbeugenden Bekämpfung von in § 100a Abs. 2 der Strafprozessordnung genannten Straftaten oder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind.

(2) Im Rahmen der Weiterverarbeitung nach Abs. 1 können insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(3) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten. Die oder der Hessische Datenschutzbeauftragte ist vor der Einrichtung oder wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen.

Im Kern habe ich mich in meiner Stellungnahme zum Gefahrbegriff und dem in der Vorschrift verwendeten Begriff des „begründeten Einzelfalls“, zur erhöhten Eingriffsqualität bestimmter Datenquellen und der Zweckbindung wie bei Daten aus dem Vorgangsbearbeitungssystem und Daten aus Funkzellenabfragen, den Zugriffsmöglichkeiten und Nutzerzahlen im Rahmen der Verhältnismäßigkeit, der Ausgestaltung der Betroffenenrechte und den verfahrensbegleitenden Schutzmaßnahmen geäußert.

Verfassungsrechtlich problematisch ist zunächst, dass die gefahrenabwehrrechtliche Vorschrift des § 25a HSOG hinsichtlich der Eingriffsschwellen nicht bestimmt genug ist. Die Ausgestaltung des Anwendungsbereichs zur vorbeugenden Bekämpfung von in § 100a StPO genannten Straftaten reicht derart weit in den Gefahrvorfeldbereich hinein, dass es schwer ist, in der Praxis Grenzen einzuziehen, die dem Eingriffsgewicht der Maßnahme ausreichend Rechnung tragen und die Gefahrenabwehr von der Strafverfolgung abgrenzen. Für Sachverhalte mit einer hinreichend konkretisierten Gefahr für gewichtige Rechtsgüter und im Bereich der schweren Kriminalität mag der Einsatz der Analyse-Software vertretbar sein, aber sie darf nicht zum Standardmittel für die polizeiliche Arbeit werden.

Des Weiteren macht § 25a Abs. 1 HSOG in Bezug auf den „begründeten Einzelfall“ keinerlei Vorgaben, wie diese Formulierung in der Praxis zu verstehen ist. Jedenfalls ist es unabdingbar, dass die Begründung für die konkrete Anwendung der Datenanalyse mit hessenDATA in jedem Einzelfall ausreichend dokumentiert ist, um sie nachprüfen zu können.

Im Hinblick auf die Datenquellen gibt der Zwischenbericht des Untersuchungsausschusses des Hessischen Landtags (Hessischer Landtag: Zwischenbericht des Untersuchungsausschusses 19/3 zu Drucksache 19/6574, LT-Drs. 19/6864, S. 18f.) einen Überblick über die in hessenDATA aktuell einbezogenen Datenquellen, wobei Daten aus sieben verschiedenen Datenquellen einfließen können. Dazu gehören die drei hessischen polizeilichen Datenbanken POLAS, Crime (ST) und ComVor, Daten aus der hessischen Anlage für Telekommunikationsüberwachung (TKÜ) nach § 100a StPO und der bundesweiten Schnittstelle für Verkehrs- und Verbindungsdaten der TKÜ-Betreiber nach § 100g StPO, forensische Extrakte (aus IT-Asservaten extrahierte Kontakt- und Verbindungslisten), Fernschreiben und manuell importierte Daten aus öffentlich zugänglichen sozialen Netzwerken. Alle von der Polizei in die Datenanalyse einbezogenen Datenquellen und die darin gespeicherten Daten werden durch die Analyse-Software zu Bestandteilen eines virtuellen Datenpools zur Analyse für weitreichende künftige Ermittlungszwecke.

Im polizeilichen Vorgangsbearbeitungssystem ComVor werden alle Vorkommnisse, mit denen die Polizei zu tun hat, dokumentiert, von Ermittlungen zu Straftaten, über Zeugenaussagen, Verkehrsunfällen, Verlustanzeigen bis hin zu Nachbarstreitigkeiten und unbelegten Verdächtigungen. Demzufolge können mit hessenDATA personenbezogene Daten jeglicher Art aus ComVor ausgewertet und gem. § 20 Abs. 9 HSOG für die Datenanalyse nach § 25a HSOG der Grundsatz der strengen Zweckbindung für Daten der Vorgangsverwaltung durchbrochen werden.

§ 20 HSOG

(…)

(9) Die Gefahrenabwehr- und die Polizeibehörden können zur Vorgangsverwaltung oder zur befristeten Dokumentation behördlichen Handelns personenbezogene Daten ausschließlich zu diesem Zweck oder zu dem in Abs. 10 Satz 1 genannten Zweck weiterverarbeiten. Abs. 1 bis 7 finden insoweit keine Anwendung. Die personenbezogenen Daten nach Satz 1 können auch zu den in den §§ 13a, 13b und 25a genannten Zwecken weiterverarbeitet werden."

(…)

Problematisch ist zudem die Reichweite des Analyse-Werkzeugs beim Zugriff von Daten aus Funkzellenabfragen, wodurch personenbezogene Daten aller Personen, die sich mit einem mobilen Endgerät zu einer bestimmten Zeit in einem bestimmten räumlichen Bereich aufgehalten haben, erfasst werden. Bei der Analyse der bei der Polizei gespeicherten Daten mit hessenDATA werden somit auch große Mengen an Daten von „unbeteiligten" Personen

einbezogen, die davon nichts erfahren und die keine Chance haben, ihre Lebensführung so einzurichten, dass sie nicht erfasst werden. Eine Weiterverarbeitung solcher Daten nach § 25a HSOG ist in der Norm selbst an keine speziellen Voraussetzungen geknüpft.

Aus dem Wortlaut des § 25a HSOG ergibt sich keine Eingrenzung der Zugriffsmöglichkeiten und Nutzung von hessenDATA, so dass sich die Frage nach der Verhältnismäßigkeit stellt. Zugriff auf diese Analyse-Software haben derzeit in Hessen über 2.000 Kriminalbeamte, die mit ihr im Jahr 2021 über 14.000 Ermittlungen durchgeführt haben. Die Eingriffstiefe einer Datenanalyse, die Komplexität der Recherchetätigkeit und die Sensibilität der gewonnenen Analyseergebnisse machen es erforderlich, die tatsächlichen Zugriffe und Nutzer einer solchen Anwendung auf das absolut notwendige Maß zu beschränken.

Des Weiteren habe ich in meiner schriftlichen Stellungnahme die unzureichende gesetzliche Verankerung der Betroffenenrechte und Rechtsschutzmöglichkeiten hinsichtlich § 25a HSOG thematisiert. Zum einen besteht die Gefahr, dass das Auskunftsrecht lediglich auf die Quellsysteme bezogen wird und damit nicht konkret auf hessenDATA. Fehlt es an der Anerkennung eines solchen Auskunftsrechts spezifisch zu § 25a HSOG, ist es einer betroffenen Person kaum möglich zu erfahren, ob personenbezogene Daten im Rahmen von hessenDATA analysiert worden sind, und in der Folge dagegen Rechtsschutz zu suchen sowie ggf. gerichtlich vorzugehen. Zum anderen ist § 25a HSOG weder von der speziellen Protokollierungspflicht bei verdeckten und eingriffsintensiven Verfahren nach § 28 HSOG noch von der Benachrichtigungspflicht nach § 29 Abs. 5 in Verbindung mit § 28 Abs. 2 HSOG umfasst.

Schließlich habe ich darauf verwiesen, dass § 25a HSOG nicht über die notwendigen und wirksamen verfahrensbegleitenden Schutzmaßnahmen verfügt. So läuft die als Absicherung in datenschutzrechtlicher Hinsicht gedachte Anhörung meiner Behörde in § 25a Abs. 3 S. 2 HSOG derzeit praktisch leer, da meine Behörde zwar bei den generellen phänomenbezogenen Anordnungen der hessischen Polizeibehörden mit einbezogen wurde (s. Kleine Anfrage und Antwort, LT-Drs. 20/660, S. 1, Stand Juli 2019: In der Antwort zu Frage 1 werden fünf generelle phänomenbezogene Anordnungen genannt). Aber seit dem Jahr 2019 hat es keine weiteren Anordnungen und folglich keine Anhörungen meiner Behörde mehr gegeben, da dies nicht vorgesehen ist, solange hessenDATA keine größere Veränderung in technischer Hinsicht erfährt und ohne wesentliche Neuerungen mit den gleichen Quellsystemen und -datenbanken genutzt wird. Ferner erstreckt sich die Pflicht zur Datenschutzkontrolle durch meine Behörde in § 29a HSOG nicht auf § 25a HSOG und es gibt keine spezifischen Richtervorbehalte oder Berichtspflichten.

Im Ergebnis habe ich daher in meiner Stellungnahme konstatiert, dass die Regelung § 25a HSOG in mehrfacher Hinsicht verfassungsrechtlichen Zweifeln ausgesetzt ist, die auch durch eine mögliche verfassungskonforme Auslegung letztlich nicht ausgeräumt werden können.

Zum Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 und den Folgen für die hessische Praxis werde ich im nächsten Tätigkeitsbericht nähere Ausführungen machen.

6.2
Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung

Im Berichtsjahr legte die Landesregierung einen Gesetzentwurf zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei vom 22. März 2022, LT-Drs. 20/8129, vor. Im Rahmen des Gesetzgebungsverfahrens gab ich eine schriftliche und mündliche Stellungnahme ab, über die ich im Folgenden berichte. Das Gesetzgebungsverfahren war zum Zeitpunkt der Erstellung des Tätigkeitsberichts noch nicht abgeschlossen.

Im Rahmen der öffentlichen Anhörung im Innenausschuss hatte ich Gelegenheit, zum Gesetzentwurf zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei vom 22. März 2022, LT-Drs. 20/8129, Stellung zu nehmen. Leider hatte ich keine Gelegenheit, meine datenschutzrechtlichen Bedenken bereits frühzeitig im Rahmen der Erstellung des Gesetzentwurfs einzubringen.

Meine Anmerkungen haben sich insbesondere auf die Vorschläge zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) konzentriert. Der Gesetzentwurf hatte auch Änderungen des Hessischen Verfassungsschutzgesetzes (HVSG) vorgesehen. Er hatte aber noch nicht die neuen Vorgaben des Urteils des BVerfG, 1 BvR 1619/17, vom 26. April 2022 zum Bayerischen Verfassungsschutzgesetz, das als teilweise verfassungswidrig eingestuft wurde, im Hinblick auf das HVSG umgesetzt. Daher beschränkte sich die Anhörung auch auf die Änderungsvorschläge zum HSOG.

Meine vollständige Stellungnahme findet sich in der Ausschussvorlage INA 20/53 Teil 1 vom 1. Juli 2022 auf den Seiten 79 ff., die ebenso Grundlage für meine Ausführungen in der öffentlichen mündlichen Anhörung des Innenausschusses des Hessischen Landtags am 15. Juli 2022 gewesen ist.

Regelüberprüfung von Bewerberinnen und Bewerbern

In der Stellungnahme habe ich mich u. a. kritisch zur vorgeschlagenen Änderung des § 13a Abs. 2 HSOG-E geäußert. Die im Gesetzentwurf vorgesehene Ergänzung, Bedienstete, die eine Tätigkeit in einer Behörde mit Vollzugsaufgaben anstreben, regelmäßig auch anhand von Datenbeständen des LfV Hessen zu überprüfen, ist zwar nachvollziehbar, birgt aber aufgrund der Besonderheit der Datenbestände des Verfassungsschutzes einige rechtliche Risiken.

Zunächst ist es bereits problematisch, eine solche als Regelvorgabe ausgestaltete Überprüfung, die im Ergebnis aufgrund „weicher" Erkenntnisse des Verfassungsschutzes Personen von bestimmten Berufsgruppen ausschließen kann, in einem Polizeigesetz zu verankern. Im Grunde handelt es sich hier um ein Hindernis für die Zulassung zum Staatsdienst, für zumeist beamtenrechtliche Tätigkeiten, und sollte daher in den entsprechenden Gesetzen verankert werden.

Zudem fehlt es im § 13a Abs. 2 HSOG-E an Regelungen, wie der Bewerber oder die Bewerberin im Fall einer Ablehnung etwa aufgrund von Erkenntnissen des Verfassungsschutzes Rechtsschutz suchen kann. Im Unterschied hierzu macht etwa § 7 Luftsicherheitsgesetz für Zuverlässigkeitsüberprüfungen konkrete Ausführungen zur Ausgestaltung des Verfahrens.

Hinzu kommt noch die Besonderheit, dass die Ablehnung einer Auskunftserteilung nach § 26 Abs. 3 HVSG keiner Begründung bedarf. So ist denkbar, dass die betroffenen Personen für die Tätigkeit als Bedienstete bei einer Behörde mit Vollzugsaufgaben aufgrund von Erkenntnissen des Verfassungsschutzes abgelehnt werden, ohne jedoch zu erfahren, um welche Erkenntnisse es sich hierbei handelt und wie sie ggf. eine solche Ablehnung konkret überprüfen lassen können.

Videoüberwachung ohne Kriminalitätsanalyse

Des Weiteren habe ich mich zum Vorschlag in Bezug auf die Videoüberwachung in § 14 Abs. 3a HSOG-E kritisch geäußert. Der Gesetzentwurf hat eine Ergänzung dergestalt vorgesehen, dass die Voraussetzungen für eine Videoüberwachung nach Abs. 3 Satz 1 „in den öffentlich zugänglichen Bereichen von Flughäfen, Personenbahnhöfen, Sportstätten, Einkaufszentren und Packstationen als erfüllt" anzusehen sind. Mithin soll an diesen Örtlichkeiten künftig die Kriminalitätsanalyse entfallen und eine Videoüberwachung regelmäßig zulässig sein.

Zunächst ist die Norm im Hinblick auf die räumlichen Grenzen der aufgezählten Örtlichkeiten problematisch, da es an einer hinreichenden Bestimmtheit der

„öffentlich zugänglichen Bereiche“ dieser Örtlichkeiten in der vorgeschlagenen Regelung mangelt. Bezüglich des Großflughafens Frankfurt am Main ergeben sich ferner spezifische räumliche Abgrenzungsprobleme, etwa wo genau der Bereich des Flughafens beginnt und endet.

Aus datenschutzrechtlicher Sicht ebenso nicht nachvollziehbar ist es, jede Packstation in Hessen unterschiedslos als Kriminalitätsschwerpunkt einzuordnen. Unklar ist auch, inwieweit eine präventive Videoüberwachung Kriminalität in öffentlich zugänglichen Bereichen von Packstationen verhindern kann. Zudem wurde im Rahmen der Gesetzesbegründung nicht dargelegt, warum eine solche Maßnahme dort überhaupt für nötig erachtet wird. Bezüglich der öffentlich zugänglichen Bereiche von allen Sportstätten in Hessen halte ich eine erweiterte Regelung für verzichtbar, da die dort auftretende Kriminalität nicht durch die Örtlichkeit ausgelöst wird. Vielmehr sind es dort stattfindende Veranstaltungen – sportliche wie gesellschaftliche und kulturelle –, die im Ausnahmefall Kriminalitätsrisiken verursachen. Diese dürfen nach individueller prognostischer Bewertung auch aufgrund der aktuellen Regelung gemäß § 14 Abs. 3 HSOG zu kriminalpräventiven Zwecken videoüberwacht werden. Die Qualifizierung aller Einkaufszentren als Kriminalitätsschwerpunkte ist ebenfalls nicht sachgerecht.

Automatisierte Verarbeitung von Kraftfahrzeugkennzeichen

Die im Gesetzentwurf vorgeschlagenen Änderungen zu § 14a HSOG-E zur automatisierten Verarbeitung von Kraftfahrzeugkennzeichen enthalten nun Klarstellungen und Einschränkungen, die das BVerfG mit Urteil vom 11. März 2008 (1 BvR 2074/05) sowie mit Beschluss vom 18. Dezember 2018 (1 BvR 3187/10) für eine solche Regelung vorgegeben hat. Sie bleiben jedoch in einem wesentlichen Aspekt hinter diesen Anforderungen zurück: Das BVerfG fordert eine Konkretisierung des Begriffs „Fahndungsbestand“, mit dem die Kraftfahrzeugkennzeichen abgeglichen werden sollen. Eine ausreichende Konkretisierung dieses Begriffs fehlt jedoch im Gesetzentwurf.

Fortgesetzte Datenspeicherung ohne Negativprognose

Schließlich habe ich auch kritische Anmerkungen zur vorgeschlagenen Gesetzesänderung zu § 27 Abs. 4 HSOG-E gemacht, die eine erhebliche Verlängerung der Aussonderungsprüffristen darstellt. So darf bei „fortbestehendem Tatverdacht“ bezüglich der kategorisierten Straftaten eine Verlängerung der Speicherung um zehn Jahre erfolgen, bei sonstigen Straftaten von erheblicher Bedeutung (§ 13 Abs. 3 HSOG) um weitere fünf Jahre.

Eine grundsätzliche personenbezogene Negativprognose als rechtliche Voraussetzung für eine polizeiliche Speicherung ist in der bisherigen Fassung des HSOG sowie auch im vorliegenden Entwurf in § 20 Abs. 6 HSOG nicht vorgesehen – eine solche Regelung, wie sie etwa § 18 Abs. 1 Nr. 3 und Abs. 2 Nr. 2 BKAG vorsehen, fehlt. Vor dem Hintergrund der erweiterten Speichermöglichkeiten erscheint als Voraussetzung für die Speicherung im polizeilichen Informationssystem POLAS-Hessen eine individuell personenbezogene Negativprognose nunmehr noch dringlicher geboten.

Die aktuelle Formulierung des Gesetzentwurfs wird dadurch letztlich zu einer Regelspeicherung von 15 oder 20 Jahren bei kategorisierten oder klassifizierten Straftaten führen, ohne dass zum Zeitpunkt der Verlängerung eine Prüfung oder Überprüfung, ob tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person solche Straftaten begehen wird, erfolgen muss. Eine entsprechende Überprüfung ist nunmehr erst bei einer weiteren Verlängerung vorgesehen (§ 27 Abs. 4 Satz 5 HSOG-E). Der Begründungsaufwand für die korrespondierenden Grundrechtseingriffe wird somit um fünf bzw. zehn Jahre in die Zukunft verschoben. In diesem Zusammenhang möchte ich, um die Brisanz dieser Problematik zu illustrieren, darauf hinweisen, dass in Abgrenzung zu den Daten aus dem Bundeszentralregister im polizeilichen Informationssystem auch Straftaten erfasst und gespeichert werden können, bei denen es nicht zu einer Anklage oder zu einer Verurteilung gekommen ist.

Es bleibt nun abzuwarten, inwieweit der Gesetzgeber auf die nicht nur von mir in der öffentlichen Anhörung im Innenausschuss des Hessischen Landtags geäußerte Kritik reagieren und den Gesetzentwurf überarbeiten wird.

6.3
Beschwerden gegen das Landesamt für Verfassungsschutz

Die Auskünfte des Landesamtes für Verfassungsschutz Hessen (LfV Hessen) gem. § 26 HVSG beinhalten regelmäßig einen Hinweis darauf, dass sich die betroffene Person an meine Behörde wenden kann. Eine Beschwerde über eine verweigerte Auskunft löste eine Überprüfung des Auskunftsverfahrens beim LfV Hessen aus. Hier kollidieren regelmäßig datenschutzrechtliche und fachlich-inhaltliche Fragestellungen.

Das Auskunftsrecht gegenüber dem LfV Hessen ist spezialgesetzlich im Hessischen Verfassungsschutzgesetz (HVSG) geregelt. Die Regelung des § 26 HVSG sieht in Abs. 2 Möglichkeiten zur Einschränkung des Auskunftsrechts vor und verweist in Abs. 3 darauf, dass die betroffene Person sich an meine Behörde wenden kann.

§ 26 HVSG

(1) Das Landesamt erteilt der betroffenen Person über zu ihrer oder seiner Person gespeicherte Daten auf Antrag unentgeltlich Auskunft, soweit die betroffene Person hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt. Legt die betroffene Person nach Aufforderung ein besonderes Interesse nicht dar, entscheidet das Landesamt nach pflichtgemäßem Ermessen. Die Auskunft erstreckt sich nicht auf

1. *die Herkunft der Daten und die Empfänger von Übermittlungen und*
2. *Daten, die nicht strukturiert in automatisierten Dateien gespeichert sind, es sei denn, die betroffene Person macht Angaben, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand steht nicht außer Verhältnis zu dem von der betroffenen Person dargelegten Auskunftsinteresse.*

Das Landesamt bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Die Auskunftserteilung unterbleibt, soweit durch sie

1. *eine Gefährdung der Erfüllung der Aufgaben zu besorgen ist,*
2. *Nachrichtenzugänge gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Landesamts zu befürchten ist,*
3. *die öffentliche Sicherheit gefährdet oder sonst dem Wohl des Bundes oder eines Landes ein Nachteil bereitet würde oder*
4. *Daten oder die Tatsache ihrer Speicherung preisgegeben werden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.*

Die Entscheidung trifft die Behördenleitung oder eine von ihr besonders beauftragte Mitarbeiterin oder ein von ihr besonders beauftragter Mitarbeiter.

(3) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung. Sie enthält einen Hinweis auf die Rechtsgrundlage für das Fehlen der Begründung und darauf, dass sich die betroffene Person an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden kann. Mitteilungen der oder des Hessischen Datenschutzbeauftragten an die betroffene Person dürfen ohne Zustimmung des Landesamts keine Rückschlüsse auf den Kenntnisstand des Landesamts zulassen.

(…)

Sofern einem Empfänger im Rahmen der Auskunft Mitteilung über eine teilweise oder vollständige Auskunftsverweigerung gemacht wird, erscheint die Möglichkeit, sich an meine Behörde zu wenden, subjektiv nicht selten als eine Möglichkeit, die vorenthaltenen Auskünfte doch noch zu bekommen. Weiterhin wenden sich auch Betroffene an mich, um auf diesem Wege die Löschung von Speicherungen zu veranlassen.

Zunächst ist festzustellen, dass eine fachlich-inhaltliche Prüfung der Rechtmäßigkeit von Speicherungen beim LfV Hessen durch meine Behörde

gesetzlich nicht vorgesehen ist. Der Gesetzgeber hat in § 26 Abs. 3 Satz 1 HVSG geregelt, dass im Falle einer vollständigen oder teilweisen Ablehnung der Auskunft ohne Begründung auf die Möglichkeit, sich an meine Behörde zu wenden, hingewiesen werden muss.

Meine Behörde kann das erfolgte Auskunftsverfahren beim LfV Hessen in datenschutzrechtlicher Hinsicht überprüfen. Die Geltung datenschutzrechtlicher Vorschriften ist jedoch gemäß § 15 HVSG eingeschränkt.

§ 15 HVSG

Bei der Erfüllung der Aufgaben nach § 2 durch das Landesamt findet das Hessische Datenschutz- und Informationsfreiheitsgesetz vom 3. Mai 2018 (GVBl. S. 82) in der jeweils geltenden Fassung wie folgt Anwendung:

1. *§ 1 Abs. 8, die §§ 4, 14 Abs. 1 und 3, § 19 sowie der Zweite Teil finden keine Anwendung,*
2. *die §§ 41, 46 Abs. 1 bis 4 und die §§ 47 bis 49, 57, 59, 78 und 79 sind entsprechend anzuwenden.*

Eine solche Prüfung erstreckt sich auf die Fragestellung, ob das LfV Hessen mit den Daten des Betroffenen im Sinn der Betroffenenrechte ordnungsgemäß umgegangen ist, es also eine nachvollziehbar dokumentierte, personen- und sachverhaltsbezogene Befassung mit dem konkreten Auskunftsbegehren und einer ganzen oder teilweisen Auskunftsverweigerung gegeben hat. Diese datenschutzrechtliche Prüfung grenzt sich von einer fachlich-inhaltlichen Prüfung zu den betreffenden Speicherungen und der Bewertung, ob diesbezügliche Auskünfte verweigert werden dürfen, ab. Um eine Offenlegung von bisher verweigerten Auskünften zu erlangen und weiterhin auch, um ggf. einzelne Löschungen zu veranlassen, muss der Betroffene gegen den diesbezüglichen Auskunftsbescheid des LfV Hessen fristgerecht vorgehen (Widerspruch und Klage). Nur auf diesem Weg können abschließend ggf. die Auskunftserteilung bisher vorenthaltener Informationen oder auch Löschungen bewirkt werden. Durch den Ausschluss der Anwendbarkeit von § 14 Abs. 3 HDSIG in § 15 Nr. 1 HVSG sind meine dort formulierten Anordnungsbefugnisse nicht auf die Datenverarbeitungen beim LfV Hessen anwendbar. Meine aufsichtsbehördlichen Möglichkeiten gegenüber dem LfV Hessen beschränken sich auf die Befugnisse gemäß § 14 Abs. 2 HDSIG, d. h. die Beanstandung gegenüber der zuständigen obersten Landesbehörde sowie die Warnung vor beabsichtigten Verarbeitungsvorgängen, soweit diese voraussichtlich gegen anwendbare datenschutzrechtliche Vorschriften verstoßen.

Soweit im datenschutzrechtlichen Beschwerdeverfahren durch meine Behörde beschieden wird, dass das Auskunftsverhalten des LfV Hessen im konkreten Einzelfall nicht zu bemängeln ist, bedeutet dies nicht, dass

einzelne Speicherungen oder Auskunftsverweigerungen des LfV Hessen fachlich-inhaltlich von meiner Dienststelle bewertet wurden, sondern nur, dass dort eine datenschutzrechtlich sachgerechte Befassung mit dem Auskunftsbegehren stattgefunden hat. Eine Klage gegen meinen Bescheid vor dem Verwaltungsgericht kann jedoch weder Löschungen beim LfV Hessen noch Auskünfte zu bisher verweigerten Speicherungen bewirken.

Insofern ist es für Betroffene wichtig, gegen einen Bescheid des LfV Hessen zu einer Auskunft gemäß § 25 HVSG ggf. fristgerecht Widerspruch einzulegen, soweit sie die Auskunftserteilung im Falle bisher abgelehnter Auskünfte oder Löschungen erreichen möchten.

6.4

Datenschutzkontrollen bei Polizeibehörden und Verfassungsschutz

In verschiedenen Bereichen schreiben gesetzliche Regelungen vor, dass ich bestimmte Datenschutzkontrollen bei hessischen Polizeibehörden und beim Landesamt für Verfassungsschutz (LfV Hessen) durchführe. Im Jahr 2022 wurde die im Jahr 2021 erstmalig durchgeführte Datenschutzkontrolle des Schengener Informationssystems der zweiten Generation (SIS II) fortgesetzt. Im Weiteren wurden die Antiterrordatei (ATD) und verdeckte Maßnahmen geprüft.

Erstmals begann Ende des Jahres 2021 eine Prüfung der Ausschreibungen nach § 17 HSOG und § 163e StPO in Verbindung mit Art. 36 Abs. 2 SIS II-Beschluss. Diese Datenschutzkontrolle wurde europaweit und auch bei Bund und Ländern durch die Datenschutzbehörden abgestimmt gestaltet. Die Polizeibehörden nutzen die Möglichkeit der Ausschreibung von Personen und Sachen sowohl zur Gefahrenabwehr als auch zur Strafverfolgung. Im Zuge der Ausschreibungen können die Polizeien der Länder und des Bundes verdeckte oder gezielte Kontrollen durchführen und daraus gewonnene personenbezogene Daten mittels Treffermeldungen an die ausschreibende Stelle weiterleiten.

Im Vorlauf der Prüfung wurde gemeinsam mit dem Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) der von der SIS II Supervision Coordination Group (SIS II SCG; die Gruppe besteht aus Vertretern der nationalen Aufsichtsbehörden der Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten) erstellte umfangreiche Fragenkatalog übersetzt und auf die Bedürfnisse der deutschen Aufsichts- und Polizeibehörden entsprechend angepasst. Durch die jeweiligen Polizeibehörden wurde dieser Fragenkatalog als Teil der Kontrollaktivität beantwortet. Inhaltlich konnten

so Arbeitsweisen und Handlungsabläufe rund um das SIS II in Erfahrung gebracht und hinterfragt werden.

Für die Datenschutzkontrolle selbst erarbeitete meine Behörde darüber hinaus ein Prüfschema, das über den Arbeitskreis Sicherheit auch den Datenschutzaufsichtsbehörden der Länder und des Bundes zur Verfügung gestellt wurde. Die Kontrollaktivität wurde von elf Aufsichtsbehörden durchgeführt und insgesamt wurden durch diese 27 Stellen geprüft. Die Ergebnisse des Fragebogens und der Prüfung wurden anschließend zusammengetragen und der SIS II SCG mitgeteilt.

Im Rahmen meiner Datenschutzkontrolle wurden stichprobenartig 26 durch hessische Polizeibehörden initiierte Ausschreibungen geprüft. Dabei habe ich einige Mängel festgestellt: Z. B. wurden die Dokumentationspflichten zu verschiedenen polizeilichen Maßnahmen nicht in allen Fällen ausreichend erfüllt. So sieht etwa § 17 Abs. 4 S. 4 HSOG bei polizeilichen Beobachtungen oder gezielten Kontrollen vor, dass spätestens nach Ablauf von jeweils drei Monaten zu prüfen ist, ob die Voraussetzungen für die Anordnung noch bestehen; das Ergebnis dieser Prüfung ist aktenkundig zu machen.

Weitere mögliche aufsichtsbehördliche Maßnahmen werden aktuell noch geprüft.

Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II-Beschluss)

Art. 36 SIS II-Beschluss

(…)

(2) Eine Ausschreibung dieser Art ist zulässig zur Strafverfolgung und zur Abwehr von Gefahren für die öffentliche Sicherheit, wenn

a) tatsächliche Anhaltspunkte dafür vorliegen, dass eine Person eine schwere Straftat, z. B. eine der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten, plant oder begeht, oder

b) die Gesamtbeurteilung einer Person, insbesondere aufgrund der bisher von ihr begangenen Straftaten, erwarten lässt, dass sie auch künftig schwere Straftaten, z. B. eine der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI genannten Straftaten, begehen wird.

(…)

Entsprechend der gesetzlichen Vorgaben aus § 10 Abs. 1 S. 1 ATDG fanden zudem Datenschutzkontrollen zu Speicherungen in der ATD statt. Diese hat nach gesetzlichen Vorgaben alle zwei Jahre zu erfolgen und erfolgte im Jahr 2022 beim LfV Hessen und dem Polizeipräsidium Frankfurt am Main zu Neuspeicherungen von Personen innerhalb der Jahre 2020 und 2021. Schwerpunkt dieser Prüfung lag auf Speicherungen gemäß § 2 und § 3 Abs. 2 ATDG.

Die Speicherung in einer solchen Verbunddatei, die Informationen für die Polizeien und Verfassungsschutzbehörden der Länder und des Bundes verfügbar macht, stellt für die betroffenen Personen einen besonders tiefen Grundrechtseingriff dar. In der Regel weiß die betroffene Person nicht, dass sie darin gespeichert ist.

Grundlage meiner Datenschutzkontrolle der ATD war dabei zunächst der Akteninhalt zur gespeicherten Person. Anhand der vorgelegten Personenakten und dem zugrundeliegenden Sachverhalt prüfte meine Behörde, ob die Voraussetzungen für eine Speicherung der entsprechenden Person vorlagen sowie ausreichend und nachvollziehbar dokumentiert wurden.

Es bestehen keine datenschutzrechtlichen Bedenken gegen die Speicherung der geprüften Personen in der ATD.

§ 2 ATDG

Die beteiligten Behörden sind verpflichtet, bereits erhobene Daten nach § 3 Abs. 1 in der Antiterrordatei zu speichern, wenn sie gemäß den für sie geltenden Rechtsvorschriften über polizeiliche oder nachrichtendienstliche Erkenntnisse (Erkenntnisse) verfügen, aus denen sich tatsächliche Anhaltspunkte dafür ergeben, dass die Daten sich beziehen auf

1. *Personen, die*

a) *einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs, die einen internationalen Bezug aufweist, oder einer terroristischen Vereinigung nach § 129a in Verbindung mit § 129b Absatz 1 Satz 1 des Strafgesetzbuchs mit Bezug zur Bundesrepublik Deutschland angehören oder diese unterstützen,*

b) *einer Gruppierung, die eine Vereinigung nach Buchstabe a unterstützt, angehören oder*

c) *eine Gruppierung nach Buchstabe b willentlich in Kenntnis der den Terrorismus unterstützenden Aktivität der Gruppierung unterstützen,*

2. *Personen, die rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden oder eine solche Gewaltanwendung unterstützen, vorbereiten oder durch ihre Tätigkeiten, insbesondere durch Befürworten solcher Gewaltanwendungen, vorsätzlich hervorrufen, oder*

(...)

§ 3 ATDG

(1) In der Antiterrordatei werden, soweit vorhanden, folgende Datenarten gespeichert:

1. zu Personen nach § 2 Satz 1 Nummer 1 und 2

a) der Familienname, die Vornamen, frühere Namen, andere Namen, Aliaspersonalien, abweichende Namensschreibweisen, das Geschlecht, das Geburtsdatum, der Geburtsort, der Geburtsstaat, aktuelle und frühere Staatsangehörigkeiten, gegenwärtige und frühere Anschriften, besondere körperliche Merkmale, Sprachen, Dialekte, Lichtbilder, die Bezeichnung der Fallgruppe nach § 2 und, soweit keine anderen gesetzlichen Bestimmungen entgegenstehen und dies zur Identifizierung einer Person erforderlich ist, Angaben zu Identitätspapieren (Grunddaten),

b) folgende weitere Datenarten (erweiterte Grunddaten):

(...)

oo) Kontaktpersonen zu den jeweiligen Personen nach § 2 Satz 1 Nr. 1 Buchstabe a oder Nr. 2,

(...)

(2) Kontaktpersonen nach Absatz 1 Nummer 1 Buchstabe b Doppelbuchstabe oo sind Personen, bei denen tatsächliche Anhaltspunkte vorliegen, dass sie mit den in § 2 Satz 1 Nummer 1 Buchstabe a oder Nummer 2 genannten Personen nicht nur flüchtig oder in zufälligem Kontakt in Verbindung stehen und durch sie weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind.

(...)

§ 10 ATDG

(1) Die Kontrolle der Durchführung des Datenschutzes obliegt nach § 9 Absatz 1 des Bundesdatenschutzgesetzes der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Die von den Ländern in die Antiterrordatei eingegebenen Datensätze können auch von den jeweiligen Landesbeauftragten für den Datenschutz im Zusammenhang mit der Wahrnehmung ihrer Prüfungsaufgaben in den Ländern kontrolliert werden, soweit die Länder nach § 8 Absatz 1 verantwortlich sind. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit arbeitet insoweit mit den Landesbeauftragten für den Datenschutz zusammen.

(2) Die in Absatz 1 genannten Stellen sind im Rahmen ihrer jeweiligen Zuständigkeiten verpflichtet, mindestens alle zwei Jahre die Durchführung des Datenschutzes zu kontrollieren.

(…)

Eine weitere gesetzlich vorgeschriebene Datenschutzkontrolle ist die der verdeckten Maßnahmen gemäß § 29a HSOG. In diesem Jahr prüfte meine Behörde daher Telekommunikationsüberwachungsmaßnahmen (TKÜ-Maßnahmen) gemäß § 15a HSOG beim Hessischen Landeskriminalamt (HLKA). TKÜ-Maßnahmen erfolgen durch Polizeibehörden sowohl als klassische Abhörmaßnahme als auch zur Ortung eines Telekommunikationsgeräts.

Grundlage der Prüfung waren die Telefon- und Mobilfunknummern, die seitens des HLKA im Zeitraum 2018 bis zum Stichtag am 14. November 2022 mit einer TKÜ-Maßnahme belegt waren. Als Schwerpunkte für diese Datenschutzkontrolle wurden die Anordnungen der einzelnen Maßnahmen, Dokumentationen von Beginn und Ende der jeweiligen Maßnahmen, Benachrichtigung betroffener Personen sowie Löschung von Altdaten gewählt.

Bis zum Redaktionsschluss des vorliegenden Tätigkeitsberichts war diese Kontrolltätigkeit noch nicht abgeschlossen.

§ 15a HSOG

(1) Die Polizeibehörden können von einem Dienstanbieter, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, verlangen, dass er die Kenntnisnahme durch Überwachung und Aufzeichnung des Inhalts der Telekommunikation ermöglicht und die näheren Umstände der Telekommunikation einschließlich des Standorts aktiv geschalteter nicht ortsfester Telekommunikationsanlagen übermittelt, wenn dies zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, unerlässlich ist. Die Maßnahme darf sich gegen eine Person richten,

1. *die nach den §§ 6 oder 7 verantwortlich ist,*
2. *bei der die Voraussetzungen des § 9 vorliegen,*
3. *bei der bestimmte Tatsachen die Annahme rechtfertigen, dass*

a) *sie für eine Person nach Nr. 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt oder*

b) *eine Person nach Nr. 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird, soweit die Maßnahme zur Verhütung terroristischer Straftaten unerlässlich ist, oder*

4. *die in § 15 Abs. 2 Satz 1 Nr. 2 oder 3 genannt ist, soweit die Maßnahme zur Verhütung terroristischer Straftaten unerlässlich ist.*

Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden. § 15 Abs. 4 Satz 4 bis 8 gilt entsprechend.

(2) Unter den Voraussetzungen des Abs. 1 können die Polizeibehörden auch Auskunft über Verkehrsdaten nach § 96 Abs. 1 des Telekommunikationsgesetzes (...), in einem zurückliegenden oder einem zukünftigen Zeitraum sowie über Inhalte verlangen, die innerhalb des Telekommunikationsnetzes in Speichereinrichtungen abgelegt sind. (...) Auskunft über Bestandsdaten nach den §§ 95 und 111 des Telekommunikationsgesetzes können die Polizeibehörden von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, unter den Voraussetzungen des § 12 Abs. 1 Satz 1, Abs. 3 und 4 verlangen (§ 113 Abs. 1 Satz 1 und 3 des Telekommunikationsgesetzes). Bezieht sich das Auskunftsverlangen nach Satz 3 auf Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird (§ 113 Abs. 1 Satz 2 des Telekommunikationsgesetzes), darf die Auskunft nur verlangt werden, wenn die gesetzlichen Voraussetzungen für die Nutzung der Daten vorliegen. Die Auskunft über Bestandsdaten anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse darf nur zur Abwehr einer erheblichen Gefahr verlangt werden. § 29 Abs. 5 bis 7 gilt für Satz 4 und 5 entsprechend.

(2a) Unter den Voraussetzungen des Abs. 1 können die Polizeibehörden von denjenigen, die geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, Auskunft über Nutzungsdaten nach § 15 Abs. 1 des Telemediengesetzes (...) verlangen. Die Auskunft kann auch über zukünftige Nutzungsdaten verlangt werden. Unter den Voraussetzungen des § 12 Abs. 1 Satz 1, Abs. 3 und 4 können die Polizeibehörden Auskunft über Bestandsdaten nach § 14 Abs. 1 des Telemediengesetzes verlangen. Der Dienstanbieter hat die Daten unverzüglich auf dem von der Polizeibehörde bestimmten Weg zu übermitteln.

(3) Die Polizeibehörden können unter den Voraussetzungen des Abs. 1 technische Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes und der Geräte- und Kartennummern einsetzen.

(4) Die Polizeibehörden können zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person oder für solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Bundes oder eines Landes oder die Grundlagen der Existenz der Menschen berührt, Telekommunikationsverbindungen durch den Einsatz technischer Mittel unterbrechen oder verhindern. (...)

6.5
Prüfung einer Staatsanwaltschaft zu Benachrichtigungen bei verdeckten Maßnahmen

Im Frühjahr 2022 habe ich eine Vor-Ort-Überprüfung bei einer hessischen Staatsanwaltschaft durchgeführt, deren Schwerpunkt auf verdeckten Maßnahmen nach § 100a StPO lag. Hierbei wurden Rechtmäßigkeit, Dokumentation sowie Benachrichtigungen Betroffener und das Unterbleiben oder endgültige Absehen von Benachrichtigungen genauer in den Blick genommen.

Im Anwendungsbereich der Richtlinie (EU) 2016/680 (JI-Richtlinie) überwache ich gemäß § 13 Abs. 1 und 2 Nr. 1 HDSIG die Anwendung und Durchsetzung der Vorschriften über den Datenschutz in Hessen. Gemäß §§ 14 Abs. 4 und 63 HDSIG, § 500 StPO in Verbindung mit § 68 BDSG stehen mir und meinen Mitarbeitern dabei Untersuchungs- und Kontrollbefugnisse zu.

Eine Telekommunikationsüberwachung nach § 100a StPO stellt eine besonders eingriffsintensive Maßnahme der Strafverfolgung dar. Im Zuge von Überwachungsmaßnahmen gem. § 100a StPO werden regelmäßig in größerem Umfang personenbezogene Daten verarbeitet. Dies betrifft neben Daten zu den Umständen der Kommunikationsvorgänge vor allem die eigentlichen Inhaltsdaten. Die anschließende Benachrichtigung gem. § 101 Abs. 4 S. 1 Nr. 3 StPO ist eine Grundvoraussetzung für den Schutz der Rechte und Freiheiten betroffener Personen und etwaiger Drittbetroffener. Auch für die Wahrnehmung von Betroffenenrechten ist eine Benachrichtigung notwendige Vorbedingung. Der Gesetzgeber hat in § 101 Abs. 6 StPO deshalb hohe Voraussetzungen an Zurückstellungen der Benachrichtigung

geknüpft. Unter den Voraussetzungen des § 101 Abs. 4 S. 3 und 4 StPO kann eine Benachrichtigung Betroffener zudem unterbleiben.

Zuständig für die Durchführung der Benachrichtigung über Maßnahmen nach § 100a StPO ist die jeweilige Staatsanwaltschaft. Aus diesem Grund hat meine Behörde im Frühjahr 2022 eine Überprüfung anhand von Verfahrensakten bei einer hessischen Staatsanwaltschaft vor Ort durchgeführt.

Es wurde als Stichprobe eine zweistellige Anzahl an Akten angefordert. Alle der angeforderten Akten betrafen Ermittlungen, während derer Maßnahmen zur Telekommunikationsüberwachung gemäß § 100a StPO angeordnet worden waren. Diese konnten bis auf eine Akte, die sich bei Gericht befand, bereitgestellt werden. Bei der Auswahl wurde darauf geachtet, möglichst viele Dezernate und örtliche Zuständigkeitsbereiche abzudecken. Innerhalb des zur Verfügung stehenden Zeitrahmens konnten insgesamt zehn Akten einer genaueren Überprüfung unterzogen werden.

Besonderes Augenmerk sollte auf dem Vorliegen der richterlichen Anordnung für die jeweilige Maßnahme und der Durchführung der Benachrichtigung betroffener Personen liegen.

Im Ergebnis war die grundsätzliche Dokumentation einschließlich der richterlichen Beschlüsse vorhanden. Es konnten jedoch ergänzende Hinweise bezüglich der Handhabung von Benachrichtigungen Drittbetroffener gegeben werden. Was die Überprüfbarkeit von Abwägungsentscheidungen beim Unterbleiben von Benachrichtigungen angeht, habe ich eine umfangreichere Dokumentation angemahnt. Mit einer schriftlichen Dokumentation wird die Rechtssicherheit für die anordnende Behörde erhöht und die Nachvollziehbarkeit der Rechtmäßigkeit im Falle von späteren Beschwerden Betroffener sichergestellt. Außerdem war in einem Fall ein richterlicher Beschluss für die Zurückstellung der Benachrichtigung vom Verantwortlichen nachzuholen.

Nach § 101 Abs. 8 StPO sind die durch die Maßnahme erlangten personenbezogenen Daten unverzüglich zu löschen, sobald sie für eine etwaige gerichtliche Überprüfung oder Maßnahme nicht mehr erforderlich sind. Löschprotokolle bezüglich der erhobenen, personenbezogenen Daten im Sinn des § 101 Abs. 8 StPO waren bei stichprobenartigen Kontrollen in den vorgesehenen Fällen vorhanden und Bestandteil der Akten. Die Mitteilung über die Vornahme der Löschung wurde jeweils in die Benachrichtigungen einbezogen.

Die Dezernate der Staatsanwaltschaft sind im Nachgang für das Thema Benachrichtigungen in der Folge von Maßnahmen zur Telekommunikationsüberwachung durch den Verantwortlichen sensibilisiert worden. Der Datenschutzbeauftragte vor Ort ist ebenfalls einbezogen worden.

§ 101 StPO

(1) Für Maßnahmen nach den §§ 98a, 99, 100a bis 100f, 100h, 100i, 110a, 163d bis 163g gelten, soweit nichts anderes bestimmt ist, die nachstehenden Regelungen. (…)

(3) Personenbezogene Daten, die durch Maßnahmen nach Absatz 1 erhoben wurden, sind entsprechend zu kennzeichnen. Nach einer Übermittlung an eine andere Stelle ist die Kennzeichnung durch diese aufrechtzuerhalten.

(4) Von den in Absatz 1 genannten Maßnahmen sind im Falle (…)

3. des § 100a die Beteiligten der überwachten Telekommunikation (…) zu benachrichtigen. Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 7 und die dafür vorgesehene Frist hinzuweisen. Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen. Zudem kann die Benachrichtigung einer in Satz 1 Nummer 2 und 3 bezeichneten Person, gegen die sich die Maßnahme nicht gerichtet hat, unterbleiben, wenn diese von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung hat. Nachforschungen zur Feststellung der Identität einer in Satz 1 bezeichneten Person sind nur vorzunehmen, wenn dies unter Berücksichtigung der Eingriffsintensität der Maßnahme gegenüber dieser Person, des Aufwands für die Feststellung ihrer Identität sowie der daraus für diese oder andere Personen folgenden Beeinträchtigungen geboten ist.

(5) Die Benachrichtigung erfolgt, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten, im Fall des § 110a auch der Möglichkeit der weiteren Verwendung des Verdeckten Ermittlers möglich ist. Wird die Benachrichtigung nach Satz 1 zurückgestellt, sind die Gründe aktenkundig zu machen.

(6) Erfolgt die nach Absatz 5 zurückgestellte Benachrichtigung nicht binnen zwölf Monaten nach Beendigung der Maßnahme, bedürfen weitere Zurückstellungen der gerichtlichen Zustimmung. Das Gericht bestimmt die Dauer weiterer Zurückstellungen. Es kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Sind mehrere Maßnahmen in einem engen zeitlichen Zusammenhang durchgeführt worden, so beginnt die in Satz 1 genannte Frist mit der Beendigung der letzten Maßnahme. Bei Maßnahmen nach den §§ 100b und 100c beträgt die in Satz 1 genannte Frist sechs Monate.

(7) Gerichtliche Entscheidungen nach Absatz 6 trifft das für die Anordnung der Maßnahme zuständige Gericht, im Übrigen das Gericht am Sitz der zuständigen Staatsanwaltschaft. Die in Absatz 4 Satz 1 genannten Personen können bei dem nach Satz 1 zuständigen Gericht auch nach Beendigung der Maßnahme bis zu zwei Wochen nach ihrer Benachrichtigung die Überprüfung der Rechtmäßigkeit der Maßnahme sowie der Art und Weise ihres Vollzugs beantragen. Gegen die Entscheidung ist die sofortige Beschwerde statthaft. Ist die öffentliche Klage erhoben und der Angeklagte benachrichtigt worden, entscheidet über den Antrag das mit der Sache befasste Gericht in der das Verfahren abschließenden Entscheidung.

(8) Sind die durch die Maßnahme erlangten personenbezogenen Daten zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich, so sind sie unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Soweit die Löschung lediglich für eine etwaige gerichtliche Überprüfung der Maßnahme zurückgestellt ist, dürfen die Daten ohne Einwilligung der betroffenen Personen nur zu diesem Zweck verwendet werden; ihre Verarbeitung ist entsprechend einzuschränken.

6.6
Bildaufnahmen bei Versammlungen

Im Zusammenhang mit öffentlicher Kritik an den Ge- und Verboten während der Corona-Pandemie kam es zum Auftreten gleichgesinnter Personen im öffentlichen Raum. Die Bewertung, ob es sich hierbei um „Spaziergänge“ oder „Versammlungen“ handelt, ist auch für die rechtlichen Möglichkeiten zum Herstellen von Bildaufnahmen von Bedeutung.

Während der Corona-Pandemie wurden die erlassenen Regelungen zur Eindämmung des Infektionsgeschehens in der Bevölkerung kontrovers aufgenommen. Die Möglichkeiten für Versammlungen wurden durch die zeitweisen Kontaktverbote, Abstandsregeln und die Maskenpflicht als einschränkend wahrgenommen. Dies führte dazu, dass sich auch in Hessen Menschen zu sogenannten „Corona-Spaziergängen“ zusammenfanden. Die Bewertung, ob es sich im Einzelfall um eine Versammlung oder um einen Spaziergang handelt, ist auch mit Blick auf den Persönlichkeitsrechtsschutz der Teilnehmer relevant.

Spaziergang versus Versammlung

Art 8 GG

(1) Alle Deutschen haben das Recht, sich ohne Anmeldung oder Erlaubnis friedlich und ohne Waffen zu versammeln.

(2) Für Versammlungen unter freiem Himmel kann dieses Recht durch Gesetz oder auf Grund eines Gesetzes beschränkt werden.

Eine Versammlung im Sinn des Art. 8 GG ist eine örtliche Zusammenkunft mehrerer Personen zur gemeinschaftlichen, auf die Teilhabe an der öffentlichen Meinungsbildung gerichteten Erörterung oder Kundgebung. Nach dieser Definition lässt sich eine Versammlung von einem „Spaziergang“ möglicherweise Gleichgesinnter im Einzelfall kaum unterscheiden.

Die staatlichen Eingriffsmöglichkeiten zum Anfertigen von Bild- und Tonaufnahmen bei Versammlungen sind in § 12a in Verbindung mit § 19a des Gesetzes über Versammlungen und Aufzüge (VersG) geregelt. Weiterhin kann jedoch auch § 100h StPO in Betracht kommen. Entscheidend für die Beurteilung, welche Norm zur Anwendung kommen kann, ist der Zweck der Maßnahme. Dieser kann präventiv auf die Gefahrenabwehr oder repressiv auf die Verfolgung von Straftaten und Ordnungswidrigkeiten gerichtet sein.

§ 12a VersG

(1) Die Polizei darf Bild- und Tonaufnahmen von Teilnehmern bei oder im Zusammenhang mit öffentlichen Versammlungen nur anfertigen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von ihnen erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(2) Die Unterlagen sind nach Beendigung der öffentlichen Versammlung oder zeitlich und sachlich damit unmittelbar im Zusammenhang stehender Ereignisse unverzüglich zu vernichten, soweit sie nicht benötigt werden

1. *für die Verfolgung von Straftaten von Teilnehmern oder*
2. *im Einzelfall zur Gefahrenabwehr, weil die betroffene Person verdächtig ist, Straftaten bei oder im Zusammenhang mit der öffentlichen Versammlung vorbereitet oder begangen zu haben, und deshalb zu besorgen ist, dass von ihr erhebliche Gefahren für künftige öffentliche Versammlungen oder Aufzüge ausgehen.*

Unterlagen, die aus den in Satz 1 Nr. 2 aufgeführten Gründen nicht vernichtet wurden, sind in jedem Fall spätestens nach Ablauf von drei Jahren seit ihrer Entstehung zu vernichten, es sei denn, sie würden inzwischen zu dem in Satz 1 Nr. 1 aufgeführten Zweck benötigt.

(3) Die Befugnisse zur Erhebung personenbezogener Informationen nach Maßgabe der Strafprozessordnung und des Gesetzes über Ordnungswidrigkeiten bleiben unberührt.

§ 19a VersG

Für Bild- und Tonaufnahmen durch die Polizei bei Versammlungen unter freiem Himmel und Aufzügen gilt § 12a.

§ 100h StPO

(1) Auch ohne Wissen der betroffenen Personen dürfen außerhalb von Wohnungen

1. *Bildaufnahmen hergestellt werden,*
2. *sonstige besondere für Observationszwecke bestimmte technische Mittel verwendet werden,*

wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger erfolgversprechend oder erschwert wäre. Eine Maßnahme nach Satz 1 Nr. 2 ist nur zulässig, wenn Gegenstand der Untersuchung eine Straftat von erheblicher Bedeutung ist.

(2) Die Maßnahmen dürfen sich nur gegen einen Beschuldigten richten. Gegen andere Personen sind

1. *Maßnahmen nach Absatz 1 Nr. 1 nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre,*
2. *Maßnahmen nach Absatz 1 Nr. 2 nur zulässig, wenn auf Grund bestimmter Tatsachen anzunehmen ist, dass sie mit einem Beschuldigten in Verbindung stehen oder eine solche Verbindung hergestellt wird, die Maßnahme zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes eines Beschuldigten führen wird und dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.*

(3) Die Maßnahmen dürfen auch durchgeführt werden, wenn Dritte unvermeidbar mitbetroffen werden.

(4) § 100d Absatz 1 und 2 gilt entsprechend.

Bild- und Tonaufnahmen nach Versammlungsgesetz (Gefahrenabwehr)

Die versammlungsrechtlichen Regelungen zum Fertigen von Bild- und Tonaufnahmen durch die Polizei sind an bestimmte Voraussetzungen gebunden. Gem. § 12a Abs. 1 VersG müssen „tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von der Versammlung erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen“, damit seitens der Polizei Bild- und Tonaufnahmen gefertigt werden können. Wichtig ist in diesem Zusammenhang, dass von der Polizei eine valide Prognose zur von der Versammlung ausgehenden Gefahr gefordert wird und nicht ein gegen einzelne Personen gerichteter Anfangsverdacht bezüglich der Begehung von rechtswidrigen Taten (d. h. Gefahrenabwehr vs. Strafverfolgung).

Hieraus ergibt sich, dass bei einer Versammlung kein Raum für eine kriminalpräventive Videoüberwachung gem. § 14 Abs. 3 HSOG ist. Die Vorschrift gestattet eine Videoüberwachung durch die Polizei und die Gefahrenabwehrbehörden zur Gefahrenabwehr, auch wenn diese Gefahr nicht als erhebliche Gefahr zu qualifizieren ist. Eine erhebliche Gefahr fordert hingegen § 12a Abs. 1 VersG. Die Eingriffsschwelle ist somit bei Versammlungen deutlich höher. Weiterhin besteht die Möglichkeit zum Fertigen von Bild- und Tonaufnahmen im versammlungsrechtlichen Kontext nur für die Polizei und nicht für andere Gefahrenabwehrbehörden.

Die fest installierten Videoüberwachungen der hessischen Kommunen auf Grundlage des § 14 HSOG, unabhängig davon, ob sie von der Polizei oder einer kommunalen Gefahrenabwehrbehörde betrieben werden, müssen daher bei Versammlungen abgeschaltet werden. Durch die Rechtsprechung wird insoweit eine Erkennbarkeit oder Wahrnehmbarkeit der Abschaltung für die Versammlungsteilnehmer gefordert (OVG Münster (15. Senat), Beschluss vom 2. Juli 2020 – 15 B 950/20; VG Köln (20. Kammer), Beschluss vom 1. Juli 2020 – 20 L 1149/20; VG Köln (20. Kammer), Beschluss vom 29. Mai 2020 – 20 L 968/20).

Bild- und Tonaufnahmen nach StPO (Verfolgung von Straftaten und Ordnungswidrigkeiten)

Gemäß § 12a Abs. 3 VersG bleiben die Befugnisse zur Erhebung personenbezogener Informationen nach Maßgabe der StPO und des OWiG unberührt. Die Regelung des § 100h StPO, der eine Erlaubnis zur Herstellung von Bildaufnahmen außerhalb von Wohnungen darstellt, ist demnach auch im versammlungsrechtlichen Kontext anwendbar. Weiterhin kann § 100h StPO durch die Regelung in § 46 OWIG auch bei der Verfolgung von Ordnungswidrigkeiten zur Anwendung kommen.

Im versammlungsrechtlichen Kontext kommt der Betrachtung der Erforderlichkeit des Herstellens von Bildaufnahmen und damit dem Verhältnismäßigkeitsgrundsatz besondere Bedeutung zu, da in Abgrenzung zu einem Spaziergang durch staatliches Handeln nicht nur in das Recht auf informationelle Selbstbestimmung, sondern auch in die Versammlungsfreiheit eingegriffen wird.

Das Herstellen von Bild- und Tonaufnahmen ist nach § 100h Abs. 1 Satz 1 StPO daher nur zulässig, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten auf andere Weise weniger erfolgversprechend oder erschwert wäre. Im versammlungsrechtlichen Kontext ist daher beispielsweise zu prüfen, ob nicht ggf. eine unmittelbare Feststellung von Personalien ordnungswidrig handelnder oder unterlassender Personen in gleicher Weise eine Verfolgung von Ordnungswidrigkeiten ermöglicht wie das Fertigen von Bildaufnahmen.

Es ist daher von großer Bedeutung, zunächst seitens öffentlicher Stellen nachvollziehbar zu bewerten, ob ein Versammlungscharakter anzunehmen ist. Soweit z. B. von mehreren Personen Transparente präsentiert oder Parolen skandiert werden, weist dies klar auf eine gemeinschaftliche, auf die Teilhabe an der öffentlichen Meinungsbildung gerichtete Erörterung oder Kundgebung und damit auf eine Versammlung hin. Wenn solche offenkundigen Hinweise nicht vorliegen, ist aufgrund der Umstände des Einzelfalls eine nachvollziehbare Entscheidung zu treffen. Im Zweifelsfall erscheint es vor dem Hintergrund der grundgesetzlich garantierten Versammlungsfreiheit und den damit einhergehenden Einschränkungen für staatliches Handeln vorzugswürdig, eine Versammlung anzunehmen.

Sodann ist zu klären, zu welchem Zweck Bildaufnahmen erstellt werden sollen. Konkret ist danach zu fragen, ob es sich um eine Maßnahme der Gefahrenabwehr oder zur Verfolgung von Straftaten und Ordnungswidrigkeiten handelt. Im Falle der Gefahrenabwehr ist die Polizei nach Maßgabe der Voraussetzungen des § 12a Abs. 1 VersG zur Fertigung von Bildaufnahmen berechtigt. § 14 Abs. 3 HSOG wird bei Versammlungen durch die

spezialgesetzliche Regelung des § 12a Abs. 1 VersG verdrängt. Handelt es sich hingegen um eine Maßnahme der Verfolgung von Straftaten oder Ordnungswidrigkeiten, gelangt § 100h StPO zur Anwendung. Neben der Polizei kann hier gemäß § 46 Abs. 1 OWiG auch die zuständige Ordnungswidrigkeitenbehörde tätig werden.

Aufgrund der individuellen Bewertung müssen die vorliegenden Rechtsgrundlagen zur Fertigung von Bildaufnahmen somit unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit und der jeweiligen Normadressaten ausgewählt werden. Aus Gründen der Nachvollziehbarkeit und Transparenz sollte das Vorgehen dokumentiert werden.

7. Allgemeine Verwaltung, Kommunen

Die Arbeit der Landesverwaltung sowie der Verwaltungen der Landkreise, Städte und Gemeinden in Hessen besteht überwiegend in der Verarbeitung personenbezogener Daten. Diese betrifft alle Bürgerinnen und Bürger Hessens. Daher ist es besonders wichtig, dass die Verwaltungstätigkeiten datenschutzrechtlichen Vorgaben entsprechen. Dies ist im weit überwiegenden Umfang der Fall. Dennoch muss ich sowohl die rechtlichen, technischen und organisatorischen Rahmenbedingungen der digitalen Transformation der Verwaltung im Auge behalten und begleiten (Kap. 7.1) als auch die datenschutzrechtlichen Vorgaben für diesen Prozess erläutern (Kap. 7.2 und 7.4). In Einzelfällen gibt es immer wieder Fragestellungen, die beantwortet werden müssen und ein aufsichtsrechtliches Einschreiten erfordern – wie hinsichtlich unzulässiger Datenabfragen (Kap. 7.3), des Erstellens von Fotografien (Kap. 7.5) und von Interessenkonflikten von Datenschutzbeauftragten (Kap. 7.6).

7.1 Digitale Transformation der öffentlichen Verwaltung und Datenschutz

Für eine gelungene Verwaltungsmodernisierung im Kontext der OZG-Umsetzung ist es – neben der qualitativen Verbesserung des Verwaltungshandelns durch Bereitstellung digitaler, effizienter und nutzerfreundlicher Verwaltungsleistungen – notwendig, dass die nutzenden Bürgerinnen und Bürger und die an der digitalen Leistungserbringung mitwirkenden Beschäftigten auf die datenschutzkonforme Ausgestaltung der eingesetzten Mittel und Verfahren vertrauen können. Wesentlicher Baustein einer datenschutzgerechten Umsetzung von Digitalisierungsprojekten ist digitale Souveränität.

Treffender, als es das Bundesverfassungsgericht in seiner Entscheidung zur Volkszählung formuliert hat, kann die Bedeutung des Datenschutzes als Voraussetzung für das Vertrauen in staatliches Handeln kaum formuliert werden:

> „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese

> ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist“ (BVerfG, Urt. vom 15.12.1983 – 1 BvR 209/83 u. a.).

Auch wenn das Volkszählungsurteil 2023 bereits seinen vierzigsten Geburtstag feiert, sind die Aussagen und Wertungen aufgrund der voranschreitenden Digitalisierung aller Lebensbereiche – einschließlich der öffentlichen Verwaltung – heute aktueller denn je. Dies zeigte sich auch anhand der Tätigkeitsfelder, die bei meiner Arbeit im vergangenen Berichtszeitraum einen wesentlichen Schwerpunkt bildeten: die Digitalisierung von Verwaltungsleistungen nach dem Onlinezugangsgesetz (OZG), die Frage der digitalen Souveränität als wesentlicher Erfolgsfaktor für die datenschutzgerechte Umsetzung von IT-Projekten (s. auch Kap. 2) und die Ausweitung von Informations-, Sensibilisierungs- und Beratungsangeboten meiner Behörde.

Zur Notwendigkeit ergänzender Regelungen im OZG

Bereits in meinem letzten Tätigkeitsbericht (50. Tätigkeitsbericht, Kap. 8.1) hatte ich auf die datenschutzrechtlichen Herausforderungen hingewiesen, die es im Zusammenhang mit der Digitalisierung von Verwaltungsleistungen nach dem OZG unter Anwendung des sogenannten „Einer für Alle“ (EfA)-Prinzips zu lösen gilt. Erwähnt hatte ich etwa die folgenden Themenkomplexe:

– Welche Verantwortlichkeiten im Sinn der DS-GVO (Verantwortlichkeit, Gemeinsame Verantwortlichkeit, Auftragsverarbeitung) entstehen zwischen den unterschiedlichen, am Digitalisierungsverfahren beteiligten Akteuren – z. B. die das System entwickelnde Einheit (Land A), die betreibende Einheit (IT-Dienstleister) und die nachnutzende Einheit (Land B, Bund, Kommune)?

– Wie können die hieran anknüpfenden Rechtsfolgen effizient realisiert werden? Bedarf es neuer gesetzlicher Grundlagen oder sind Verträge abzuschließen?
– Müssen für die Verarbeitung personenbezogener Daten im OZG-Kontext neue Rechtsgrundlagen geschaffen werden oder genügen die bereits vorhandenen Rechtsgrundlagen?

In der Praxis hat sich gezeigt: Die datenschutzrechtlichen Fragen der Digitalisierung von Verwaltungsleistungen nach dem EfA-Prinzip lassen sich unter Umständen zwar auch ohne weitere gesetzliche Regelungen durch die von der DS-GVO bereitgestellten Handlungsinstrumente (z. B. den Abschluss von Auftragsverarbeitungsverträgen nach Art. 28 DS-GVO) realisieren. Die hiermit einhergehenden Aufwände sind aber kaum zu überschätzen und bringen für die Umsetzungsverantwortlichen erhebliche Schwierigkeiten mit sich. Im Rahmen meiner Beratung einzelner OZG-Umsetzungsprojekte in Hessen bin ich insbesondere auf die folgenden Probleme gestoßen:

– Die Vielzahl der potenziellen Akteure (Bund, 16 Bundesländer, 294 Landkreise und ca. 11.000 Gemeinden) führt ggf. zur Notwendigkeit des Abschlusses und der Pflege einer Unmenge von – zur datenschutzrechtlichen Legitimation – erforderlichen Verträgen.
– Um dieser Problematik entgegenzuwirken, haben sich in einzelnen Bundesländern unterschiedliche Rechtsauffassungen und „datenschutzrechtliche Umsetzungsmodelle“ herausgebildet, die teilweise nicht miteinander vereinbar sind – wie der Abschluss von Verwaltungsvereinbarungen oder das Modell des Kommunalvertreters.

Durch die komplexe Gemengelage entstehen erhebliche Rechtsunsicherheiten, die in letzter Konsequenz zu Vertrauensverlusten bei Bürgerinnen und Bürgern führen können. Denn wenn schon für die verantwortlichen Akteure selbst die Rechtslage nur schwer zu überblicken ist, wie sollen dann Bürgerinnen und Bürger bei der Inanspruchnahme von digitalisierten Verwaltungsleistungen rechtssicher bestimmen können, wer was wann und bei welcher Gelegenheit über sie weiß?

Dabei liegen Problem und Lösung auf der Hand: Es bedarf ergänzender Regelungen im OZG, die sowohl die Frage der datenschutzrechtlichen Verantwortlichkeit zwischen den beteiligten Akteuren klären als auch zusätzliche Rechtsgrundlagen für die Verarbeitung personenbezogener Daten bieten.

Hierauf hatte die DSK bereits im Herbst 2021 hingewiesen und eine gesetzliche Neuregelung des OZG bis zu Beginn des III. Quartals 2022 gefordert (Protokoll der 102. DSK vom 24. und 25 November 2021, Top 10, https://www.datenschutzkonferenz-online.de/protokolle.html). Um das Gesetzesvorhaben

zu unterstützen, wurde seitens der DSK im Frühjahr 2022 eine Kontaktgruppe OZG 2.0 eingerichtet, in der auch Beschäftigte meiner Behörde mitwirken. Die Kontaktgruppe OZG 2.0 sollte nach dem Willen der DSK Gespräche und Beratungen mit dem Bundesministerium des Innern und für Heimat (BMI) und der Föderalen IT-Kooperation (FITKO) führen und datenschutzrechtliche Anforderungen in das Gesetzgebungsverfahren zum OZG einbringen (Protokoll der 103. DSK vom 23. bis 24 März 2022, Top 14, https://www.datenschutzkonferenz-online.de/protokolle.html).

Leider ist es im Berichtszeitraum nicht gelungen, die dringend notwendigen Neuregelungen zu schaffen. Dies zeichnete sich schon im September 2022 ab. Die DSK stellte daher bereits zu diesem Zeitpunkt fest, dass die rechtlichen Rahmenbedingungen für eine datenschutzkonforme Umsetzung des EfA-Prinzips im OZG weiterhin nicht geschaffen worden seien und durch den zwangsläufigen Rückgriff auf diverse Übergangsregelungen zur Zuweisung der datenschutzrechtlichen Verantwortlichkeit erhebliche datenschutzrechtliche Risiken und Zweifel an der Rechtmäßigkeit des Verwaltungshandelns entstünden. Davon betroffen sei potenziell eine rasch anwachsende Zahl von Bürgerinnen und Bürgern, da in absehbarer Zeit mit der Umsetzung zahlreicher OZG-Leistungen zu rechnen sei (Protokoll der 3. Zwischenkonferenz am 21. September 2022, Top 8, https://www.datenschutzkonferenz-online.de/protokolle.html).

Aktuell bin ich zuversichtlich, dass im kommenden Berichtszeitraum die notwendigen Neuregelungen des OZG verabschiedet werden, da zwischenzeitlich ein Referentenentwurf zum OZG vorliegt (Referentenentwurf des BMI vom 20. Januar 2023, Entwurf eines Gesetzes zur Änderung des OZG sowie weiterer Vorschriften, https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/DE/ozg-2-0-referentenentwurf-ozgaendg.html).

Bis zur Verabschiedung der erforderlichen Vorschriften wird meine Behörde den OZG-Umsetzungsverantwortlichen in Hessen beratend zur Seite stehen und bei der Findung datenschutzrechtskonformer, pragmatischer Übergangslösungen unterstützen.

Bedeutung der digitalen Souveränität für den Datenschutz in Digitalisierungsprojekten

Bereits im vergangenen Berichtszeitraum habe ich zudem auf die besondere Bedeutung der digitalen Souveränität für die datenschutzgerechte Umsetzung von Digitalisierungsprojekten hingewiesen und hier einen Schwerpunkt auf die Rechtsprechung des EuGH zur Übermittlung personenbezogener Daten in Drittländer gelegt (50. Tätigkeitsbericht, Kap. 3). Auch die DSK hat den Stellenwert der digitalen Souveränität für den Datenschutz erkannt und festge-

stellt, dass die gesetzesgebundene Erfüllung der Staatsaufgaben Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten verlangt (Entschließung der DSK, Digitale Souveränität in der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen, 2020, https://www.datenschutzkonferenz-online.de/entschliessungen.html).

Im Frühjahr 2022 hat die DSK – vor dem Hintergrund der zunehmenden Auslagerung von IT-Prozessen in die Cloud auch im öffentlichen Bereich – eine Task Force zum Thema „Souveräne Cloud“ eingerichtet, in der meine Behörde ebenfalls mitarbeitet (Protokoll der 103. DSK vom 23. bis 24 März 2022, Top 9, https://www.datenschutzkonferenz-online.de/protokolle.html). Ziel der Task Force ist es, den Begriff der „Souveränen Cloud“ von anderen Cloud-Angeboten abzugrenzen und wesentliche Anforderungen an „Souveräne Clouds“ zu formulieren. Im November 2022 stellte die Task Force „Souveräne Cloud“ ihre ersten Arbeitsergebnisse vor (Protokoll der 104. DSK vom 22. bis 24. November 2022, Top 11, https://www.datenschutzkonferenz-online.de/protokolle.html), aktuell dauern die Arbeiten an diesem Themenkomplex allerdings noch an. Ich hoffe aber, dass die Ergebnisse der Task Force zukünftig auch bei hessischen Digitalisierungsprojekten eine Hilfestellung bieten können.

Zu meiner Beratung bei der datenschutzgerechten Umsetzung von IT-Projekten im Bereich der hessischen Landesverwaltung und den hierbei erzielten Fortschritten bei der digitalen Souveränität siehe auch Kap. 3.4.

Information, Sensibilisierung und Beratung

Um sicherzustellen, dass Datenschutz als elementarer Baustein einer erfolgreichen Digitalisierung verstanden wird, ist es notwendig, die verschiedenen Mitwirkenden über das Datenschutzrecht zu informieren, für neue Entwicklungen zu sensibilisieren und bei der Lösung komplexer Fragestellungen kooperativ und vertrauensvoll zu beraten. Ich habe meine Informations- und Beratungstätigkeit für den öffentlichen Bereich der öffentlichen Verwaltung im vergangenen Berichtszeitraum daher noch einmal ausgeweitet. So wurde 2022 zum Beispiel gemeinsam mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz und dem Berufsverband der Datenschutzbeauftragten Deutschlands e. V. (BvD) der „1. Datenschutztag Hessen & Rheinland-Pfalz“ veranstaltet (s. Kap. 18), die kommunalen Spitzenverbände wurden anlassbezogen über neue datenschutzrechtliche Entwicklungen mit Auswirkungen auf ihre Tätigkeitsfelder informiert (zum Betrieb von Facebook-Seiten und zur Nutzung von Microsoft 365) und es wurde ein regelmäßiger Austausch zu datenschutzrechtlichen Themenkomplexen mit

den Dienstleistern für Informations- und Kommunikationstechnik der hessischen Landesverwaltung (Hessische Zentrale für Datenverarbeitung) und der Kommunen (ekom21) initialisiert.

7.2
Datenschutz in Kommunen

Im Berichtszeitraum haben mich Anfragen und Beschwerden hinsichtlich verschiedener Bereiche der Kommunalverwaltung erreicht. Im Folgenden werden mehrere ausgewählte Themenkomplexe aus der Aufsichtspraxis näher beleuchtet. Wenngleich die umfangreichen datenschutzrechtlichen Anforderungen durch die hessischen Kommunen in der täglichen Praxis überwiegend eingehalten werden, sind auch einzelne Verstöße gegen den Datenschutz zu verzeichnen.

Keine Datenverarbeitung ohne Rechtsgrundlage

Die Verarbeitung personenbezogener Daten ist nach Art. 5 Abs. 1 Buchst. a und Art. 6 DS-GVO nur rechtmäßig, sofern für die jeweilige Verarbeitung eine Rechtsgrundlage einschlägig ist. Dieser zentrale datenschutzrechtliche Grundsatz ist auch im kommunalen Bereich stets zu berücksichtigen. Im Laufe des Berichtszeitraumes gelangten mir mehrere diesbezügliche Verstöße zur Kenntnis:

Art. 5 DS-GVO

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“)

(…)

Art. 6 DS-GVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(…)

Übermittlung personenbezogener Daten zwischen (kreisangehöriger) Kommune und Landkreis

Für eine Übermittlung personenbezogener Daten zwischen (kreisangehöriger) Kommune und Landkreis (etwa zwischen der Versammlungsbehörde einer Gemeinde und der Ordnungs- und Kommunalaufsichtsbehörde eines Landkreises) bedarf es stets einer datenschutzrechtlichen Rechtsgrundlage. Die Stellung des Landrats als Aufsichtsbehörde nach § 136 Abs. 3 HGO und § 86 Abs. 1 Nr. 3 HSOG begründet an sich noch keine Befugnis für eine Datenübermittlung.

§ 136 HGO

(…)

(3) Aufsichtsbehörde der übrigen Gemeinden ist der Landrat als Behörde der Landesverwaltung, obere Aufsichtsbehörde der Regierungspräsident.

(…)

§ 86 HSOG

(1) Aufsichtsbehörden sind

(…)

3. für die örtlichen Ordnungsbehörden in den übrigen Gemeinden der Landrat, das Regierungspräsidium und die zuständigen Ministerien.

(…)

Datenübermittlung einer Gemeindebehörde an den Vorsitzenden der Gemeindevertretung

Auch die Datenübermittlung seitens der Behörde einer Gemeinde oder eines Landkreises an den Vorsitzenden der Gemeindevertretung oder des Kreistages bedarf stets einer Rechtsgrundlage. Dies kann etwa § 22 Abs. 1 HDSIG sein. Dafür muss die Übermittlung jedoch zum einen zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle (hier der Behörde einer Gemeinde oder eines Landkreises) oder des Dritten, an den die Daten übermittelt werden, (hier Vorsitzende der Gemeindevertretung bzw. des Kreistages) liegenden Aufgaben erforderlich sein. Zum anderen müssen die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 HDSIG zulassen würden (etwa sofern Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, oder die Verarbeitung der Wahrnehmung von Aufsichts- und Kontrollbefugnissen dient).

§ 22 HDSIG

(1) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden. Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist unter den Voraussetzungen des § 21 zulässig.

(…)

§ 21 HDSIG

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn

1. *offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,*
2. *Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,*
3. *sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder Ordnung, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- oder Zollaufkommens erforderlich ist,*
4. *sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Straf-*

gesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,

5. *sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist oder*
6. *sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.*

(…)

Äußerungen in Sitzungen von kommunalen Gremien

Bei Äußerungen in Sitzungen insbesondere von Gemeindevertretungen und Kreistagen muss (zumal sofern diese mit der Arbeit in dem Gremium nicht unmittelbar zusammenhängen) ggf. hinterfragt werden, ob eine namentliche Bezeichnung des Mitglieds erforderlich ist oder es nicht vielmehr ausreicht, diese oder diesen etwa als „Mitglied der Fraktion x“ zu benennen. Wenngleich auch personenbezogene (zugespitzte) Äußerungen im Rahmen des politischen Meinungskampfes zulässig sind, ist zu berücksichtigen, dass infolge des Grundsatzes der Sitzungsöffentlichkeit von einer hohen Breitenwirkung derartiger Äußerungen – ggf. auch in den Medien und über das Internet – auszugehen ist und die betroffene Person daher mit etwaigen negativen Konsequenzen außerhalb der kommunalen Tätigkeit konfrontiert sein könnte. Solche personenbezogenen Äußerungen können daher das Persönlichkeitsrecht der betroffenen Person verletzen.

Amtshilfe ist keine Rechtsgrundlage

Die Vorschriften über die Amtshilfe, etwa in §§ 4 ff. HVwVfG, stellen keine taugliche Rechtsgrundlage für eine Übermittlung personenbezogener Daten dar. Dies ist schon deshalb der Fall, da diese eine Datenverarbeitung nicht regeln und die Maßgaben des Art. 6 Abs. 3 DS-GVO nicht erfüllen.

§ 4 HVwVfG

(1) Jede Behörde leistet anderen Behörden auf Ersuchen ergänzende Hilfe (Amtshilfe).

(2) Amtshilfe liegt nicht vor, wenn

1. *Behörden einander innerhalb eines bestehenden Weisungsverhältnisses Hilfe leisten;*
2. *die Hilfeleistung in Handlungen besteht, die der ersuchten Behörde als eigene Aufgabe obliegen.*

Art. 6 DS-GVO

(…)

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(…)

Übermittlung personenbezogener Daten seitens Kommunen an Rechtsanwälte

Eine Übermittlung personenbezogener Daten seitens einer Kommune an einen Rechtsanwalt oder eine Rechtsanwältin als nicht öffentliche Stelle kann insbesondere zulässig sein, sofern ein Tatbestand des § 22 Abs. 2 HDSIG einschlägig ist.

§ 22 HDSIG

(…)

(2) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nicht öffentliche Stellen ist zulässig, wenn

1. *sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden,*
2. *der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder*

3. es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

(…)

Dahingehend ist ausdrücklich darauf hinzuweisen, dass die Übermittlung nicht alleine deshalb zulässig ist, weil Rechtsanwälte nach § 2 der Berufsordnung für Rechtsanwälte (BORA) zur Verschwiegenheit verpflichtet sind.

§ 2 BORA

(1) Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet und berechtigt. Dies gilt auch nach Beendigung des Mandats.

(…)

Datenübermittlungen durch die Meldebehörden

Im Berichtszeitraum erreichten mich – wie auch in den vorherigen Jahren – mehrere Anfragen und Beschwerden, die Datenübermittlungen durch Meldebehörden betreffen.

Die Meldebehörden dürfen personenbezogene Daten in vielen Fallkonstellationen verarbeiten. Gleichwohl stehen betroffenen Personen mehrere Rechte zu, um eine Datenübermittlung sperren oder einschränken zu lassen. Betroffene Personen können sich auf meiner Webseite über die Regelungen informieren (Auskunftssperren und mehr, Rechte der Betroffenen bei Meldebehörden; abrufbar unter https://datenschutz.hessen.de/datenschutz/kommunen/rechte-der-betroffenen-bei-meldebehoerden).

Wenngleich Datenschutzverstöße durch die Meldebehörden in meiner aufsichtsrechtlichen Praxis nur selten festzustellen sind, kam es in Einzelfällen zu rechtswidrigen Übermittlungen. Beispielhaft soll dies folgender Fall illustrieren:

Ein Rechtsanwalt begehrte eine erweiterte Melderegisterauskunft über den Mieter seiner Mandantin, insbesondere auch hinsichtlich der Wohnanschrift der getrennt lebenden Ehefrau des Mieters. Der Mieter hatte Mietforderungen nicht beglichen. Die Ehefrau selbst war nicht Vertragspartnerin des Mietvertrages.

Eine erweiterte Melderegisterauskunft kann gemäß § 45 BMG über verschiedene personenbezogene Daten erteilt werden, „soweit ein berechtigtes

Interesse glaubhaft gemacht wird“. Diese enthält ggf. auch „Familienname und Vornamen sowie Anschrift des Ehegatten oder des Lebenspartners“.

§ 45 BMG

(1) Soweit ein berechtigtes Interesse glaubhaft gemacht wird, darf zu den in § 44 Absatz 1 genannten Daten einzelner bestimmter Personen eine erweiterte Melderegisterauskunft erteilt werden über

1. *frühere Namen,*
2. *Geburtsdatum und Geburtsort sowie bei Geburt im Ausland auch den Staat,*
3. *Familienstand, beschränkt auf die Angabe, ob verheiratet oder eine Lebenspartnerschaft führend oder nicht,*
4. *derzeitige Staatsangehörigkeiten,*
5. *frühere Anschriften,*
6. *Einzugsdatum und Auszugsdatum,*
7. *Familienname und Vornamen sowie Anschrift des gesetzlichen Vertreters,*
8. *Familienname und Vornamen sowie Anschrift des Ehegatten oder des Lebenspartners sowie*
9. *Sterbedatum und Sterbeort sowie bei Versterben im Ausland auch den Staat.*

(…)

Unter einem „berechtigten Interesse“ ist jedes von der Rechtsordnung erlaubte Interesse rechtlicher, wirtschaftlicher oder auch ideeller Art zu verstehen. Dieses muss nach Abwägung für jedes einzelne Datum („soweit“) gegenläufige schutzwürdige Interessen der betroffenen Person an der Nichtoffenbarung der Meldedaten überwiegen (Schwabenbauer, in: Engelbrecht/Schwabenbauer, BMG § 45 Rn. 6).

Das Wort „soweit“ macht deutlich, dass sich das berechtigte Interesse auf jedes einzelne Datum, über welches Auskunft begehrt wird, beziehen muss. Werden Name und Anschrift des Ehegatten des Betroffenen verlangt, § 45 Abs. 1 Nr. 8 BMG, ist besonders sorgfältig zu prüfen, ob hierfür ein berechtigtes Interesse besteht (denkbar etwa wegen Ehegattenhaftung nach § 1357 BGB) (Schwabenbauer, in: Engelbrecht/Schwabenbauer, BMG § 45 Rn. 15).

In diesem Fall erachtete die Meldebehörde ein „berechtigtes Interesse“ als gegeben und erteilte eine erweiterte Melderegisterauskunft, die sämtliche in § 45 Abs. 1 BMG genannten personenbezogenen Daten enthielt. Dabei wurde jedoch verkannt, dass zwar ein rechtliches und wirtschaftliches Interesse hinsichtlich der personenbezogenen Daten des säumigen Mieters bestand, derartige Interessen bezogen auf die personenbezogenen Daten der Ehefrau jedoch nicht ersichtlich waren. Insoweit wurde das Ermessen seitens der Meldebehörde fehlerhaft ausgeübt.

Die erteilte Auskunft auch über Name und Anschrift der Ehefrau hatte zudem spürbare Auswirkungen. Mehrere Personen erschienen persönlich vor der Wohnung der Ehefrau, verlangten die ausstehende Miete des getrennt lebenden Ehemannes und drangen damit ohne Rechtsgrund in deren persönliche Lebenssphäre ein.

Datenschutz bei Wertstoffhöfen

Wertstoffhöfe (Recyclinghöfe) sind häufig als kommunale Eigenbetriebe organisiert. Diesbezüglich ist zu berücksichtigen, dass diese nach § 2 Abs. 2 HDSIG als nicht öffentliche Stellen gelten, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

Folge dessen ist, dass die Vorschriften des HDSIG ganz überwiegend ausgeschlossen sind und stattdessen die für nicht öffentliche Stellen geltenden Vorschriften des BDSG Anwendung finden.

§ 2 HDSIG

(…)

(2) Öffentliche Stellen gelten als nicht öffentliche Stellen, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Insoweit finden die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes und die §§ 5 bis 18 und 23 Anwendung.

(…)

Datenschutzrechtlich bedeutsam ist insbesondere die Verarbeitung des Kfz-Kennzeichens und des Personalausweises der Einwohnerinnen und Einwohner.

Der Wertstoffhof einer Kommune ist regelmäßig nur für die Entsorgung des Abfalls der Einwohnerinnen und Einwohner der betreffenden Kommune zuständig. Eine diesbezügliche Regelung findet sich häufig in einer kommunalen Satzung, etwa in § 3 der Abfallsatzung des Wetteraukreises.

„§ 3 Abfallsatzung des Wetteraukreises

(1) Zur Benutzung der Abfallentsorgungsanlagen des Wetteraukreises sind die kreisangehörigen Gemeinden außer Bad Vilbel berechtigt, soweit diese Satzung nichts anderes bestimmt.

(2) Der Besitzer/die Besitzerin, dessen/deren Abfälle vom Einsammeln und Befördern durch eine kreisangehörige Gemeinde ausgeschlossen sind, ist nach Maßgabe dieser Satzung berechtigt, die bei

ihm/ihr angefallenen Abfälle dem Wetteraukreis unmittelbar bei den dafür zugelassenen Abfallentsorgungsanlagen zum Zwecke des Behandelns, Lagerns und Ablagerns zu überlassen. Diese Regelung gilt nicht für Abfälle, die gemäß § 2 von der Entsorgung ausgeschlossen sind.

(3) Der Wetteraukreis nimmt an den Recyclinghöfen in Echzell, Friedberg/Bad Nauheim und Niddatal Abfälle aus privaten Haushaltungen des Wetteraukreises außer Bad Vilbel an. Über die Benutzung der Recyclinghöfe, die Abfallarten und die Erhebung von Gebühren erlässt der Kreistag eine gesonderte Satzung.

(4) Werden Abfälle nicht sortenrein gemäß den Vorgaben des § 1 Abs. 4 Satz 2 angeliefert, so entscheidet der Wetteraukreises über die weitere Verwertung oder Beseitigung der Abfälle."

Beschäftigte des Wertstoffhofes können das Kfz-Kennzeichen des Anliefernden kontrollieren, um sicherzustellen, dass nur Abfälle von Einwohnerinnen und Einwohnern der betreffenden Kommune angenommen werden. Bei kreisfremden Kfz-Kennzeichen ist es datenschutzrechtlich zulässig, den Personalausweis des Fahrers zu kontrollieren, um feststellen zu können, ob es sich eventuell doch um einen Einwohner des betreffenden Landkreises handelt. Die Verarbeitung hat sich regelmäßig auf eine bloße Sichtkontrolle zu beschränken. Eine Speicherung etwa mittels Kopie oder Foto des Kfz-Kennzeichens oder des Personalausweises ist dagegen grundsätzlich nicht zulässig. Eine Ausnahme ist lediglich im Falle von besonderen Vorkommnissen statthaft. Beispielhaft ist die Durchsetzung eines Hausverbotes für einen bestimmten Fahrer zu nennen (s. zur Müllbeseitigung auch Kap. 7.5).

Handreichung für den Datenschutz in Kommunen

Zwecks Unterstützung bei der Umsetzung des Datenschutzes habe ich Informationen für Kommunen auf meiner Webseite zur Verfügung gestellt (abrufbar unter https://datenschutz.hessen.de/datenschutz/kommunen/datenschutz-in-kommunen). Dort können kommunale Datenschutzbeauftragte und Beschäftigte einen ersten Überblick zu verschiedenen Thematiken erhalten (z. B. zu Verarbeitung personenbezogener Daten; Rechte der betroffenen Personen, Auskunft nach Art. 15 ff. DS-GVO; Auftragsverarbeitung, Art. 28 DS-GVO, und gemeinsame Verantwortlichkeit, Art. 26 DS-GVO).

7.3
Mitarbeiterexzess durch Datenabfragen im Kraftfahrzeugregister

Nachdem in der Vergangenheit in den Medien mehrfach über rechtswidrige Abfragen durch Polizeibedienstete berichtet wurde, zeigt sich am nachfolgenden Sachverhalt, dass die Problematik auch in Kommunalverwaltungen bestehen kann.

Rechtswidrige Abfragen in Dateisystemen waren in den vergangenen Jahren vorwiegend im polizeilichen Kontext Gegenstand von datenschutzrechtlichen Aufsichts- oder Bußgeldverfahren. Automatisierte Abrufmöglichkeiten auf Daten des Zentralen Verkehrsinformationssystems ZEVIS, das vom Kraftfahrt-Bundesamt betrieben wird, bestehen jedoch auch bei den kommunalen Ordnungsämtern. ZEVIS wird insbesondere genutzt, um im Rahmen von Verfahren zu Verkehrsordnungswidrigkeiten festzustellen, wer Halter eines Kraftfahrzeugs ist („Halterdaten"). Das Dateisystem ZEVIS unterliegt dabei den Vorschriften zur Protokollierung gem. § 36 Abs. 6 Straßenverkehrsgesetz (StVG). Alle Zugriffe auf die in ZEVIS gespeicherten Datensätze werden protokolliert und sind daher nachvollziehbar.

§ 36 Abs. 6 StVG

(6) Das Kraftfahrt-Bundesamt oder die Zulassungsbehörde als übermittelnde Stelle hat über die Abrufe Aufzeichnungen zu fertigen, die die bei der Durchführung der Abrufe verwendeten Daten, den Tag und die Uhrzeit der Abrufe, die Kennung der abrufenden Dienststelle und die abgerufenen Daten enthalten müssen. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden. Die nach Satz 1 protokollierten Daten dürfen auch dazu verwendet werden, der betroffenen Person darüber Auskunft zu erteilen, welche ihrer in Anhang I, Abschnitt I und II der Richtlinie (EU) 2015/413 enthaltenen personenbezogenen Daten an Stellen in anderen Mitgliedstaaten der Europäischen Union zum Zweck der dortigen Verfolgung der in Artikel 2 der Richtlinie (EU) 2015/413 aufgeführten, die Straßenverkehrssicherheit gefährdenden Delikte übermittelt wurden. Das Datum des Ersuchens und die zuständige Stelle nach Satz 1, an die die Übermittlung erfolgte, sind der betroffenen Person ebenfalls mitzuteilen. § 36a gilt für das Verfahren nach den Sätzen 3 und 4 entsprechend. Liegen Anhaltspunkte dafür vor, dass ohne ihre Verwendung die Verhinderung oder Verfolgung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person aussichtslos oder wesentlich erschwert wäre, dürfen die Daten auch für diesen Zweck verwendet werden, sofern das Ersuchen der Strafverfolgungsbehörde unter Verwendung von Halterdaten einer bestimmten Person oder von Fahrzeugdaten eines bestimmten Fahrzeugs gestellt wird. Die Protokolldaten sind durch geeignete Vorkehrungen gegen zweckfremde Verwendung und gegen sonstigen Missbrauch zu schützen und nach sechs Monaten zu löschen.

Ein Bürger führte bei mir Beschwerde darüber, dass nach seiner Vermutung eine ehemalige Liebschaft eine Halteranfrage zu seinem Kraftfahrzeug ausgelöst habe. Das Verhältnis zwischen den Beteiligten war über eine Dating-Plattform zustande gekommen und – zumindest seitens des Beschwerdeführers – nicht auf Dauer angelegt. Aus „Datenschutzgründen“ verzichtete der Beschwerdeführer daher auch auf die Preisgabe seines tatsächlichen Namens, zumal parallel eine feste Beziehung zu einer Lebensgefährtin bestand, die nach dem Willen des Beschwerdeführers durch die Liebschaft nicht belastet werden sollte.

Das über die Dating-Plattform zustande gekommene Verhältnis wurde offenbar nicht einvernehmlich beendet und löste so bei den Beteiligten enttäuschte Erwartungen und vor allem auch Reaktionen aus. Nach Prüfung der möglichen Handlungsalternativen – so darf an dieser Stelle unterstellt werden – wurde seitens der verlassenen Dame der Entschluss gefasst, die dauerhafte Lebensgefährtin des Beschwerdeführers über die Aktivitäten ihres Partners zu informieren.

Dies war angesichts des zurückhaltenden Umgangs des Beschwerdeführers mit seinen personenbezogenen Daten keine leichte Aufgabe. Als Ansatz für die „Ermittlung“ des tatsächlichen Namens diente das Kennzeichen des Fahrzeugs, mit dem der Beschwerdeführer zu den amourösen Abenteuern erschienen war. Eine unmittelbare Möglichkeit, die begehrten Daten zu erhalten, bot sich für die Dame mangels Zugriff auf ZEVIS nicht. Sie kannte aber eine Person, die in guter Position für die Kommunalverwaltung (erster Stadtrat) tätig war und bat diese, ihr die personenbezogenen Daten des Fahrzeughalters zu beschaffen. Aufgrund der Anfrage des ersten Stadtrats veranlasste daraufhin ein Mitarbeiter der Kommunalverwaltung die Halterfeststellung und übermittelte die Daten des Beschwerdeführers. Die enttäuschte Dame nutzte die gewonnenen Informationen, um den Beschwerdeführer und seine Lebensgefährtin in sozialen Netzwerken ausfindig zu machen und letztgenannte über die Untreue ihres Partners zu informieren. Wenig überraschend wurde der Beschwerdeführer von seiner Lebensgefährtin damit konfrontiert, was einmal mehr die jeweiligen Erwartungen enttäuschte und letztlich die Beschwerde bei meiner Behörde zur Folge hatte.

Da amtliche Kfz-Kennzeichen als personenbeziehbare Daten den datenschutzrechtlichen Regelungen unterliegen, wäre – dem Grundsatz der Rechtmäßigkeit nach Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 DSGVO entsprechend – für den Abruf der Daten des Fahrzeughalters eine Rechtsgrundlage oder aber die Einwilligung des Beschwerdeführers erforderlich gewesen.

Durch die Überprüfung der Protokolldaten zum Abruf der Halterdaten des Beschwerdeführers konnte die im fraglichen Zeitfenster erfolgte Abfrage durch die Kommunalverwaltung ermittelt und nachgewiesen werden, dass der Abruf räumlich und sachlich nicht im Kontext einer zuständigen Befassung, z. B. der Verfolgung von Verkehrsordnungswidrigkeiten, stand. Die Abfrage war somit rechtswidrig, da die Datenverarbeitung gem. Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 Abs. 1 DS-GVO rechtsgrundlos erfolgte.

Im Weiteren konnte der erste Stadtrat, der die Anfrage offenbar aus Gefälligkeit ausgelöst und die personenbezogenen Daten des Beschwerdeführers weitergegeben hatte, identifiziert werden. Er gab im Rahmen der Anhörung im Bußgeldverfahren den Verstoß zu. Gegen den ersten Stadtrat wurde ein Bußgeldbescheid über 350 € erlassen. Der Bescheid ist rechtskräftig.

7.4
Anforderungen an Dokumentenabholboxen

In mehreren hessischen Städten und Gemeinden sind in den vergangenen beiden Jahren sog. „Dokumentenabholboxen" aufgestellt worden. Dort können Bürgerinnen und Bürger verschiedene Dokumente (z. B. Personalausweise und Reisepässe, Personenstandsurkunden, Fundsachen) auch außerhalb der Öffnungszeiten des Bürgerbüros abholen. Dieses als grundsätzlich bürgerfreundlich einzustufende Angebot muss allerdings die datenschutzrechtlichen Anforderungen vollständig erfüllen.

Die deutschlandweit erste Dokumentenabholbox wurde im Jahr 2019 in der Stadt Ludwigsburg in Baden-Württemberg aufgestellt. Inzwischen sind auch in Hessen mehrere Boxen installiert, etwa in Wiesbaden, Hanau und Bensheim.

Funktionsweise und Prozess der Dokumentenabholbox

In Wiesbaden steht neben dem Bürgerbüro in der Marktstraße 18 seit März 2021 die sog. „WI-Box" als Abholstation des Ordnungsamtes Wiesbaden. Ich habe mir die Funktionsweise und den Prozess beginnend von der Reservierung bis zur Abholung von Dokumenten von Beschäftigten des Bürgerbüros bei einem Vor-Ort-Termin im August 2022 vorführen lassen.

Die „WI-Box" besteht aus zwei getrennten Boxen, deren Funktionsweise Abholstationen von Lieferdiensten ähnelt. Die Boxen sind videoüberwacht und besonders gesichert. Sofern man etwa einen Personalausweis im Bürgerbüro bestellt, kann dieser anstelle einer Abholung im Bürgerbüro während der Öffnungszeiten an der „WI-Box" täglich an 24 Stunden abgeholt werden.

Der Hersteller sowohl der Boxen als auch der für ihre Nutzung entwickelten Software ist die schweizerische Kern AG.

An der einen Box, die über 46 Fächer verfügt, können bestellte Personalausweise und Reisepässe abgeholt werden. Dafür müssen zunächst ein Fingerabdruck im Bürgerbüro eingescannt und weitere Daten (Name, Vorname, Adresse, E-Mail-Adresse) angegeben werden. Der Fingerabdruck wird mittels des Gerätes der Bundesdruckerei gescannt, das auch für die Abnahme der Fingerabdrücke für die Ausweisdokumente verwendet wird. Die genutzte Software-Anwendung, die von dem Hersteller der Box entwickelt wird, ist unabhängig von der Software für den Scan des Fingerabdruckes für den Personalausweis.

Die Verarbeitung der personenbezogenen Daten erfolgt durch die Software des Herstellers der Box, die auf Servern der Stadt Wiesbaden lokal ausgeführt wird. Es erfolgt keine Übermittlung der Daten an Dritte. Sämtliche Daten werden spätestens sieben Tage nach Bereitstellung der Dokumente gelöscht (s. u.). Nach der Registrierung wird zuerst eine Bestätigungs-E-Mail an die angegebene E-Mail-Adresse versendet. Die Einlage der Dokumente in die „WI-Box“ erfolgt durch entsprechend geschulte Beschäftigte des Bürgerbüros nach dem Vier-Augen-Prinzip. Diese authentifizieren sich dazu über eine RFID/NFC-Karte. Sobald der Ausweis in der „WI-Box“ zur Abholung bereitliegt, erhält die antragstellende Person über eine zweite E-Mail einen TAN-Code als Nummer und QR-Code.

Als weiteres Verfahren bietet der Hersteller die Funktion an, den Code per SMS zuzusenden. Die E-Mail enthält keine weiteren Daten, sondern lediglich die Information, dass ein Dokument (Ausweis) zur Abholung bereitliegt. An der „WI-Box“ kann man sodann entweder den Code einscannen oder manuell eingeben sowie den Fingerabdruck einscannen (zwei getrennte Faktoren für Authentifikation).

An der anderen Box können Personenstandsurkunden sowie andere Unterlagen und Fundsachen abgeholt werden. Dafür wird der Fingerabdruck nicht benötigt. Zu der Abholung genügt der TAN-Code, den man per E-Mail erhält. Die Dokumente oder Fundsachen verbleiben für maximal sieben Tage in der „WI-Box“. Sofern die Dokumente innerhalb dieses Zeitraumes nicht abgeholt werden, werden sie von Beschäftigten des Bürgerbüros aus der „WI-Box“ entnommen und zurück in das Bürgerbüro verbracht. Der eingescannte Fingerabdruck sowie die weiteren Daten der Bürgerinnen und Bürger werden bei Abholung des Dokumentes oder spätestens nach Ablauf der sieben Tage gelöscht.

Im Falle einer weiteren Abholung müssen der Fingerabdruck und die weiteren Daten erneut erfasst werden.

Die „WI-Box“ wird nach Angaben der Stadt Wiesbaden seitens der Bürgerinnen und Bürger bereits häufig genutzt. Seit der Aufstellung im März 2021 sei das System für die Abholung von ca. 1.200 Ausweisdokumenten verwendet worden (Stand August 2022). Die zur Abholung angebotenen Dokumente sollen zudem kontinuierlich erweitert werden. Auch viele andere hessische Kommunen zeigten Interesse und würden sich nach den gesammelten Erfahrungen erkundigen.

Datenschutzrechtliche Fragestellungen

Wenngleich Dokumentenabholboxen wie die „WI-Box“ insbesondere vor dem Hintergrund der fortschreitenden Digitalisierung der Verwaltung als bürgerfreundlich zu begrüßen sind, muss den Anforderungen des Datenschutzes umfassend entsprochen werden. Auch um etwaigen späteren Mehraufwand zu vermeiden, sollten die datenschutzrechtlichen Maßgaben von Beginn an mitbedacht und fortlaufend überprüft werden. Dahingehend sind insbesondere die folgenden Leitlinien zu berücksichtigen.

Verarbeitung von Fingerabdrücken als biometrische Daten

Sofern bei dem Beantragungs- und Abholungsprozess (wie bei der „WI-Box“) eine Abnahme von Fingerabdrücken stattfindet, werden biometrische Daten verarbeitet. Diese sind gemäß Art. 4 Nr. 14 DS-GVO „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen“. Die Verarbeitung „biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person“ als Verarbeitung besonderer Kategorien personenbezogener Daten im Sinn des Art. 9 DS-GVO (s. DSK, Kurzpapier Nr. 17 – Besondere Kategorien personenbezogener Daten, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_17.pdf) bedarf grundsätzlich einer ausdrücklichen Einwilligung der betroffenen Person in die Verarbeitung des Fingerabdruckes für einen festgelegten Zweck (Identifikation der betroffenen Person zur Abholung des Personalausweises) gem. Art. 9 Abs. 2 Buchst. a DS-GVO.

Art. 4 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

(…)

14. „biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

(…)

Art. 9 DS-GVO

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten,

biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

(…)

Anforderungen an die Einwilligungserklärung

Die Einwilligungserklärung muss zudem den Anforderungen des Art. 7 DS-GVO entsprechen (s. EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf; sowie DSK, Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf). Diesbezüglich sind insbesondere die Informiertheit der betroffenen Person, die jederzeitige Widerruflichkeit sowie die Freiwilligkeit der erteilten Einwilligung zu berücksichtigen. Ferner hat eine klare Trennung zwischen der Verarbeitung eines Fingerabdruckes und der Verarbeitung weiterer „einfacher" personenbezogener Daten (Name, E-Mail-Adresse etc.) zu erfolgen.

Art. 7 DS-GVO

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Informationspflicht

Die betroffenen Personen sind nach Art. 13 DS-GVO über die Datenverarbeitungen zu informieren (s. Art. 29-Datenschutzgruppe, Guidelines on transparency under Regulation 2016/679, https://ec.europa.eu/newsroom/article29/redirection/document/51025, sowie DSK, Kurzpapier Nr. 10 – Informationspflichten bei Dritt- und Direkterhebung, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf). Zu den Informationsinhalten zählen insbesondere auch „die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung".

Dahingehend ist zwischen der Verarbeitung von Fingerabdrücken (Art. 9 DS-GVO) und der Verarbeitung der weiteren personenbezogenen Daten wie Name und E-Mail-Adresse (Art. 6 DS-GVO) zu differenzieren. Für die Verarbeitung der weiteren Daten ist eine „einfache" Einwilligung entsprechend Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 DS-GVO erforderlich.

Da die Dokumentenabholbox ein zusätzliches, gesetzlich nicht geregeltes Angebot darstellt, ist weder eine „rechtliche Verpflichtung" im Sinn des Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO noch eine Erforderlichkeit der Verarbeitung für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe nach Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO anzunehmen. Die Informationen sollten sowohl an der Dokumentenabholbox als Aushang vor Ort als auch auf der Webseite der Kommune erteilt werden.

Art. 13 DS-GVO

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;

b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;

c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;

d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;

c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;

d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(…)

Datenschutz-Folgenabschätzung

Die Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO ist nicht ganz eindeutig, jedoch grundsätzlich anzunehmen. Dafür sprechen nach Art. 35 Abs. 1 und 3 Buchst. b DS-GVO der große Umfang der Datenverarbeitung (potenziell sämtliche Einwohnerinnen und Einwohner der jeweiligen Kommune), die Verarbeitung der Daten von schutzbedürftigen Betroffenen (Machtungleichgewicht zwischen der Kommune und den Einwohnerinnen und Einwohnern; Minderjährige), die Verarbeitung auch besonderer Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO sowie die mit der Verarbeitung der Fingerabdrücke einhergehenden Missbrauchsgefahren (s. u.) (s. Art. 29-Datenschutzgruppe, Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt", insbesondere S. 9 ff., https://www.datenschutz-bayern.de/technik/orient/wp248.pdf; sowie DSK, Kurzpapier Nr. 5 – Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf).

Art. 35 DS-GVO

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(…)

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(…)

Technische und organisatorische Maßnahmen

Des Weiteren sind geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO (insbesondere hinsichtlich der Verarbeitung der Fingerabdrücke als biometrisches Datum) zu ergreifen, um ein dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes Schutzniveau zu gewährleisten (s. DSK, Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf).

Art. 32 DS-GVO

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(…)

Bei der Abholung von Personenstandsurkunden sowie von anderen Unterlagen und Fundsachen ist es infolge des Medienbruchs als zusätzlicher Sicherheitsfaktor begrüßenswert, wenn Einwohnerinnen und Einwohner die Möglichkeit erhalten, ihre Mobilfunknummer anzugeben, um – zusätzlich zu einer E-Mail – auch eine SMS erhalten zu können.

Die zu der Abholung von Ausweisen – zusätzlich zu der erforderlichen Abnahme des Fingerabdruckes – möglichen Verfahren E-Mail- oder SMS-Versand sind als gleichwertig zu qualifizieren.

Da aufgrund der leichten Zugänglichkeit zu E-Mail-Postfächern und Fingerabdrücken im häuslich-familiären Umfeld etwaige Missbräuche nicht

auszuschließen sind, sollte entsprechend Art. 32 Abs. 2 DS-GVO eine Risikoanalyse und -bewertung erfolgen, welche auf realistisch möglichen Missbrauchs-Szenarien basiert.

Die Verarbeitung der Fingerabdrücke als biometrisches Datum sollte auf einem dem Risiko angemessenen Schutzniveau erfolgen (u. a. durch ein IT-Sicherheitskonzept und ein Rollen- und Berechtigungskonzept) und entsprechend Art. 24 und Art. 5 Abs. 2 DS-GVO nachgewiesen werden können. Insofern darf – wenngleich der Prozess für die Bürgerinnen und Bürger eine anwendungsfreundliche Methode darstellt – nicht verkannt werden, dass die Abnahme von Fingerabdrücken für Fälschungen durchaus anfällig ist.

Dahingehend sind zwei Aspekte relevant: zum einen die nicht autorisierte Abholung von Ausweisdokumenten aus der Dokumentenabholbox mittels eines gefälschten Fingerabdrucks. Dafür ist das Schutzniveau des Fingerabdruckscanners an der Dokumentenabholbox gegen gefälschte Fingerabdrücke maßgeblich (vor allem hinsichtlich des Erkennens und Abwehrens von verbreiteten und einfach durchzuführenden Angriffen).

Zum anderen die Kompromittierung im Sinn einer Offenlegung der gespeicherten Fingerabdrücke gegenüber unberechtigten Dritten oder der Öffentlichkeit. Insofern ist relevant, welche Fingerabdruckdaten genau erfasst und gespeichert werden (eine grafische Repräsentation des Fingerabdrucks, die für eine Fälschung oder Nutzung bei anderen Systemen genutzt werden kann, oder extrahierte Fingerabdruckmerkmale, die nicht ohne weiteres für andere Zwecke missbraucht werden können (s. DSK, Positionspapier zur biometrischen Analyse https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_positionspapier_biometrie.pdf).

Hinsichtlich des E-Mail-Versands seitens der Kommune an Bürgerinnen und Bürger ist die Orientierungshilfe der DSK „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ (abrufbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf) zu berücksichtigen. Diese stellt hohe Anforderungen an den E-Mail-Versand von personenbezogenen Daten, zu denen in der Regel bereits die Empfänger-E-Mail-Adresse zählt. Die versendeten E-Mails sollten möglichst wenig Informationen und keine weiteren personenbezogenen Daten enthalten (wie etwa bei der „WI-Box“, bei der lediglich die Information erfolgt, dass ein Dokument – z. B. ein Ausweis – zur Abholung bereitliegt).

7.5
Fotografien von Sperrmüll durch einen kommunalen Abfallbetrieb

Auch im Rahmen der alltäglichen Abfallentsorgung werden Prozesse vermehrt automatisiert und digitalisiert. So werden z. B. zum Management der Logistikprozesse oder der Kundenbeziehungen vermehrt digitale Lösungen eingesetzt, die einer datenschutzrechtlichen Betrachtung unterzogen werden müssen.

Oft geht eine Beschwerdesituation durch die Kommunikation meiner Dienststelle mit dem Verantwortlichen fließend in eine Beratungssituation über, die zu einer Erhöhung des Informations- und Datenschutzniveaus insbesondere in der Etablierung und Weiterentwicklung digitaler Prozesse führen kann.

Im Berichtszeitraum erreichte mich eine Beschwerde gegen einen Abfallentsorgungsbetrieb, der hinsichtlich der Sperrmüllentsorgung für einen öffentlich-rechtlichen Entsorgungsträger tätig ist.

Im Rahmen eines Abholauftrags fertigte das Außendienstpersonal Fotografien von Sperrmüll an und verknüpfte diese sodann im Kundenmanagementsystem mit dem Abholauftrag des Auftraggebers. Im Kontext eines Reklamationsfalls erfuhr der Beschwerdeführer von den Fotografien und zweifelte an der Rechtmäßigkeit dieses Vorgehens. In diesem Zusammenhang erklärte er, dass er keine Information über das Anfertigen von Fotografien erhalten habe.

Damit der Anwendungsbereich der Datenschutzgrundverordnung eröffnet ist, ist zunächst erforderlich, dass es sich bei dem geschilderten Vorgehen um eine „Verarbeitung personenbezogener Daten“ handelt. Nach Art. 2 Abs. 1 DS-GVO kommt es darauf an, ob personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden oder ob bei einer nichtautomatisierten Verarbeitung eine Speicherung in einem Dateisystem erfolgen soll.

Die Begriffe „personenbezogene Daten“ und „Verarbeitung“ sind in Art. 4 Nr. 1 und 2 DS-GVO definiert.

Art. 4 Nr. 1 und 2 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

(1) „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;

(2) „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

(...)

Während eine digitale Fotografie im technischen Sinne unproblematisch dem Verarbeitungsbegriff unterfällt, war jedoch fraglich, ob mit Blick auf den Sperrmüll personenbezogene Daten verarbeitet werden. Bei Sperrmüll handelt es sich um eine Ansammlung von Gegenständen. Eine Fotografie des Sperrmülls enthält zunächst ausschließlich Informationen mit Bezug zu diesen Gegenständen. Ohne Verbindung zu einer natürlichen Person handelt es sich daher um sogenannte Sachdaten, bei denen zunächst kein Personenbezug nach Art. 4 Nr.1 DS-GVO besteht (Taeger/Gabel/Arning/Rothkegel, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 10). Ein Personenbezug kann sich jedoch auch erst im Zuge der weiteren Verarbeitung der Daten ergeben. So können verschiedene Daten mit Sachbezug derart zusammengeführt und kombiniert werden, dass die Person identifizierbar wird, also ein Personenbezug hergestellt werden kann (Taeger/Gabel/Arning/Rothkegel, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 13). Erst recht ist dies der Fall, wenn ausschließlich sachbezogene Daten mit weiteren personenbezogenen Daten verknüpft werden.

Daher ändert sich die Datenqualität durch die Verknüpfung der Fotografie mit dem Abholauftrag im Kundenmanagementsystem, da hier eine Verbindung der Informationen mit Identifikationsdaten einer natürlichen Person hergestellt wird. Mit anderen Worten: In dem Moment, in dem das Bild der Gegenstände dem Kundenauftrag zugeordnet und mit diesem verknüpft wird, erhält das Sachdatum einen Personenbezug im Sinne des Art. 4 Nr. 1 DS-GVO.

Ich habe das Entsorgungsunternehmen im Rahmen des Beschwerdeverfahrens zur Stellungnahme und zur Beantwortung verschiedener Fragen hinsichtlich der Erfüllung der Informationspflichten, zu den Zwecken und dem Hintergrund des Vorgehens sowie zu dem tatsächlichen und technischen Verarbeitungsprozess aufgefordert.

In seiner Stellungnahme hat das Entsorgungsunternehmen die Grundlagen und Prozesse rund um die fotografische Aufnahme von Sperrmüll ausführlich dargelegt. Es hat insbesondere erläutert, dass die Fotografien des Sperrmülls Dokumentationszwecken dienen und in Reklamationsfällen verwendet werden. Sie werden nur in folgenden Fällen angefertigt:

– wenn mehr Sperrmüll an der Abholstelle liegt, als angemeldet oder kostenfrei abzuholen ist,
– wenn kein Sperrmüll an der Abholstelle liegt,
– wenn Müll, der nicht zur Sperrmüllabfuhr gehört, an der Abholstelle liegt.

In diesem Zusammenhang wurde dargelegt, dass nach der entsprechenden Abfallwirtschaftssatzung das Entsorgen von Sperrmüll nur unter bestimmten Voraussetzungen kostenfrei ist:

Auszug aus der Abfallsatzung:

„(…)

(2) Jeder Grundstückseigentümer und jeder Haushalt von an die Abfallentsorgung angeschlossenen Grundstücken im Verbandsbereich ist berechtigt, bis zu Zweimal im Kalenderjahr kostenlos die Entsorgung von Sperrmüll anzufordern. (…)

(4) Die Gesamtmenge ist auf 2 m² pro Abholung begrenzt. (…)

(5) Es werden nur Abfalle mitgenommen, die bei der Anmeldung angegeben wurden. (…)“

Durch die Fotografien soll daher sichergestellt werden, dass die satzungsgemäßen Voraussetzungen im Kontext der Entsorgung eingehalten werden und, sollten sich Ungereimtheiten ergeben, der Müll und die Müllmenge der richtigen Person zugeordnet werden können. Wie im zugrundeliegenden Beschwerdefall wird die Bearbeitung von Reklamationssachverhalten ermöglicht oder erleichtert, z. B. wenn nicht (nur) der Sperrmüll des Anmeldenden, sondern fremder Sperrmüll entsorgt oder stehengelassen worden ist.

Als Rechtsgrundlage für die Datenverarbeitung kommt Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO in Betracht.

Art. 6 DS-GVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

(…)

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; (…)

Nach § 20 Abs. 1 KrWG haben die öffentlich-rechtlichen Entsorgungsträger die in ihrem Gebiet angefallenen und überlassenen Abfälle aus privaten Haushaltungen und Abfälle zur Beseitigung aus anderen Herkunftsbereichen zu beseitigen.

Den nach Landesrecht zur Entsorgung verpflichteten juristischen Personen (Gemeinden, Städte und Kreise oder Zusammenschlüsse als Zweckverbände) regeln gemäß § 1 Abs. 6 Nr. 2 HAKrWG durch Satzung, unter welchen Voraussetzungen, in welcher Weise, an welchem Ort und zu welcher Zeit ihnen die Abfälle zu überlassen sind.

In der Satzung des betreffenden öffentlich-rechtlichen Versorgungsträgers ist geregelt, dass dieser sich zur Erfüllung seiner Aufgaben Dritter, insbesondere privater Unternehmen, bedienen kann, wovon im vorliegenden Fall Gebrauch gemacht worden ist.

Das Entsorgungsunternehmen handelt bei Durchführung der Sperrmüllabfuhr folglich in Erfüllung seiner Verpflichtungen gegenüber dem öffentlich-rechtlichen Entsorgungsträger. Dem Bürger gegenüber tritt es als sog. Verwaltungshelfer auf und verarbeitet dessen Daten im Zusammenhang mit der Abwicklung des kostenfreien Sperrmüllkontingents also in Erfüllung öffentlicher Aufgaben und daher auf der Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO.

Das Fotografieren des Sperrmülls und die Verknüpfung mit dem Abholauftrag stellt unter den jeweiligen Voraussetzungen mithin eine rechtmäßige Datenverarbeitung im Sinne des Art 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO dar. Irrtümlich hatte das Entsorgungsunternehmen in seiner Datenschutzinformation Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO (vertragsbezogene Datenverarbeitung) als Rechtsgrundlage für die Datenverarbeitung aufgeführt. Diesbezüglich habe ich einen entsprechenden Hinweis erteilt.

Die Prüfung der Datenschutzinformation hat weiterhin ergeben, dass darin bereits Ausführungen zur Erstellung und Verknüpfung von Fotografien des Sperrmülls enthalten waren. Zur Bereitstellung der Datenschutzinformation sicherte die Verantwortliche zu, neben der Möglichkeit des Abrufs auf der Webseite, bei Übermittlung des telefonisch, elektronisch oder per Post zu vereinbarenden Abholtermins die entsprechende Datenschutzinformation zu übermitteln. Die Übermittlung des Abholtermins erfolge per E-Mail oder schriftlich per Post. Die Einrichtung einer automatisierten Übermittlung sei in die Wege geleitet.

Die Prüfung der Verarbeitungsprozesse selbst hat weiterhin ergeben, dass die technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO ein ausreichendes Sicherheitsniveau gewährleisten.

Da bei dem Entsorgungsunternehmen derzeit ein interner Prüfungs- und Anpassungsprozess im Bereich des Datenschutzes eingeleitet worden ist, konnte ich, neben Hinweisen zur Rechtsgrundlage und zur Datenschutzerklärung, einige Hinweise zu technischen Verbesserungen bei der Datenübermittlung, der Sicherung der Software auf den Endgeräten sowie zur Absicherung der Endgeräte selbst geben, die eine zusätzliche Optimierung darstellen.

7.6
Interessenkonflikte des Datenschutzbeauftragten in einer Kommune

Personelle oder fachliche Führungsfunktionen sowie die Verantwortung für maßgebliche Datenverarbeitungsvorgänge in Kommunen führen in der Regel zu einem Interessenkonflikt mit der Funktion des Datenschutzbeauftragten im Sinne von Art. 38 Abs. 6 S. 2 DS-GVO, § 7 Abs. 2 S. 2 BDSG und § 7 Abs. 2 S. 2 HDSIG.

Das Vorliegen von Interessenkonflikten ist eine der häufigsten Fragen, die mir zur Stellung und zu den Aufgaben des Datenschutzbeauftragten gestellt wird. Bei der Bestellung von Datenschutzbeauftragten besteht häufig die Neigung, dieses Amt einer bereits vertrauten Führungskraft zu übertragen. Offenbar wird hierbei davon ausgegangen, dass die Ausübung der Funktion des Datenschutzbeauftragten durch vertraute Führungskräfte sanft und im Sinne des Bürgermeisters erfolgt. Gleichwohl ist eine derartige Übertragung unzulässig, weil der dabei bestehende Interessenkonflikt personelle und fachliche Führungskräfte sowie Verantwortliche innerhalb der Datenverarbeitung von der Funktion des Datenschutzbeauftragten ausschließt.

In einem durch mich zu prüfenden Fall war die Funktion des Datenschutzbeauftragten auf eine Person übertragen worden, die gleichzeitig die Funktionen Hauptamtsleiter mit der Verantwortung für die IT-Systemadministration und Digitalisierung, Leiter der Steuer- und Liegenschaftsverwaltung, Leiter des Ordnungsdienstes, IT-Sicherheitsbeauftragter, Digitalisierungsbeauftragter, Antikorruptionsbeauftragter und Beschwerdestelle nach dem AGG innehatte. Hierbei lag ein Interessenkonflikt im Sinne von Art. 38 Abs. 6 S. 2 DS-GVO, § 7 Abs. 2 S. 2 BDSG und § 7 Abs. 2 S. 2 HDSIG nahe.

Zwar muss die Tätigkeit des Datenschutzbeauftragten nicht exklusiv ausgeübt werden. Der Datenschutzbeauftragte kann auch andere Funktionen wahrnehmen. Ein Interessenkonflikt darf jedoch nicht vorliegen. Wann genau ein Interessenkonflikt vorliegt, definiert das Gesetz nicht. Im Allgemeinen ist jedoch anerkannt, dass Datenschutzbeauftragte keine Funktionen ausüben dürfen, die sie in der Rolle des Datenschutzbeauftragten selbst überwachen würden. Mitglieder der obersten Führungsebene können daher nicht gleich-

zeitig Datenschutzbeauftragte sein. Das Gleiche gilt auch für Personen, die in maßgeblichem Umfang für die Datenverarbeitung in einer Organisation zuständig oder verantwortlich sind.

Kontrolliert eine Person unterhalb der Geschäftsleitung aufgrund ihrer Funktion oder Verantwortlichkeit bereits den Inhalt und den Umfang der Verarbeitung personenbezogener Daten, kann sie zur Überwachung ihrer eigenen Funktion nicht eingesetzt werden. Dies gilt beispielsweise für Personen mit Leitungsverantwortung innerhalb der IT-Abteilung. Anerkannt ist ein Interessenkonflikt auch für den Leiter der Marketingabteilung oder für Vertriebsleiter, weil diese verantwortlich für die Verarbeitung der Kundendaten sind. Innerhalb einer Kommune ist die Leitung eines Amtes, die in maßgeblichem Umfang Bürgerdaten verarbeitet, in etwa vergleichbar mit dem Leiter einer Marketingabteilung oder einem Vertriebsleiter. Auch in dieser Funktion einer Kommune sind Führungskräfte maßgeblich für Inhalt und Umfang der Verarbeitung personenbezogener Daten verantwortlich. Alle vorgenannten Führungsfunktionen beinhalten daher zur Funktion des Datenschutzbeauftragten einen Interessenkonflikt. Jede einzelne dieser Funktionen wäre bereits geeignet gewesen, die betroffene Person aufgrund eines bestehenden Interessenkonfliktes von der Funktion des Datenschutzbeauftragten auszuschließen.

Auch die Funktionen im Beauftragtenwesen können einen Interessenskonflikt beinhalten. So hat der Digitalisierungsbeauftragte vornehmlich ein Interesse an der Digitalisierung und damit der vereinfachten Verarbeitung von personenbezogenen Daten. Der IT-Sicherheitsbeauftragte ist üblicherweise an der Verarbeitung eines großen Umfangs von personenbezogenen Daten interessiert, um die IT-Sicherheit überwachen zu können. Beide Funktionen beinhalten daher einen Interessenkonflikt zur Funktion des Datenschutzbeauftragten. Das Gleiche gilt für den Antikorruptionsbeauftragten, der ebenfalls, ähnlich einem Geldwäschebeauftragten, an der Verarbeitung möglichst vieler Daten interessiert ist, um Korruption im Zweifel erkennen zu können. Die drei vorgenannten Funktionen im Beauftragtenwesen beinhalten daher ebenfalls einen Interessenkonflikt mit der Funktion des Datenschutzbeauftragten.

Nicht mehr geprüft werden musste, ob auch mit der Beschwerdestelle nach dem AGG ein Interessenkonflikt vorliegt, da es hierauf nicht mehr ankam. Ein Interessenkonflikt ist aber jedenfalls nicht offensichtlich.

In dem zu bearbeitenden Fall wurde die Kommune auf die bestehenden Interessenkonflikte hingewiesen, ein Austausch des Datenschutzbeauftragten erfolgte allerdings trotz mehrfacher Mahnungen nicht. Dieser Austausch erfolgte erst, nachdem die Kommune gemäß Art. 58 Abs. 2 Buchst. b DSGVO verwarnt und die Kommunalaufsicht eingeschaltet wurde.

8. Schule und Hochschulen

Das Hessische Kultusministerium setzt mehrere große Digitalisierungsprojekte für die hessischen Schulen um, die zu einem großen Digitalisierungsschub für den Schulunterricht und die schulische Kommunikation führen. Hierzu gehören nicht nur das Hessische Schulportal, das Schulverwaltungsnetz, die Lehrer- und Schülerdatenbank, weitere Unterrichtsprogramme und der einheitliche Schulzugang. Hierzu gehört seit kurzem auch ein datenschutzgerechtes souveränes Videokonferenzsystem (s. dazu Kap. 3.2). Auch im Hochschulbereich war die Etablierung datenschutzgerechter Videokonferenzsysteme eine wichtige Aufgabe (s. Kap. 3.3). Im Berichtszeitraum ist es gelungen, diese Digitalisierungsprojekte hinsichtlich des Datenschutzes erfolgreich zu begleiten und zu beraten.

8.1 Einheitlicher Schulzugang (ESZ)

Mit dem Digitalisierungsprojekt „Einheitliche Schul-ID" soll der Zugang zu den mittlerweile vielfältigen digitalen Werkzeugen, die das Hessische Kultusministerium (HKM) zur Verfügung stellt, erleichtert werden. Hierfür wird ein einheitliches Authentifizierungsverfahren etabliert. Die Zielsetzung des HKM ist nachvollziehbar und das Projekt erleichtert den Nutzern den Zugang zu den vielfältigen Angeboten. Allerdings gilt es auch, die datenschutzrechtlichen Fragestellungen in angemessener Form zu berücksichtigen.

Das Digitalisierungsangebot wird komplexer

Lehrkräfte, Schülerinnen und Schüler, Erziehungsberechtigte und andere Personen und Personengruppen nutzen im Schulumfeld digitale Angebote unterschiedlicher Anbieter. Dazu gehören digitale Anwendungen des Landes Hessen wie z. B. die Lehrer und Schülerdatenbank (LUSD) oder das Schulportal Hessen (SPH). Auch Angebote der Schulträger wie etwa die Bildungsplattformen I-Serv, SchulCloud oder wtk.edu werden genutzt. Hinzu kommen kommerzielle Anbieter wie etwa WebUntis, der u. a. eine digitale Stundenplanung oder den Einsatz digitaler Klassenbücher ermöglicht. Es besteht also ein breites Spektrum von digitalen Werkzeugen, die in der Schule in verschiedenen Kontexten zum Einsatz kommen. Um diese Werkzeuge nutzen zu können, werden private Endgeräte sowie die über den Digitalpakt beschafften Endgeräte der Schulträger genutzt.

Für viele Zugriffe auf die digitalen Verfahren sind derzeit jeweils eigene Anmeldewege und -daten erforderlich. Ferner sind für die Verarbeitung von sensiblen Daten weitere Schutzmaßnahmen, wie z. B. ein besonders sicheres

Anmeldeverfahren über eine Zwei-Faktor-Authentifizierung, notwendig. Dieses wird beispielsweise bei den dienstlichen E-Mail-Adressen für Lehrkräfte genutzt. Zudem fordert das HKM für die Nutzung weiterer Anwendungen (z. B. Online-Noteneingabe, individuelle und sonderpädagogische Förderung) auch im Sinn zusätzlicher Maßnahmen zum Datenschutz ebenfalls eine starke Authentifizierung. Mit dem Projekt „Einheitliche Schul-ID“ soll die Integration der verschiedenen Anwendungen in einen einheitlichen und sicheren Anmeldeprozess umgesetzt werden.

Zielsetzung des Kultusministeriums

Das HKM setzt derzeit das Programm „Digitale Schule Hessen“ um, in dessen Rahmen folgende Ziele erreicht werden sollen:

– Alle Personen, die im Schulumfeld tätig sind, können einen einheitlichen Zugang (Schul-ID Hessen) erhalten. Dies schließt Landes-, Kirchen- und Schulträgerpersonal, Schülerinnen und Schüler, Erziehungsberechtigte, aber auch andere Personen oder Institutionen mit schulischem Bezug ein.
– Es soll eine zentrale Zugangsseite eingerichtet werden, von der aus alle Anwendungen ohne erneute Anmeldung (Single-Sign-On) erreichbar sind.
– Zusätzlich soll der Zugang auch dezentral in bestehende Verfahren, wie z. B. Schulträgerportale, implementiert werden können. Hierbei dient der Einheitliche Schulzugang (ESZ oder auch Schul-ID Hessen) als zentraler Authentifizierungsdienst.
– Erreichbar sein sollen alle schulischen Systeme des Landes Hessen, aber auch Systeme Dritter (insbesondere der Schulträger) sollen eingebunden werden können.
– Bestehende Netze (wie z. B. das Hessische Schulverwaltungsnetz – HSVN) sollen durch den einheitlichen Zugang transformiert oder ganz ersetzt werden.

Die Umsetzung des Datenschutzes ist in besonderem Maße anspruchsvoll

Kernelement des Projekts ist ein einheitliches Authentifizierungsverfahren. Daraus ergeben sich diverse Vorteile für die Nutzerinnen und Nutzer. So sind u. a. die Anmeldeprozeduren ebenso einheitlich wie Passwortregeln. Passwörter und Authentifizierungswege werden zentral verwaltet. Für Anwendungen mit einem hohen Schutzbedarf steht eine sichere Anmeldung bereit. Zur Anmeldung selbst genügen der Benutzername und eine ID.

Daraus ergibt sich, dass ein leistungsfähiger Public Cloud-Dienst ausgesucht werden musste. Dass am Ende vom HKM ein Microsoft-Produkt (Azure) zur

Umsetzung herangezogen wurde, stieß bei mir im Hinblick auf die Rechtsprechung des EuGH (Schrems II-Urteil) (s. 50. Tätigkeitsbericht, Kap. 3) und die Kritik der DSK an Microsoft-Cloud-Produkten (s. Kap. 2) auf starke Vorbehalte, die ich wiederholt dem Minister selbst vorgetragen habe. Da eine dem Urteil des EuGH Rechnung tragende technische Lösung den Einsatz von Microsoft-Produkten problematisch macht, sofern personenbezogene Daten in die USA übertragen und dort verarbeitet werden oder Zugriffsmöglichkeiten von US-Nachrichtendiensten auf personenbezogene Daten bestehen, war eine Verständigung auf Grundlage der gewählten technischen Lösung komplex.

Sie war nur möglich, weil ich deutlich machen konnte, dass die Nutzung der MS-Cloud allenfalls temporären Charakter haben kann, soweit Microsoft in absehbarer Zeit nicht selbst Anpassungen umsetzt, die zu einer Datenschutzkonformität führen. Im anderen Fall muss die Migration des Anmeldedienstes in eine souveräne und datenschutzkonforme Cloud im Jahr 2023 erfolgen. Das Ministerium hat demzufolge beim Erwerb der erforderlichen Lizenzen von Microsoft einen sehr begrenzten Nutzungszeitraum gewählt.

Das Authentifizierungsverfahren zum ESZ sieht vor, die dienstliche E-Mail-Adresse der Lehrkräfte, die sich u. a. aus Vor- und Nachnamen zusammensetzt, zu verwenden. Eine mögliche Nutzung von Pseudonymisierungsverfahren der Lehrer-E-Mail-Adressen im Clouddienst zur Vermeidung der Angabe des Klarnamens, den ich zunächst präferierte, hätte jedoch in der Realisierung einen unverhältnismäßig hohen zeitlichen Aufwand in Anspruch genommen und den Zeitpunkt für eine mögliche Migration in die souveräne Verwaltungs-Cloud im Jahr 2023 überschritten. Deshalb war es nicht zielführend, auf der Pseudonymisierung zu bestehen, auch wenn dies zunächst folgerichtig erschien. Vielmehr muss nun durch geeignete organisatorische Maßnahmen sichergestellt werden,

– dass die von der Datenverarbeitung Betroffenen in geeigneter Weise über den Dienst und die Übertragung von Telemetrie-Daten informiert werden und
– den Lehrkräften die Möglichkeit für eine alternative Anmeldung aufgezeigt wird.

Weitere Vereinbarungen mit dem HKM

Ich habe darüber hinaus mit dem Ministerium vereinbart, mich in regelmäßigen zeitlichen Abständen über das angestrebte Migrationsverfahren in eine souveräne Verwaltungs-Cloud informieren zu lassen. Ich begrüße auch, dass das HKM sich um ein künftig von den Cloud-Anbietern SAP, Arvato und Microsoft ausgeschriebenes Pilotprojekt (Delos Cloud) bemüht, um u. a. Fragestellungen zur Migration von Daten in eine datenschutzkonforme Cloud zu lösen.

Darüber hinaus steht das HKM mit dem staatlichen Landes-Dienstleister Hessische Zentrale für Datenverarbeitung (HZD) in einem regelmäßigen Austausch, um im Rahmen der Bemühungen um eine souveräne Landes-Cloud auch kultusspezifische Aspekte in den Prozess einzubringen.

Ich habe in den umfangreichen Gesprächen auf der Fachebene und im Austausch mit dem Kultusminister den Eindruck gewonnen, dass das Ministerium mein Anliegen um eine rechtskonforme Lösung, auch und insbesondere im Sinne der Lehrkräfte, nachvollziehen kann und unterstützt. Die Erkenntnis, dass der Prozess für eine möglichst zeitnahe Herstellung der Datenschutzkonformität eine große Priorität hat, ist die Voraussetzung für eine absehbar sichere und souveräne Nutzung der einheitlichen Schul-ID.

8.2
Datenschutzrechtliche Beratung zum Schulportal Hessen

Das Schulportal Hessen (SPH) ist ein gelungenes Beispiel dafür, wie digitale Souveränität praktiziert werden kann. Bemerkenswert ist, dass bei den im SPH integrierten Anwendungen grundsätzlich Open Source-Software zum Einsatz kommt. Ein Teil der Anwendungen wurde ausgebaut und auf eine skalierbare Cloud-Umgebung migriert, um als nutzerfreundliche Plattform allen hessischen Schulen zur Verfügung zu stehen. Das HKM als oberste Schulaufsichtsbehörde sowie die HZD als zentraler IT-Dienstleister für die Hessische Landesverwaltung arbeiten dabei mit externen Dienstleistern zusammen, die im Anwendungsbereich der DS-GVO tätig sind.

Bereits in meinem 50. Tätigkeitsbericht habe ich berichtet, dass ich eine zentrale Beratungsaufgabe in den Bereichen des schulischen Datenschutzes, der Digitalisierung der Schulen und insbesondere zum SPH sehe (s. 50. Tätigkeitsbericht, Kap. 9.7). Dieser Aufgabe bin ich auch im Berichtsjahr nachgekommen.

Das HKM hat umfassende datenschutzrechtliche Unterlagen zum SPH erstellt und mir zu einer ersten Sichtung vorgelegt. Diese beinhalteten auch Anwendungen, die aufgrund der fortlaufenden Digitalisierung der Schulen neu in das SPH integriert wurden. Auf Grundlage dieser Unterlagen hat sich mein erster Eindruck bestärkt, dass es sich bei dem SPH um eine Plattform handelt, die datenschutzkonform betrieben werden kann.

Nachdem die Unterlagen seitens des HKM an meine Mitarbeiter übergeben wurden, startete eine Phase umfassender Beratungsleistungen meines Hauses gegenüber den einzelnen Fachabteilungen des HKM. Sowohl schriftlich als auch in mehreren Gesprächsrunden wurden die unterschiedlichen da-

tenschutzrechtlichen Aspekte des SPH besprochen. Beispielsweise wurde von meinen Mitarbeitern angeregt, einige Verträge, die mit einzelnen Dienstleistern zum SPH schon seit einigen Jahren bestehen, an neue rechtliche Erfordernisse anzupassen. Ein anderes Ergebnis der Beratungen war, dass die vorgelegten datenschutzrechtlichen Unterlagen an einigen Stellen zu konkretisieren sind, um die verschiedenen datenschutzrechtlichen Aspekte noch transparenter gegenüber den Nutzerinnen und Nutzern des SPH wie auch gegenüber meiner Behörde darzustellen. Beispielsweise sind in dem Rollen- und Berechtigungskonzept die verwendeten Kategorien betroffener Personen an diejenigen des Hauptdokuments zum Datenschutzkonzept anzupassen oder die Verwendung der globalen Rolle „Beschäftigte“ klarzustellen. Ein anderes Beispiel ist das Versäumnis, innerhalb der Datenschutzfolgenabschätzung die Bewertung der Verfahren hinsichtlich Notwendigkeit und Zweck durchzuführen. Auch dies ist seitens des HKM nachzuholen.

Eine Überprüfung des IT-Sicherheitskonzepts aus technischer Sicht ließ nur kleinere Ergänzungsbedarfe erkennen. Positiv hervorzuheben war dabei, dass das HKM bereits einen IT-Grundschutz-Check gemäß der Grundschutz-Schriftenreihe 200 des Bundesamts für Sicherheit in der Informationstechnik durchgeführt und damit eine gut zugängliche und überprüfbare Methode gewählt hatte.

Ein nächster Schritt muss nun sein, dass das HKM die vorgelegten Unterlagen entsprechend der Beratung meines Hauses überarbeitet, so dass eine finale Prüfung des SPH erfolgen kann.

8.3
Überprüfung schulischer Zugangsberechtigungen zum Schulverwaltungsnetz

Wiederholte Beschwerden haben mich im Berichtsjahr veranlasst, im Rahmen einer Stichprobe an hessischen Schulen den Prozess der Zugangsverwaltung von Schulleitungen und anderen Funktionsträgern auf die Lehrer- und Schülerdatenbank (LUSD) sowie die Schulverwaltungspostfächer zu überprüfen. Die Prüfergebnisse haben mich veranlasst, mit dem HKM Kontakt aufzunehmen, um eine nachhaltige und datenschutzkonforme Änderung des Prozesses zu erreichen.

Was die LUSD beinhaltet

Die Lehrer- und Schülerdatenbank ist ein Schulverwaltungsverfahren. Das webbasierte System verwaltet Schüler-, Unterrichts-, Leistungs- und Einsatzdaten der Lehrkräfte, prüft Kursbelegungen bis hin zur Zulassung für

Abitur, Haupt- und Realschulabschlüsse, druckt Zeugnisse und liefert die Grunddaten für Planung und Statistik. Die LUSD speichert die Daten zentral bei der HZD und stellt den Schulen einen gemeinsamen, stets aktuellen Datenbestand zur Verfügung.

Informationsanforderung

Ich habe die ausgewählten Schulen angeschrieben und darum gebeten,

1. mir auf die LUSD bezogen eine Übersicht zukommen zu lassen, aus der hervorgeht, warum welche Personen aufgrund welcher Funktion Zugriff für die befragte Schule auf die LUSD haben. Außerdem sollte mir seitens der einzelnen Schulen das entsprechende Rollen- und Berechtigungskonzept zu der Anwendung LUSD übersandt werden. Dieses sollte auch beinhalten, wann welchen Personen ihre Zugriffsrechte entzogen werden.
2. Bezogen auf die Schulverwaltungspostfächer sollten die Schulen darlegen, wer auf die einzelnen Postfächer warum Zugriff hat. Außerdem sollte auch diesbezüglich seitens jeder einzelnen Schule ein Rollen- und Berechtigungskonzept übermittelt werden, das auch beinhalten sollte, wann welche Personen ihre jeweiligen Berechtigungen verlieren.

Aus den mir übermittelten Unterlagen geht hervor, dass die Schulen eine Übersicht über die Rollen in der LUSD und auch bezogen auf die Schulverwaltungspostfächer führen. Allerdings konnte lediglich eine der 26 Schulen ein Rollen- und Berechtigungskonzept vorlegen, das auch die Entziehung von Berechtigungen durch organisatorische Maßnahmen gewährleistet. Eine weitere Schule hat zwar ein Rollen- und Berechtigungskonzept bezogen auf die LUSD und die Schulverwaltungspostfächer erstellt, in diesem wurde allerdings die Entziehung von Berechtigungen nicht geregelt.

Die Auswertung der Unterlagen ließ den Eindruck entstehen, dass viele Schulleitungen und deren Teams nicht wissen, dass ein Rollen- und Berechtigungskonzept, sowohl für die LUSD als auch für die Schulverwaltungspostfächer, aus datenschutzrechtlicher Sicht erstellt und vorgehalten werden muss. Meinen Eindruck unterstreicht beispielsweise das folgende Zitat aus einem Schreiben einer Schulleitung:

> „Da mir ein wenig unklar ist, was ein Rollen- und Berechtigungskonzept beinhalten sollte – neben der bereits vorliegenden Rechteverteilung, die sich aus der jeweiligen Funktion an der Schule ergibt – …“.

Ein Rollen- und Berechtigungskonzept ist für Schulen zwingend erforderlich

Mit einem Rollen- und Berechtigungskonzept können die Schulen sicherstellen, dass lediglich diejenigen Personen auf die durch die Schulen verarbeiteten personenbezogenen Daten Zugriff haben, die hierzu auch befugt sind. Es dient der Vereinfachung der schulinternen Organisation und Kommunikation. Mit einem solchen Konzept kann die Vergabe der Zugriffsberechtigungen einfach organisiert werden. Dabei sollte allerdings stets beachtet werden, dass lediglich absolut notwendige Zugriffsberechtigungen verteilt werden.

Es ist mithin zwingend erforderlich, dass die Schulen in Hessen künftig vollständige Rollen- und Berechtigungskonzepte bezogen auf die LUSD wie auch die Schulverwaltungspostfächer implementieren. Es wäre aus Sicht des Datenschutzes begrüßenswert, wenn eine zentrale Stelle, wie beispielsweise das HKM als zuständige Fachaufsicht, diesbezüglich Anforderungen an die Schulen vermitteln würde. Dies könnte etwa in der Form eines Musters eines Rollen- und Berechtigungskonzepts erfolgen.

Nachfolgend genannte Inhalte sind dabei von Bedeutung, wobei sich die zuständigen Stellen in methodischer Hinsicht auch dem hierfür zugrunde gelegten Baustein „Zugriffe auf Daten, Systeme und Prozesse regeln“ des Standard-Datenschutzmodells orientieren können:

– Ausgehend von Funktionen innerhalb der Schulorganisation (z. B. Schulleitung, Sekretariat) sind funktionsbezogene Rollen zu definieren, die in den IT-Systemen und -Diensten umzusetzen sind.
– Für jede Rolle ist festzulegen, über welche Berechtigungen diese bezogen auf das jeweilige IT-System und den IT-Dienst verfügt. Dabei soll eine Orientierung an den elementaren Verarbeitungsvorgängen personenbezogener Daten (Lesen, Schreiben, Löschen) erfolgen.
– Es ist vorzusehen, wann Berechtigungen an Personen vergeben werden (z. B. Eintritt in eine Funktionsstelle).
– Es ist vorzusehen, wann Berechtigungen entzogen werden. Dies muss sowohl allgemein erfolgen (z. B. „Ausscheiden einer Lehrkraft aus dem Schuldienst“) als auch – sofern absehbar – für konkrete Personen (z. B. „Ende des Referendariats von Frau Mustermann zum 31.12.2022“).
– Es ist festzuhalten, welchen Personen welche Berechtigungen zugeordnet sind. Diese Dokumentation ist stets aktuell zu halten.
– Das Entziehen von Berechtigungen ist durch organisatorische Maßnahmen zu gewährleisten (z. B. als Teil einer Offboarding-Checkliste, mit der etwa auch die Rückgabe von Dienstschlüsseln protokolliert wird). Diese Festlegungen sind in den Konzepten zu dokumentieren.

– Sofern Berechtigungen nicht personenbezogen vergeben werden können (z. B. Sammelpostfächer), ist namentlich festzuhalten, welchem Personenkreis eine geteilte Rolle zugewiesen ist. Es ist festzulegen, wie bei einer Veränderung der Zusammenstellung dieses Personenkreises eine unbefugte Weiternutzung ausgeschlossen wird (z. B. Passwortänderung).
– Als Teil der Konzepte ist eine regelmäßige Überprüfung und ggf. Anpassung dieser Konzepte an veränderte Gegebenheiten (z. B. neue Funktionen in der Schulorganisation oder neue technische Konfigurationen) vorzusehen. Der Grundsatz der Minimierung von vergebenen Berechtigungen ist dabei zu berücksichtigen.
– Die Konzepte sind mit dem Datum der letzten daran vorgenommenen Änderung sowie dem Namen der für Änderungen zuständigen Person(-en) zu versehen.

Ergebnis

Zusammenfassend bleibt festzuhalten, dass es notwendig ist, dass die Schulen ein Rollen- und Berechtigungskonzept sowohl bezogen auf die LUSD als auch die Schulverwaltungspostfächer erstellen und vorhalten. Aus diesem Grund bin ich in der ersten Jahreshälfte 2022 an das HKM herangetreten, damit Muster und Orientierungshilfen für die Schulen zu dieser Thematik erarbeitet werden. Am Ende des Berichtsjahres hat das HKM mir einen ersten Entwurf angepasster Unterlagen für die Schulen übermittelt, die mit Stand zum Redaktionsschluss zwischen dem HKM und mir abgestimmt werden.

9. Volkszählung 2022

Die Durchführung des Zensus 2022 in Hessen haben meine Mitarbeiter intensiv und mit hohem Aufwand begleitet. Dabei konnte festgestellt werden, dass es im Rahmen der Verfahrensabläufe in den 33 Erhebungsstellen des Landes sowie im Zusammenhang mit der Einschaltung privater Unternehmen für den Versand der Erhebungsunterlagen und deren Aufbereitung zu keinen Unregelmäßigkeiten gekommen ist, die das Projekt hätten in Frage stellen können.

Arbeitsumfang im Rahmen der Prüftätigkeit

Um eine Vorstellung über den Prüfumfang und den damit verbundenen Aufwand für meine Behörde zu erhalten, ist die Darstellung einiger Zahlenwerte hilfreich: So waren etwa 18 Personentage erforderlich, um die 33 hessischen Erhebungsstellen zu überprüfen. Zudem benötigte die Auswertung der Prüfergebnisse etwa acht Personentage. Hinzu kamen zwei Prüfungstermine bei externen Dienstleistern mit Standorten in Baden-Württemberg und Schleswig-Holstein. In diesem Zusammenhang haben meine Mitarbeiter etwa 6.000 Kilometer zurückgelegt und eine Vielzahl von Prüfprotokollen geschrieben, Gesprächsvermerke gefertigt sowie schriftliche Korrespondenz mit den geprüften Einrichtungen abgewickelt. Schließlich galt es, mit dem Hessischen Statistischen Landesamt (HSL) und den anderen Aufsichtsbehörden einen regelmäßigen Erfahrungsaustausch zu praktizieren, um sich gegenseitig über neue Entwicklungen und Erkenntnisse zu informieren. Mehr als ein Dutzend Termine fanden hierzu im Jahr 2022 statt.

Online-First Strategie der Statistischen Ämter

Wie schon der Zensus 2011 war auch der Zensus 2022 eine vornehmlich registergestützte Erhebung. Dabei wurden aus den bei Bundesbehörden (z. B. Bundesamt für Kartographie und Geodäsie) und Kommunen (z. B. Melderegister, Grundsteuerstellen) gespeicherten Anschriften und personenbezogenen Daten die für den konkreten statistischen Zweck erforderlichen Daten herausgefiltert und an die amtliche Statistik übermittelt. Neben einer Befragung der ca. 2,14 Millionen Gebäude- und Wohnungseigentümer im Rahmen der Gebäude- und Wohnungszählung (GWZ) war zusätzlich eine Haushaltsbefragung vorgesehen, die in Hessen etwa 850.000 Personen umfasste. Die Befragungen sollten möglichst online erfolgen, weshalb den Gebäude- und Wohnungseigentümern mit einem persönlichen Anschreiben auch die Zugangsdaten für eine Online-Plattform genannt wurden, die von einem Dienstleister des Statistischen Bundesamtes (ITZBund) betrieben

wurde. Die Werbekampagne für „Online-First“ war in der Folge offensichtlich aufgegangen, weil die Nachfrage nach papiergebundenen Unterlagen im Vergleich zum Zensus 2011 deutlich geringer ausgefallen ist. In Hessen lag die Online-Quote bei der GWZ bei 89,7 %. Das zeigte sich u. a. auch beim externen Dienstleister Rhenus Docs to Data, der für die Digitalisierung der Bögen zuständig war. Das Arbeitsaufkommen dort blieb unter den allgemeinen Erwartungen.

Erhebungsstellen

In den 21 hessischen Landkreisen, den Großstädten sowie den Städten mit Sonderstatus (z. B. Bad Homburg, Rüsselsheim) wurden bereits Ende des Jahres 2021 Statistikstellen eingerichtet. Rechtliche Grundlage hierfür war § 19 Zensusgesetz 2022 vom 26. November 2019 (BGBl. I S. 1851 ff, zuletzt geändert durch Gesetz zur Verschiebung des Zensus in das Jahr 2022 vom 3. Dezember 2021, BGBl. I, S. 2675) und § 3 des Hessischen Ausführungsgesetzes zum Zensus 2022 vom 25. März 2020 (GVBl. Nr. 15 S. 228). Für die Einrichtung und den Betrieb dieser Stellen, die für die Abwicklung der Haushaltsbefragung verantwortlich waren und die Zusatzerhebungen zu organisieren hatten, waren vom Hessischen Statistischen Landesamt (HSL) Mindestanforderungen und Empfehlungen erarbeitet worden. Der Umsetzung dieser Vorgaben hinsichtlich der personellen, administrativen und organisatorischen Abwicklung des Zensus 2022 galt mein Prüfinteresse.

Trennung von anderen Verwaltungseinheiten

In § 6 des hessischen Zensusausführungsgesetzes war geregelt, dass die Erhebungsstellen für die Dauer der Bearbeitung und Aufbewahrung von Einzelangaben räumlich und organisatorisch von anderen Verwaltungseinheiten zu trennen waren. Die Umsetzung dieser Vorgabe erfolgte durch die verantwortlichen Stellen zum Teil sehr unterschiedlich. Während es eine Reihe von Kreisen und Kommunen gab, die die räumliche Trennung durch die Einrichtung autonomer Erhebungsstellen gewährleisteten (so z. B. die Städte Darmstadt und Frankfurt, die Kreise Bergstraße, Main-Kinzig oder der Werra-Meißner-Kreis), waren andere Verwaltungsstellen „großzügiger“. Im Landkreis Groß-Gerau war die Erhebungsstelle auf drei Räume „komprimiert“, die im Fachdienst Gebäudemanagement angesiedelt waren. In einem anderen Fall (Main-Taunus-Kreis) war die Erhebungsstelle in einem vorgelagerten Impfzentrum untergebracht. Vom Impfzentrum aus konnte man ungehindert die Erhebungsstelle betreten. Ein anderes Beispiel: Bei der Stadt Wiesbaden wurde der in der Erhebungsstelle gelegene Sozialraum von den Mitarbeitern der Erhebungsstelle und jenen des Amtes für Wahlen und

Statistik gemeinsam genutzt. Kurzum, die Auslegung der vom Gesetzgeber geforderten räumlichen Trennung erfolgte zum Teil großzügig.

Auch an Kuriositäten mangelte es nicht. Die Stadt Fulda zum Beispiel richtete ihre Erhebungsstelle auf dem städtischen Friedhof ein. Das Gebäude wurde von den Mitarbeitern der Friedhofsverwaltung genutzt; einige Räume wurden der Zensus-Erhebungsstelle zugeordnet. Das Trennungsgebot konnte man jedoch trotzdem angemessen umsetzen. Auch der Landkreis Fulda konnte für seine Erhebungsstelle ein Alleinstellungsmerkmal reklamieren. Diese war im 11. Stock eines Verwaltungsgebäudes untergebracht, der mithin höchste Ort der Stadt.

Räumliche Unterbringung

Wie nicht anders zu erwarten und die Erfahrungen aus dem Zensus 2011 bestätigend, war die räumliche Unterbringung in vielen Fällen vorbildlich, andererseits jedoch auch grenzwertig. Dies betrifft nicht nur die Belange des Datenschutzes, sondern auch die Arbeitsbedingungen, denen das Erhebungsstellenpersonal ausgesetzt war. In Anbetracht auch zumindest in der Anfangsphase unzulänglicher Technik erscheint es in besonderem Maße schwierig zu sein, den gestellten Ansprüchen hinsichtlich der statistischen Geheimhaltung und zeitlicher sowie inhaltlicher Vorgaben stets in erforderlichem Umfang Rechnung zu tragen. Dort, wo man sich für eine externe Unterbringung fern der eigentlichen Verwaltung entschieden hatte, waren die räumlichen Verhältnisse und in der Regel auch die Arbeitsbedingungen angemessen. Hatte man sich jedoch dafür entschieden, die Erhebungsstelle im Rathaus oder in der Kreisverwaltung unterzubringen, ergaben sich in einigen Fällen Kalamitäten, die zumindest Zweifel dahingehend aufkommen ließen, ob denn die statistische Geheimhaltung jederzeit gewährleistet werden konnte. Das gilt z. B. für den getrennten Besucherbereich oder für den Empfang der Erhebungsbeauftragten.

Festzustellen war, dass eine Fülle von Erhebungsstellen auf den Besucherbereich und den sog. „Kommunikations-PC“ (die Möglichkeit für Bürger, in der Erhebungsstelle seine Daten online einzugeben) verzichtet haben, da man davon ausging, dass sich das Interesse der Bürger an einer Kontaktaufnahme vor Ort in Grenzen halten würde. In fast allen Fällen ging diese Rechnung auch auf. Der Kontakt mit den Erhebungsbeauftragten verlief ebenfalls sehr unterschiedlich. Teils wurden die Erhebungsunterlagen im Rahmen externer Schulungsveranstaltungen ausgehändigt, teilweise den Beauftragten auch zugestellt oder in der Erhebungsstelle übergeben, obwohl ein separater Raum für Besucher und Erhebungsbeauftragte nicht zur Verfügung stand.

Mindestanforderungen und Musterunterlagen des HSL

Das HSL hatte einen Maßnahmenkatalog zur Einrichtung von Erhebungsstellen erstellt, der die Themen IT und Informationssicherheit und die Einrichtung und Abschottung der Erhebungsstelle zum Inhalt hatte. Zusätzlich wurden Empfehlungen und Hinweise, u. a. zur regelmäßigen Prüfung der Hardware in der Erhebungsstelle, gegeben. Zudem hatte das HSL eine Musterdienstanweisung, das Muster einer Datenschutz-Folgenabschätzung (DSFA) sowie Beispiele für die erforderlichen Verzeichnisse der Verarbeitungstätigkeiten (VVT) zur Verfügung gestellt, welche die Erhebungsstellen verwenden sollten. Die Dienstanweisungen, DSFA und VVT konnten im Rahmen der Prüfungen von allen Erhebungsstellen vorgelegt werden.

Die vom Statistikamt für erforderlich gehaltenen technischen Maßnahmen zur IT- und Informationssicherheit wurden von den Erhebungsstellen ebenfalls weitgehend umgesetzt.

Eine umfassende technische Prüfung der meisten Stellen konnte aus Verfahrensgründen allerdings nicht erfolgen.

Erhebungsstellenleitung und Personal

Nach § 4 des Ausführungsgesetzes waren für die Erhebungsstellen eine Leitung und deren Stellvertretung zu bestellen. Diesem wichtigen gesetzlichen Erfordernis war mit der förmlichen Zuweisung der Aufgabe und Bestellung durch den Oberbürgermeister oder den Landrat in allen Erhebungsstellen entsprochen worden. Hinsichtlich des Anforderungsprofils musste gewährleistet sein, dass die Leitungsfunktion, soweit diese von Mitarbeitern aus der Verwaltung wahrgenommen wurde, „unkritischen“ Verwaltungseinheiten angehörte. Im Jahr 2011 hatte der Gesetzgeber ausdrücklich ausgeschlossen, dass aus bestimmten Bereichen wie z. B. der Vollstreckung, den Baubehörden, den Meldeämtern und den Ausländerbehörden Personal in der Erhebungsstelle eingesetzt wird. Diese Vorgabe war im Ausführungsgesetz für den Zensus 2022 nicht mehr enthalten. Dennoch waren alle Stellen bemüht, Personal aus Bereichen der Verwaltung einzusetzen, die dem Anspruch aus dem Jahr 2011 Genüge leisteten. In wenigen Fällen wurde für die Leitungsfunktion externes Personal rekrutiert.

Fast ausnahmslos zeichneten sich die Erhebungsstellenleiter und deren Vertreter durch kompetente Antworten aus. Auch die Vorlage der Unterlagen wie z. B. die Bestellung als Leitung, die Dienstanweisung und andere Dokumente erfolgte bis auf wenige Ausnahmen vollständig. Eine Vielzahl von Leitungen, aber auch das teilweise zeitlich nur temporär eingestellte Personal

in der Erhebungsstelle zeichneten sich durch hohen Einsatz und ein gutes Wissen auch datenschutzrechtlicher Fragestellungen aus.

In einigen Fällen übernahm Erhebungsstellenpersonal, soweit es sich aus der Verwaltung rekrutierte, temporär auch wieder Aufgaben ihres eigentlichen Aufgabenbereichs. Der Gesetzgeber hat dies nicht ausgeschlossen, doch ob dies tatsächlich im Sinne des Trennungsgebotes von Zensus und Verwaltung akzeptanzfördernd war, bleibt dahingestellt.

Erhebungsbeauftragte

Nach § 20 des Zensusausführungsgesetzes konnten die Kommunen für die Durchführung der Erhebung sog. Erhebungsbeauftragte (EB) rekrutieren. Diese waren dann für den Bereich der Haushaltsstichprobe tätig. Diese umfasste zunächst die „Existenzfeststellung", also die Ermittlung der in einem Haushalt lebenden Personen. In einem zweiten Schritt wurde eine Teilmenge in eine erweiterte Befragung einbezogen. Die Antworten konnten entweder online (der EB händigte dann die Zugangsdaten und Kennungen zum Portal aus) oder schriftlich mit einem Fragebogen erfolgen, den man vom Erhebungsbeauftragten bekam. Nach meinen Informationen, die ich aus den Erhebungsstellen erhalten habe, gab es eine „gute Onlinequote". Papier war dennoch gefragt, das dann beim Auftragsverarbeiter Rhenus Docs to Data in Schwarzenbek in Schleswig-Holstein aufbereitet, das heißt digitalisiert wurde (s. näher unten).

An die Erhebungsbeauftragten wurden im Vergleich zum Zensus 2011 keine Vorgaben hinsichtlich des ausgeübten Berufs gemacht, soweit dieser in einem Beschäftigungsverhältnis stand. Nur sollte der EB nicht in seiner unmittelbaren Wohnumgebung eingesetzt werden. Beschwerden über EB gingen bei mir nur vereinzelt ein. Allerdings war in wenigen Fällen die Zuverlässigkeit des EB nicht gewährleistet (s. unten).

Besucher

Flächendeckend haben die Erhebungsstellen festgestellt, dass es kaum zu Besucherverkehr gekommen ist. Nicht wenige Erhebungsstellen hatten überhaupt keine Besucher zu vermelden, andere nur in einstelliger Zahl. Die räumlichen und technischen Ressourcen blieben dort, wo man diese zur Verfügung gestellt hatte, weitgehend ungenutzt. Manche Erhebungsstellen verzichteten deshalb auf diesen Service. Soweit es dann doch einmal einen Auskunftspflichtigen in die Erhebungsstelle bewegte, behalf man sich z. B. beim Ausfüllen des Fragebogens mit einer pragmatischen Verfahrensweise. Auch diese Erkenntnis deutet auf eine verstärkte Online-Antwortquote hin.

Insoweit wiederholen sich die Erfahrungen, die man bereits beim Zensus 2011 gemacht hat.

Hinzu mag kommen, dass das Interesse der Bevölkerung anderen Themen galt. Ukraine-Krieg, Inflation, Energiekrise: Die Menschen sahen sich Problemen ausgesetzt, die den Zensus 2022 nicht zu einem relevanten öffentlichen Ereignis werden ließen.

IT und Informationssicherheit

Im Unterschied zum Zensus 2011 war die technische Ausgestaltung des Zensus 2022 maßgeblich von einem zentralistischen Ansatz bestimmt. Das Statistische Bundesamt und sein Auftragsverarbeiter „ITZBund“ waren für große Teile der technischen Abwicklung des Zensus 2022 zuständig. Die Aufgabe der Länder reduzierte sich daher auf die Vorgaben für die Einrichtung und den technischen Betrieb der Erhebungsstellen. Die Umsetzung dieser Vorgaben erfolgte dann durch die Städte und Landkreise.

Im Zusammenhang mit der Einrichtung der Erhebungsstelle hatten die für den Betrieb Verantwortlichen die nachfolgenden, nicht abschließend dargestellten Anforderungen umzusetzen:

– Bestellung eines Informationssicherheitsbeauftragten,
– Zugriffskontrolle auf der Ebene der Betriebssysteme in Form einer Benutzerverwaltung und eines Rollen- und Berechtigungskonzepts,
– Abschottung der IT-Systeme von der übrigen Verwaltung,
– Verschlüsselung der Datenablage,
– keine Software auf den IT-Systemen, die für den Betrieb der Anwendungen nicht erforderlich ist,
– Verwendung von aktuellen Virenscannern,
– Einrichtung eines Schnittstellenschutzes und
– Monitoring der relevanten IT-Systeme.

Nur vereinzelt Unzulänglichkeiten bei der Umsetzung

Im Rahmen der Prüfserie haben meine Mitarbeiter keine gravierenden Umsetzungsdefizite festgestellt. Vereinzelt war auf Rechnern Software installiert, die für den Zensus nicht erforderlich war. In einem Fall war keine Antiviren-Software auf dem EHU-PC (PC mit den Erhebungs-Unterstützungsprogrammen für den Zensus) installiert. Auch gab es Erhebungsstellen, die kein regelmäßiges Update des Virenscanners vorgenommen hatten. In einer Erhebungsstelle war der Standort des Druckers für den Quittungsaus-

druck nicht bekannt, soweit ein Auskunftspflichtiger den Auskunfts-PC für seine Online-Eingaben in der Erhebungsstelle zu nutzen beabsichtigte und am Ende eine Quittung für die gemachte Eingabe erhalten sollte. In einem anderen Fall waren drei Drucker für die Erhebungsstelle freigeschaltet, von deren Standort man nichts wusste.

Alle Mängel wurden auf Intervention meiner Mitarbeiter umgehend abgestellt. Hinsichtlich der technischen Qualität des Mangels verwundert es schon, dass insbesondere z. B. der unzulängliche Virenschutz kein Einzelfall war, sondern wiederholt festgestellt werden musste.

Zensus-Fragebogen auf Abwegen

Im Rahmen einer Großzählung, auch wenn bei den Haushalten eine Stichprobe durchgeführt wurde, kann es zwangsläufig zu Datenpannen kommen. Ob dies den Verlust von Erhebungsbögen betrifft oder die Nichtabgabe von Unterlagen durch Erhebungsbeauftragte: Vor menschlichem Fehlverhalten waren die Erhebungsstellen nicht gefeit. Um keinen falschen Eindruck zu erwecken: Tausende von hessischen Erhebungsbeauftragten haben im Sinn der amtlichen Statistik ihre Aufgaben vorbildlich erledigt. Insoweit handelte es sich um bedauerliche Einzelfälle, wenn z. B. in Darmstadt eine Erhebungsbeauftragte die ausgefüllten Fragebögen in einem Wohnblock im Hausgang vergaß und die Unterlagen dann entwendet wurden. Oder wenn in Frankfurt einige Erhebungsbeauftragte ihre Unterlagen nicht abgaben und die Erhebungsstellenleitung juristische Schritte einleiten musste. In allen meiner Behörde bekannten Fällen wurde durch die Verantwortlichen eine ordnungsgemäße Meldung über die Verletzung des Schutzes personenbezogener Daten nach Art. 33 DS-GVO abgegeben.

Beschwerden

Die Anzahl der Beschwerden (zum Zeitpunkt des Redaktionsschlusses etwa 70) hielt sich in Grenzen und war etwas geringer als 2011 (etwa 100). In einigen Fällen wurde die Rechtmäßigkeit des Zensus in Zweifel gestellt. In vielen Fällen ging es um nicht zugestellte Unterlagen oder die Nichterreichbarkeit der Hotline, die von einem externen Dienstleister betrieben wurde. Auch gab es vereinzelt Probleme mit Erhebungsbeauftragten, die sich vermeintlich nicht ausweisen konnten oder mit einer burschikosen Ansprache gegenüber den Auskunftspflichtigen auftraten. Mehr als einmal mussten meine Mitarbeiter telefonische Aufklärungsarbeit in Sachen Zensus vornehmen, eine Aufgabe, die eigentlich der Telefon-Hotline zugeordnet war.

In einer Reihe von Fällen konnte im direkten Kontakt mit den zuständigen Stellen des HSL Abhilfe geschaffen werden, insbesondere wenn es sich um vermeintlich oder tatsächlich falsche Adressen der Auskunftspflichtigen handelte.

Die geführten Telefonate beliefen sich wie 2011 auf eine Zahl im dreistelligen Bereich, reichte aber deutlich nicht an das Volumen von seinerzeit 700 Gesprächen heran.

Zusammenfassend ist festzustellen, dass massive Proteste gegen den Zensus, was datenschutzrechtliche Fragestellungen anbelangt, ausgeblieben sind. Ohne Zweifel kam es im Zusammenhang mit der Abwicklung des Zensus in einzelnen Fällen zu Problemen. Nicht erfasste Bögen, zugestellte Erhebungsunterlagen für nicht vorhandene Immobilien im Rahmen der GWZ oder aber unzuverlässige Erhebungsbeauftragte bei der Haushaltsbefragung: So etwas gab es im Einzelfall. Dennoch handelt es sich hierbei im Vergleich zu dem Gesamtvolumen von mehr als 2,4 Millionen Gebäude- und Wohnungseigentümern, die angeschrieben, und knapp 850.000 Einwohnern, die im Rahmen der Haushaltsbefragung kontaktiert wurden, um eine geringe Quote.

Mahnverfahren

Im Datenverarbeitungsprozess war vorgesehen, ein Mahnverfahren einzuleiten, soweit Gebäude- und Wohnungseigentümer oder einzelne Haushalte ihrer gesetzlich festgelegten Auskunftspflicht nicht nachkamen. Sowohl die Vorgehensweise als auch die Anzahl derer, die in ein solches Verfahren überführt wurden, war in den Erhebungsstellen unterschiedlich geregelt. Bis Ende November 2022 konnten noch Eingaben in das zentrale Verfahren des Bundes erfolgen. Insoweit war es ab dem Frühherbst geboten, säumige Auskunftgebende per Mahnverfahren doch noch zu animieren, ihre Daten an die amtliche Statistik zu übermitteln. In vielen Fällen war die damit verbundene Androhung eines Zwangsgeldes erfolgreich, so dass die personenbezogenen Daten doch noch geliefert wurden. Allerdings beabsichtigten nicht wenige Stellen, die Mahnverfahren oder gar ein angedrohtes Zwangs- oder Bußgeld nicht durchzusetzen, weil der Grund hierfür mit dem Ende der Eingaben und der Schließung der Erhebungsstellen zum 31. Dezember 2022 entfallen war.

Auftragsverarbeitung

Gab es beim Zensus 2011 bei einigen Aufsichtsbehörden für den Datenschutz noch rechtliche Bedenken hinsichtlich der Beauftragung von externen Dienstleistern, so war das im Jahr 2022 grundsätzlich kein Thema mehr. Im

Übrigen eröffnete die DS-GVO Freiräume, die u. a. mit einem Vertrag über eine Auftragsverarbeitung gem. Art. 28 Abs. 3 genutzt werden konnten.

Für drei Bereiche wurden externe Unternehmen von der amtlichen Statistik in Anspruch genommen:

– Telefon-Hotline,
– Versand von personalisierten Fragebögen und
– Digitalisierung der Fragebögen.

Telefon-Hotline

Nach den Erfahrungen aus dem Jahr 2011 war das Interesse der Statistischen Ämter groß, die Telefon-Hotline nicht selbst zu managen, sondern hierfür einen externen Dienstleister einzuschalten. Die datenschutzrechtliche Fragestellung lautete, in welchem Umfang auch Dienstleistungen erfolgen konnten, die über eine telefonische Auskunft oder die Veranlassung des Versandes von Erhebungsbögen an Auskunftspflichtige hinausgingen. Das betraf u. a. die Fallkonstellation, dass ein Auskunftspflichtiger seinen Bogen direkt mit dem Hotline-Mitarbeiter ausfüllen wollte. Ich habe an dieser Stelle deutlich gemacht, dass ich hierfür keine sich aus dem Zensusgesetz ergebende Rechtsgrundlage erkenne und die statistische Geheimhaltung der personenbezogenen Daten greift. Vielmehr war hier das HSL mit einem Second-Level-Support gefordert, um die Daten aufzunehmen.

Mit dem Dienstleister tricontes360 GmbH, einem Contact-Center Spezialisten, habe ich mich wiederholt zu datenschutzrechtlichen Aspekten hinsichtlich des Auftragsverarbeitungsprozesses ausgetauscht und relevante Fragestellungen zum Datenschutzkonzept für den Zensus erörtert.

Personalisierung und Versand der Erhebungsbögen der GWZ

Ebenfalls intensiv ausgetauscht haben meine Mitarbeiter sich mit dem Ricoh Document Center in Brackenheim bei Heilbronn. Das Unternehmen hat die Bögen der GWZ sowie der Haushaltsbefragung gedruckt, die Bögen der GWZ personalisiert (also mit Adressen versehen) und versendet. Dies erfolgte, soweit ein Auskunftspflichtiger nicht das Online-Verfahren zur Beantwortung gewählt hatte, sondern die Zusendung eines Papier-Fragebogens wünschte. Unter anderem ging es in den Gesprächen um die Transportverschlüsselung der vom Statistikamt zu übermittelnden Adressdaten sowie deren Löschung nach dem Druck der Unterlagen. Eine Besprechung im Unternehmen sowie die Prüfung der Verarbeitungsprozesse erfolgte ebenfalls.

Digitalisierung und Übermittlung der Fragebögen an das ITZBund

Die vom Auskunftspflichtigen ausgefüllten Fragebögen wurden an das Unternehmen Rhenus Docs to Data weitergeitet. Der Auftragsverarbeiter scannte die Bögen und übermittelte die Digitalisate an das ITZBund. Die datenschutzrechtlichen Fragestellungen ergaben sich hinsichtlich der Verarbeitung der Unterlagen nach dem Posteingang im Unternehmen selbst. So waren die Eingangsdokumentation, also die Protokollierung über den Eingang der Bögen, deren Erfassung im Rahmen des Scanvorgangs, die verschlüsselte Übermittlung sowie die erforderliche Mandantentrennung wichtige Themen wiederholter Vorbesprechungen. Ebenso wie den anderen externen Dienstleistern wurde Rhenus vorab ein Fragenkatalog ausgehändigt, der zu beantworteten war. Zudem machte sich mein Mitarbeiter auf den Weg nach Schleswig-Holstein, um vor Ort weitere Gespräche zu führen und die Verarbeitungsprozesse zu kontrollieren.

Schließlich ging es auch um die Lagerung und im späteren Verlauf die Vernichtung der Unterlagen beim Scan-Dienstleister. So wie 2011 gab es keine Beanstandungen. Die Zensus-Unterlagen der Bundesländer wurden auf dem videoüberwachten Betriebsgelände in einer Halle getrennt von anderen dort gelagerten Dokumenten aufbewahrt. Die Vernichtung der Bögen übernahm ein Tochterunternehmen im Rahmen eines Unterauftrags. Die Dokumentation dieses abschließenden Datenverarbeitungsprozesses war ebenfalls vorbildlich geregelt. Für meinen Mitarbeiter gab es deshalb keinen Grund, einen der in Schwarzenbek stattfindenden Verarbeitungsprozesse zu kritisieren.

Unzulänglichkeiten gab es hingegen wohl beim ITZBund. Die Übermittlung der Daten dorthin geriet zwischenzeitlich ins Stocken, weil der Prozess der Quittierung des Eingangs der digitalisierten Fragebögen nicht funktionierte. Die Folge war ein zwischenzeitlicher Übermittlungsstau, den das Unternehmen aber meisterte.

Zusammenarbeit mit dem Hessischen Statistischen Landesamt

Eine reibungslose Zusammenarbeit mit der zuständigen Fachaufsicht für Großerhebungen wie den Zensus 2022 ist für die Bewertung datenschutzrechtlicher Fragestellungen evident. Die Zusammenarbeit mit den zuständigen Mitarbeitern des HSL war ebenso kooperativ wie vertrauensvoll. Insbesondere hinsichtlich der Auftragsverarbeitung wurden meine Mitarbeiter stets aktuell unterrichtet. Alle notwendigen Unterlagen wurden im Vorfeld zur Verfügung gestellt. Regelmäßige Treffen im Vorfeld der Erhebung waren darauf ausgerichtet, datenschutzrechtliche Fragestellungen zu erkennen und hierfür Lösungen zu finden. Dies ist keine Selbstverständlichkeit, in Hessen aber seit vielen Jahren etabliert.

Zusammenarbeit mit den anderen Aufsichtsbehörden

Vom Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) war eine Ad-hoc-Arbeitsgruppe zum Zensus 2022 eingerichtet worden. Diese Einrichtung hatte sich bereits 2011 bewährt. Die Gruppe, bestehend aus dem Bund und den Ländern Hamburg, Sachsen-Anhalt und Hessen, beschäftigte sich mit einzelnen statistik- und datenschutzrechtlichen Fragestellungen, die sodann im zuständigen Arbeitskreis Statistik des Bundes und der Länder weiterbehandelt wurden und zur Entscheidung gelangten. Die Zusammenarbeit war dazu geeignet, knappe personelle Ressourcen konzertiert einzusetzen und für eine möglichst einheitliche Sprachregelung der Aufsichtsbehörden gegenüber der amtlichen Statistik Sorge zu tragen.

Vorläufiges Fazit

Für ein riesiges Datenverarbeitungsprojekt wie den Zensus 2022 waren die datenschutzrechtlichen Anforderungen groß. Von den Städten und Landkreisen sind diese im Rahmen des Betriebs der Erhebungsstellen im Großen und Ganzen umgesetzt worden.

Wie nicht anders zu erwarten, kam es im Verlauf der einzelnen Phasen immer wieder einmal zu Beschwerden oder Nachfragen, denen meine Mitarbeiter nachgingen. Gravierende Verstöße gab es keine. Unzulänglichkeiten entsprangen dem Fehlverhalten einzelner Mitarbeiter oder hatten organisatorische Hintergründe. Diese Einschätzung gilt sowohl für die Erhebungsstellenorganisation, die Abwicklung der Gebäude- und Wohnungszählung als auch für die Haushaltsbefragung. Die Beauftragung externer Dienstleister führte zu einer höheren Komplexität der Datenverarbeitungsprozesse und bedeutete für meine Mitarbeiter ein erhebliches Mehr an Aufwand. Dennoch gelang es, die Abwicklung auch in diesem Bereich stetig zu begleiten und auch zu kontrollieren.

Die Datenverarbeitung durch den Bund zu kontrollieren, also insbesondere das ITZ-Bund, das als Auftragsverarbeiter für das Statistische Bundesamt tätig ist, lag hingegen in der Zuständigkeit des BfDI.

Zukünftig ein registerbasiertes Verfahren

Die Zensusmethode wird weiterentwickelt. Bis 2031 will die amtliche Statistik schrittweise auf ein rein registerbasiertes Verfahren (Registerzensus) umstellen, bei dem keine zusätzlichen Befragungen mehr nötig sind. Die Daten sollen aus vorhandenen Quellen der Verwaltung oder Statistik weitgehend automatisiert gewonnen werden. Leitgedanke ist das Once Only-Prinzip: Bürgerinnen und Bürger müssen ihre Informationen nur noch einmal über-

mitteln und für belastbare Zensusergebnisse nicht mehr selbst Auskunft geben. Dafür müssen teilweise neue Register nach entsprechender Gesetzesgrundlage aufgebaut werden. Für die Gebäude- und Wohnungsangaben im Registerzensus ist es zum Beispiel erforderlich, ein Gebäude- und Wohnungsregister (GWR) als Verwaltungsregister aufzubauen. Das GWR liefert damit auch Informationen, die Politik, Verwaltung und Wissenschaft für ihre eigenen Aufgaben brauchen.

Auch bei diesem Projekt werden datenschutzrechtliche Fragestellungen zu klären sein. Um nur einige Beispiele zu nennen: Die Übermittlung von personenbezogenen Daten an ein zentrales Register ist per se mit der Frage verbunden, wer Zugriff auf die Datenbestände hat und die Aktualisierungen vornimmt. Zudem ergeben sich Anforderungen hinsichtlich der Löschung und Protokollierung. Die Aufsichtsbehörden für den Datenschutz werden den Prozess für einen Registerzensus ebenfalls eng begleiten.

10. Beratung des Hessischen Landtags

Auf Bitte der Präsidentin des Hessischen Landtags beriet ich die Landtagsverwaltung in der Aktualisierung des Leitfadens zum Datenschutz bei der Angabe personenbezogener Daten in parlamentarischen Initiativen für Abgeordnete des Hessischen Landtags.

Der Leitfaden soll Abgeordneten des Hessischen Landtags eine Arbeitshilfe für die Frage bieten, wie personenbezogene Daten – hier insbesondere Namen – zu behandeln sind, wenn sie in parlamentarischen Initiativen genannt werden sollen und dadurch in öffentliche Materialien gelangen, die von jeder Person einsehbar sind. Dieser Leitfaden sollte an das geänderte neue Datenschutzrecht und an die neue Datenschutzordnung des Hessischen Landtags (DSO) angepasst werden.

Ausgangspunkt ist § 9 Abs. 1 DSO, der zum Schutz des Rechts auf informationelle Selbstbestimmung natürlicher Personen den Grundsatz formuliert, dass personenbezogene Daten in Landtagsdrucksachen nicht veröffentlicht und in öffentlichen Sitzungen des Landtags nicht behandelt werden dürfen. Von diesem Grundsatz sieht die DSO zur Wahrnehmung parlamentarischer Aufgaben jedoch bestimmte Ausnahmen vor. Zum einen kann nach § 3 Abs. 1 Nr. 2 DSO eine einschlägige Einwilligung erlauben, personenbezogene Daten zu nennen. Zum anderen sieht § 9 Abs. 2 DSO auch ohne Einwilligung Ausnahmen vor, wenn die Kontrollaufgabe des Landtags das Recht auf informationelle Selbstbestimmung der betroffenen Person überwiegt. In diesem Fall ist für die Angabe personenbezogener Daten in parlamentarischen Initiativen eine Abwägung zwischen dem Recht auf informationelle Selbstbestimmung der betroffenen Person und der Kontrollaufgabe des Landtags vorzunehmen. Den Rahmen für diese Abwägung gibt § 9 Abs. 2 S. 2 Nr. 1 bis 3 sowie Abs. 3 und Abs. 4 DSO vor. Der Leitfaden gibt konkrete Hinweise, wie diese abstrakten und wertausfüllungsbedürftigen Ausnahmen in typischen Fällen zu verstehen sind.

Insbesondere für die Abwägung zwischen der Kontrollaufgabe des Landtags und dem Recht auf informationelle Selbstbestimmung der betroffenen Person gibt der Leitfaden Hinweise für die Abgeordneten:

Mit vollem Namen können nach § 9 Abs. 2 S. 2 Nr. 3 DSO Personen des öffentlichen Lebens genannt werden, sofern ihr öffentliches Wirken betroffen ist. Eine Abwägung mit ihrem Recht auf informationelle Selbstbestimmung ist in diesem Fall nicht erforderlich. Personen des öffentlichen Lebens sind insbesondere politische Mandatsträger (z. B. Bundestags- und Landtagsabgeordnete, Mitglieder des Kreistags, Stadtverordnete), Funktionsträger (z. B.

Minister, Staatssekretäre, Bürgermeister) sowie Personen der Zeitgeschichte (z. B. King Charles III., Nobelpreisträger, Olympiasieger).

Sollten diese Voraussetzungen nicht vorliegen oder Zweifel bestehen, ist nach § 9 Abs. 2 S. 2 Nr. 1 DSO grundsätzlich auf eine Namensnennung zu verzichten. Wenn zur Behandlung des Sachverhalts persönliche Merkmale erforderlich sind, wird die Funktions-, Dienst- oder Berufsbezeichnung der betreffenden Person verwandt und soweit notwendig wird der Nachname abgekürzt (z. B. Präsident B., Staatsanwalt A.).

Sollte gemäß § 9 Abs. 2 S. 2 Nr. 2 DSO eine Behandlung des Sachverhalts nur unter Nennung des Namens und der Daten der Person möglich sein und würden die Belange dieser Person durch eine öffentliche Erörterung erheblich beeinträchtigt, soll der Sachverhalt in einer nicht öffentlichen Sitzung eines Ausschusses oder einer Arbeitsgruppe behandelt werden.

Nach § 9 Abs. 4 DSO können Daten einer betroffenen Person selbst bei einer erheblichen Beeinträchtigung ihrer Belange ausnahmsweise öffentlich diskutiert werden, wenn es die parlamentarische Kontrolle erfordert. Dies ist z. B. bei einem Abschlussbericht eines Untersuchungsausschusses oder der parlamentarischen Debatte über diesen denkbar, bei denen es auf diese konkrete Person entscheidend ankommt.

Die Entscheidung über die Form der parlamentarischen Behandlung sowie die Veröffentlichung von Namen in parlamentarischen Initiativen trifft in umstrittenen Fällen die Präsidentin oder der Präsident.

11. Beschäftigtendatenschutz

Die Bedingungen des Datenschutzes von Beschäftigten werden massiv durch die Digitalisierung des Arbeitslebens, die Virtualisierung von Arbeitskontakten und Arbeitsabläufen und die Verbreitung smarter Geräte als Arbeitsmittel oder in der Arbeitsumgebung verändert. Dies ermöglicht, das Verhalten und die Leistung von Beschäftigen leichter, tiefer und umfassender zu erfassen (zu Kameraüberwachung Kap. 11.2). Spätestens durch diese ist eine umfassende Regulierung des Beschäftigtendatenschutzes überfällig (Kap. 11.1). Auch im Vorfeld des Bewerbungs- oder Beschäftigungsverhältnisses finden Verarbeitungsvorgänge zu Daten potenziell Beschäftigter statt (Kap. 11.3).

11.1 Veränderungen im Beschäftigtendatenschutz

Die voranschreitende Digitalisierung der Arbeitswelt verändert die Bedingungen des Persönlichkeitsrechtsschutzes im Beschäftigungsverhältnis. Durch eine IT-unterstützte Organisation und Leistungserbringung der Arbeit fallen immer mehr und immer präzisere personenbezogene Daten der Beschäftigten an. Zeitgleich eröffnen etwa algorithmenbasierte Entscheidungsunterstützungssysteme (KI) neue Möglichkeiten der Datenanalyse und damit leichtere, tiefere und umfassendere Kontrollen der Beschäftigten. Es ist an der Zeit, den Beschäftigtendatenschutz neu und umfassend zu regeln.

2009 wurde vor dem Hintergrund der Datenskandale einer Reihe von Großunternehmen erstmals eine eigenständige Regelung zum Beschäftigtendatenschutz geschaffen (§ 32 BDSG a. F.). Schon zum damaligen Zeitpunkt war sich der Gesetzgeber darüber bewusst, dass das Beschäftigtendatenschutzrecht der Weiterentwicklung bedarf (BT-Drs. 16/13657, 20). Trotz Absichtserklärungen in Koalitionsverträgen, Gesetzesinitiativen und der Möglichkeit der Neuregulierung im Zusammenhang mit dem Inkrafttreten der DS-GVO 2018 – die Regelung zum Beschäftigtendatenschutz besteht als § 26 BDSG bis heute ohne wesentliche inhaltliche Änderungen weitgehend fort.

§ 26 BDSG

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der

Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung hat schriftlich oder elektronisch zu erfolgen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

(3) Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Absatz 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 22 Absatz 2 gilt entsprechend.

(4) Die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Artikel 88 Absatz 2 der Verordnung (EU) 2016/679 zu beachten.

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Artikel 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(…)

EuGH-Vorlage zu den Vorschriften des Beschäftigtendatenschutzes

Dies könnte sich möglicherweise bald ändern, da die Frage der Unionsrechtskonformität der nahezu wortgleichen hessischen Vorschrift zum Beschäftigtendatenschutz, § 23 HDSIG, dem EuGH in der Rechtssache C-34/21 aktuell zur Prüfung vorliegt. Die Entscheidung des EuGH wird daher nicht nur Auswirkungen auf § 23 HDSIG, sondern auch auf § 26 BDSG haben.

§ 23 HDSIG

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung, Beendigung oder Abwicklung sowie zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist. Dies gilt auch zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Dienstherr oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Dienstherr oder Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 der Verordnung (EU) Nr. 2016/679 in Textform aufzuklären.

(3) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Abs. 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 20 Abs. 2 gilt entsprechend.

(4) Die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Art. 88 Abs. 2 der Verordnung (EU) Nr. 2016/679 zu beachten.

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Art. 5 der Verordnung (EU) Nr. 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(…)

Vorausgegangen war dem Vorlagebeschluss des VG Wiesbaden vom 21. Dezember 2020 (23 K 1360/20.WI.PV, ZD 2021, 393) ein Rechtsstreit zwischen dem Hauptpersonalrat der Lehrerinnen und Lehrer und dem Hessischen Kultusministerium über die Frage, ob die Einführung eines Livestream-Unterrichts durch Videokonferenzsysteme der Einwilligung der jeweiligen Lehrkraft bedarf oder ob die hier erfolgende Datenverarbeitung durch § 23 Abs. 1 S. 1 HDSIG gedeckt ist.

Das VG Wiesbaden äußerte in seinem Vorlagebeschluss zum einen Zweifel daran, dass es sich bei § 23 Abs. 1 Satz 1 HDSIG um eine spezifischere Vorschrift im Sinne der Öffnungsklausel des Art. 88 Abs. 1 und Abs. 2 DS-GVO handelt. Zum anderen hatte das Gericht Bedenken, ob die in § 23 Abs. 5 HDSIG enthaltene Regelung, wonach der Verantwortliche geeignete Maßnahmen ergreifen muss, um sicherzustellen, dass insbesondere die in Art. 5 der DS-GVO dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden, eine ausreichende Umsetzung des Art. 88 Abs. 2 DS-GVO darstellt.

Art. 88 DS-GVO

(1) Die Mitgliedstaaten können durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.

(2) Diese Vorschriften umfassen geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz.

(…)

Die Entscheidung des EuGH steht zum Ende des Berichtszeitraums zwar noch aus, sowohl die Europäische Kommission als auch der Generalanwalt haben sich aber bereits der Auffassung des VG Wiesbaden angeschlossen und zum Ausdruck gebracht, dass § 23 HDSIG nicht die Anforderungen der Öffnungsklausel des Art. 88 Abs. 1 DS-GVO erfülle, da es sich – im Verhältnis zu den Regelungen der DS-GVO – nicht um spezifizierende nationale

Vorschriften handle und der Verweis in § 23 Abs. 5 HDSIG und § 26 Abs. 5 BDSG keine ausreichende Umsetzung „besonderer Maßnahmen“ im Sinn des Art. 88 Abs. 2 DS-GVO sei (Schlussantrag des Generalanwalts vom 22. September 2022 in der Rechtssache C-34/21, Rn. 58, 72, 75).

Neue Regelungen zum Beschäftigtendatenschutz

Zu begrüßen ist daher, dass die Bundesregierung in ihrem Koalitionsvertrag bereits angekündigt hat, „Regelungen zum Beschäftigtendatenschutz zu schaffen, um Rechtsklarheit für Arbeitgeber sowie Beschäftigte zu erreichen und die Persönlichkeitsrechte effektiv zu schützen“ (Koalitionsvertrag zwischen SPD, Bündnis90/Die Grünen und FDP, 20. Legislaturperiode, S. 17). Auch die DSK fordert schon seit einigen Jahren gesetzliche Standards für das Beschäftigungsverhältnis (Entschließung der DSK vom 27. März 2014 „Beschäftigtendatenschutz jetzt!“ und vom 29. April 2022 „Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt“!“, https://www.datenschutzkonferenz-online.de/entschliessungen.html).

Was mögliche neue Regelungen zum Beschäftigtendatenschutz betrifft, kommt es daher gelegen, dass bereits in der vergangenen Legislaturperiode durch das Bundesministerium für Arbeit und Soziales (BMAS) mit dem Beirat zum Beschäftigtendatenschutz eine Expertenkommission einberufen worden war, um Handlungsempfehlungen zur Frage der Notwendigkeit eines eigenständigen Gesetzes zum Beschäftigtendatenschutz zu erarbeiten und erste inhaltliche Vorschläge für ein solches Gesetz zu prüfen. Der Beirat veröffentlichte seinen Bericht zum Beschäftigtendatenschutz im Januar 2022 (https://www.denkfabrik-bmas.de/schwerpunkte/beschaeftigtendatenschutz/bericht-des-unabhaengigen-interdisziplinaeren-beirats-zum-beschaeftigtendatenschutz).

Er kommt hierin zu dem Ergebnis, dass die generalklauselartige Regelung des § 26 BDSG vielfach keine treffsicheren Aussagen über die Zulässigkeit konkreter Verarbeitungen im Beschäftigungsverhältnis ermögliche, sondern dies der Einzelfallkasuistik der Gerichte überlasse, und fordert konkretisierende Regelungen (Bericht des Beirats zum Beschäftigtendatenschutz vom 17. Januar 2022, S. 5, https://www.denkfabrik-bmas.de/schwerpunkte/beschaeftigtendatenschutz/bericht-des-unabhaengigen-interdisziplinaeren-beirats-zum-beschaeftigtendatenschutz).

Auch nach Auffassung der DSK ist § 26 BDSG nicht hinreichend praktikabel, normenklar und sachgerecht (Stellungnahme der DSK zur Evaluierung des BDSG vom 2. März 2021, S. 8, https://www.datenschutzkonferenz-online.de/stellungnahmen.html) und führt daher sowohl auf Arbeitgeber- als auch auf Arbeitnehmerseite zu Rechtsunsicherheiten („Die Zeit für ein Beschäftigten-

datenschutzgesetz ist „Jetzt“!“, 1 https://www.datenschutzkonferenz-online.de/entschliessungen.html).

Erste Vorschläge zur inhaltlichen Ausgestaltung

Sowohl der Beirat zum Beschäftigtendatenschutz als auch die DSK geben erste Hinweise für mögliche Regelungskomplexe eines neuen Beschäftigtendatenschutzgesetzes und lassen dabei Parallelen erkennen, z. B. was die Notwendigkeit der Präzisierung des Beschäftigtendatenschutzrechts, die wesentlichen Leitgedanken der Ausgestaltung etwaiger Regelungen und die zwingend materiell-rechtlich auszugestaltenden Regelungskomplexe betrifft. Zudem hat der Deutsche Gewerkschaftsbund im Februar 2022 einen eigenen Entwurf zum Beschäftigtendatenschutz vorgelegt (https://www.dgb.de/uber-uns/dgb-heute/recht/++co++82a3178c-88c4-11ec-b434-001a4a160123).

Da mich im Bereich des Beschäftigtendatenschutzes eine Vielzahl von Anfragen und Beschwerden erreicht, stehe ich bei einer etwaigen Neuregulierung des Beschäftigtendatenschutzrechts in Hessen sehr gerne beratend zur Verfügung.

11.2
Fahrerüberwachung durch Kameras

Permanente Leistungs- und Verhaltenskontrollen von Beschäftigten bergen Potenzial für erhebliche datenschutzrechtliche Verstöße und sind regelmäßig rechtswidrig. Dies gilt auch für die Überwachung von Fahrerinnen und Fahrern einer Spedition durch Dashcams. Insbesondere das Filmen der Fahrerinnen und Fahrer durch eine in die Fahrerkabine ausgerichtete Kamera hat zu unterbleiben.

Beschwerden von Beschäftigten

Mich erreichten mehrere anonyme Beschwerden von Fahrerinnen und Fahrern einer Spedition. Die Beschäftigten gaben an, bei ihrer Tätigkeit durch sogenannte „Dashcams“ überwacht zu werden. Hierbei handelt es sich um Videokameras, die im oder am Fahrzeug angebracht sind und die das Fahrgeschehen aufzeichnen. Die erstellten Aufnahmen werden etwa zur Aufklärung von Verkehrsunfallhergängen und als Beweismittel in Gerichtsverfahren genutzt.

In ihren Beschwerden führten die Beschäftigten aus, dass die Dashcams über zwei Kamerawinkel verfügten, von denen einer das Verkehrsgeschehen auf der Straße filmte (Außenbereich) und der andere Aufnahmen von Beschäftigten in der Fahrerkabine anfertigte (Innenbereich).

Die Beschwerden habe ich zum Anlass genommen, den Verantwortlichen zu dem Verarbeitungsverfahren anzuhören. Es stellte sich heraus, dass die Angaben der Beschäftigten zutreffend waren. Meine Untersuchungen ergaben, dass die gefertigten Aufzeichnungen anlasslos für eine Dauer von 60 Stunden in einem geschlossenen System gespeichert wurden (sogenannter Ringspeicher). Bei bestimmten Anlässen – wie z. B. plötzlichem Lenken, starkem Bremsen, Übersehen von Verkehrsschildern oder Ablenkungen der Fahrerin oder des Fahrers von mehr als vier Sekunden – wurden aus den Aufzeichnungen des Ringspeichers automatisiert Videoclips erstellt und in eine Cloud hochgeladen. Ein bestimmter Personenkreis der Spedition hatte sodann die Möglichkeit, die erstellten Videoclips zu sichten. Die Videoclips wurden über einen Zeitraum von bis zu sechs Monaten in der Cloud-Instanz gespeichert.

Zur Rechtfertigung des Datenverarbeitungsverfahrens sollten die Betroffenen eine Einwilligung unterschreiben, hatten aber nicht die Möglichkeit, diese abzulehnen, sondern nur, diese zu „widerrufen“. Die Erklärung lautete wie folgt (Auszug):

> „Ich bin damit einverstanden, dass die mit der im Dienstfahrzeug installierten DashCam anlassbezogenen Aufzeichnungen mit persönlichen Daten meiner Person, im Rahmen der Verfolgung von Straftaten oder Ordnungswidrigkeiten, unter Beachtung der Datenschutz-Grundverordnung (DS-GVO) des Bundes- und Hessisches Datenschutzgesetzes (BDSG und HessDSG) an Berechtigte Dritte (diese wurden konkret genannt) übermittelt werden.
>
> Weiter bin ich darauf hingewiesen worden, dass die Nutzung meiner Daten auf freiwilliger Basis erfolgt. Ferner, dass ich diese Einwilligung jederzeit gemäß Art. 7 DS-GVO mit Wirkung auf die Zukunft widerrufen kann. Meine Widerrufserklärung richte ich an (Hier wurde die E-Mail-Adresse des Datenschutzbeauftragten des Verantwortlichen genannt). Hiermit erkläre ich, dass ich in dieser Art der Vorgehensweise aus freiem Willen einwillige.“

Zu dem Zeitpunkt, als den Beschäftigten die Einwilligungserklärung vorgelegt wurde, waren die Kameras bereits eingebaut und in Betrieb genommen.

Neben der Einwilligung machte der Verantwortliche geltend, dass die Videoüberwachung des Verkehrsgeschehens einerseits als Gegenmaßnahme hinsichtlich eigenverschuldeter Unfälle der Beschäftigten erfolgte und andererseits, um bei fremdverschuldeten Unfällen Beweise zu sammeln.

Einwilligung?

Der Grundsatz der Rechtmäßigkeit der Datenverarbeitung aus Art. 5 Abs. 1 Buchst. a DS-GVO in Verbindung mit Art. 6 DS-GVO verlangt für die Rechtmäßigkeit der Datenverarbeitung eine Rechtsgrundlage oder eine Einwilligung der Betroffenen.

Für den Bereich des Beschäftigtendatenschutzes sieht Art. 88 DS-GVO eine Öffnungsklausel vor, die es den Mitgliedsstaaten ermöglicht, spezifische Vorschriften für den Bereich des Beschäftigtendatenschutzes zu erlassen. Mit der Vorschrift des § 26 BDSG hat der Gesetzgeber von dieser Möglichkeit Gebrauch gemacht. Grundsätzlich kann nach § 26 Abs. 2 BDSG (s. Kap. 11.1) auch im Beschäftigtenverhältnis eine Einwilligung die Datenverarbeitung legitimieren; dies allerdings nur unter sehr engen Voraussetzungen:

Die Datenverarbeitung im Rahmen der Kameraüberwachung war nicht durch eine den Anforderungen des § 26 Abs. 2 BDSG entsprechende Einwilligung gerechtfertigt. Denn bei der Beurteilung der Freiwilligkeit der Einwilligung kommt dem Umstand der im Beschäftigungsverhältnis bestehenden Abhängigkeit (sog. Über-Unterordnungsverhältnis) besondere Bedeutung zu.

So muss für eine freiwillige und somit wirksame Einwilligung immer ein rechtmäßiges Alternativverhalten (z. B. die Ablehnung des Datenverarbeitungsverfahrens) möglich sein, so dass die Betroffenen eine echte Wahlmöglichkeit haben. In dem zu beurteilenden Fall waren die Kameras bereits in die Fahrzeuge eingebaut, bevor die Beschäftigten überhaupt Gelegenheit hatten, in das Datenverarbeitungsverfahren „einzuwilligen“. Die betroffenen Fahrerinnen und Fahrer wurden somit von Beginn an vor vollendete Tatsachen gestellt. Eine wirksame Einwilligung lag jedoch mangels Freiwilligkeit der Einwilligung nicht vor.

Nach meiner Anhörung und dem Hinweis, dass die vorgelegte Einwilligungserklärung nicht den Anforderungen des § 26 Abs. 2 BDSG entsprach, berief der Verantwortliche sich nicht länger auf eine Einwilligung als Rechtsgrundlage, sondern auf § 26 Abs. 1 S. 1 BDSG (s. Kap. 11.1).

Notwendigkeit für das Beschäftigungsverhältnis?

Die Überwachung der Beschäftigten war allerdings auch nicht nach § 26 Abs. 1 S. 1 BDSG rechtmäßig. Gemäß § 26 Abs. 1 S. 1 BDSG dürfen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigtenverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigtenverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.

Im Rahmen der Erforderlichkeitsprüfung sind die Interessen des Arbeitgebers und die schutzwürdigen Interessen der Beschäftigten abzuwägen und zu einem Ausgleich zu bringen, der beiden Interessen möglichst weitgehend gerecht wird (praktische Konkordanz).

Zu fordern ist hierfür eine Prüfung am Maßstab des Verhältnismäßigkeitsgrundsatzes, was wiederum voraussetzt, dass seitens des Verantwortlichen ein legitimer Zweck verfolgt wird, das Verarbeitungsverfahren für die Verwirklichung dieses Zwecks geeignet ist und es sich um das mildeste aller gleich effektiv zur Verfügung stehenden Mittel handelt. Darüber hinaus muss es auch unter Abwägung der Umstände des Einzelfalles angemessen sein.

Eine offene Videoüberwachung ist somit nach § 26 Abs. 1 S. 1 BDSG als Maßnahme im Rahmen der Durchführung des Beschäftigungsverhältnisses zulässig, wenn der mit der Datenverarbeitung verfolgte Zweck auf die Eingehung, Durchführung oder Beendigung des Beschäftigungsverhältnisses gerichtet ist und den Anforderungen des Verhältnismäßigkeitsgrundsatzes entspricht.

Soweit durch die Überwachung des Fahrverhaltens der Beschäftigten selbstverschuldete Unfälle vermieden werden sollen, ist eine flächendeckend eingebaute Videoüberwachung nicht erforderlich. Selbst wenn angenommen wird, dass die Videoüberwachung insofern einen legitimen Zweck im Sinn des § 26 Abs. 1 S. 1 BDSG darstellt, und unterstellt wird, dass es sich hierbei um eine geeignete Maßnahme handelt, kommen mindestens vergleichbar effektive, mildere Maßnahmen in Betracht, wie etwa die Durchführung regelmäßiger Sensibilisierungs- oder Schulungsmaßnahmen der betroffenen Fahrerinnen und Fahrer.

Zu berücksichtigen ist weiterhin, dass der unterschiedslose Einbau in die Fahrzeuge aller Beschäftigten auch unter Abwägung der Umstände des Einzelfalles unangemessen ist. Hier wäre eine Unterscheidung hinsichtlich der Unfallgeneigtheit der Beschäftigten in der Vergangenheit notwendig, so dass gegebenenfalls lediglich den Fahrerinnen und Fahrern das Kamerasystem für den Außenbereich in ihr Fahrzeug eingebaut wird, die bereits vermehrt in selbstverschuldete Unfälle verwickelt waren.

Ein Filmen des Innenbereichs der Fahrerkabine – d. h. die Fertigung von Aufnahmen der Beschäftigten – ist datenschutzrechtlich nicht zu rechtfertigen und stellt einen erheblichen Verstoß gegen die Bestimmungen des Datenschutzrechts seitens des Verantwortlichen dar.

Bei der Videoüberwachung des Innenbereichs der Fahrerkabine handelt es sich um eine Leistungs- und Verhaltenskontrolle der Beschäftigten, durch die ein dauerhafter Überwachungsdruck entsteht. Denn Betroffene müssen

damit rechnen, dass jedes Verhalten überwacht werden kann (vgl. BAG: Offene Videoüberwachung – Beweisverwertungsverbot und Zulässigkeit der Datenerhebung, NZA 2019, 1212). Gestik und Mimik, bewusste oder unbewusste Gebärden, der Gesichtsausdruck bei der Arbeit oder der Kommunikation mit Vorgesetzten oder Kolleginnen und Kollegen unterliegen der Möglichkeit dokumentierter Betrachtung, so dass ein Druck entsteht, sich permanent möglichst unauffällig zu verhalten (vgl. BAG: Videoaufnahmen am Arbeitsplatz – allgemeines Persönlichkeitsrecht der Arbeitnehmer – Grundsatz der Verhältnismäßigkeit, NZA 2004, 1278). Ein solch intensiver Eingriff in das Persönlichkeitsrecht in Form einer Vollkontrolle ist datenschutzrechtlich unzulässig.

Speicherbegrenzung?

Die automatische Speicherung aller Aufzeichnungen für eine Dauer von 60 Stunden verstößt zudem gegen den Grundsatz der Speicherbegrenzung des Art. 5 Abs. 1 Buchst. e DS-GVO. Danach darf ein Personenbezug nur so lange ermöglicht werden, wie es für die Zwecke der Datenverarbeitung erforderlich ist. Werden die Daten für diesen Zweck nicht mehr benötigt, ist der Verantwortliche somit verpflichtet, diese unverzüglich zu löschen. Dies ergibt sich, den Grundsatz der Speicherbegrenzung konkretisierend, aus Art. 17 DS-GVO (s. Kurzpapier Nr. 11 der DSK zum Recht auf Löschung, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf).

Zwar ist hinsichtlich des Nachweises zum Ablauf eines Verkehrsunfalls zu beachten, dass eine Videoaufnahme ein wirksames Mittel zur Aufklärung eines Sachverhalts darstellt (vgl. Balzer/Nugel, Minikameras im Straßenverkehr – Datenschutzrechtliche Grenzen und zivilprozessuale Verwertbarkeit der Videoaufnahmen, NJW 2014, 1622). Allerdings wird gerade bei fremdverschuldeten Unfällen das Fahrverhalten der Fahrerinnen und Fahrer aufgezeichnet, ohne dass die Aufzeichnung in Zusammenhang mit einem konkreten Fehlverhalten steht. Ein solcher Eingriff in das Persönlichkeitsrecht, der verdachtslos und ohne Veranlassung durch die Betroffenen entsteht, weist eine hohe Intensität auf (vgl. Balzer/Nugel, Minikameras im Straßenverkehr – Datenschutzrechtliche Grenzen und zivilprozessuale Verwertbarkeit der Videoaufnahmen, NJW 2014, 1622).

Eine permanente anlasslose Aufzeichnung des Verkehrsgeschehens ist datenschutzwidrig (vgl. Positionspapier der DSK zur Unzulässigkeit von Videoüberwachungen aus Fahrzeugen (sog. Dashcams) vom 28. Januar 2019, https://www.datenschutzkonferenz-online.de/media/oh/20190128_oh_positionspapier_dashcam.pdf).

Diese Eingriffsintensität lässt sich absenken, indem Ringspeicher verwendet werden, die in festen periodischen Abständen die gefertigten Videoaufnahmen löschen und nur solche Videoaufnahmen speichern, bei denen bestimmte Voraussetzungen – wie beispielsweise das Auslösen eines Erschütterungssensors bei starkem Bremsen – gegeben sind.

Hinsichtlich der eingriffsmindernden Wirkung ist die Dauer der regelmäßigen Aufzeichnung im Ringspeicher und die konkrete Auslösung der nachhaltigen Speicherung in der Cloud-Instanz zu beachten (vgl. Starnecker, in: Gola/Heckmann, DSGVO/BDSG, 3. Auflage 2022, BDSG § 4 Rn. 47-51).

Weiter ist zu berücksichtigen, dass sich das Interesse des Aufzeichnenden bezüglich des Sammelns von Beweisen allein auf die Aufzeichnung des unmittelbaren Unfallgeschehens beziehen kann (vgl. Giesen, Dashcam-Aufnahmen im Zivilprozess, NZV 2020, 70). Somit sind in der Regel lediglich Aufnahmen unmittelbar vor, während und kurz nach dem Unfallgeschehen als erforderlich anzusehen (vgl. BGH, Dashcam-Aufnahmen als Beweismittel im Unfallhaftpflichtprozess, NJW 2018, 2883).

Die von dem Verantwortlichen vorgenommene Aufzeichnung mit einem Ringspeicher mit einer periodischen Aufzeichnung von 60 Stunden genügte diesen Anforderungen nicht und verstieß daher auch gegen den Grundsatz der Speicherbegrenzung des Art. 5 Abs. 1 Buchst. e, Art. 17 Abs. 1 Buchst. a DS-GVO.

Dies gilt auch für die Speicherung der in die Cloud hochgeladenen Videoclips für eine Dauer von bis zu sechs Monaten. Werden Daten für den Zweck der Datenverarbeitung nicht mehr benötigt, ist der Verantwortliche verpflichtet, diese unverzüglich zu löschen. Dies ist bei erstellten Videoaufzeichnungen der Fall, wenn z. B. eine Beweissicherung nicht mehr notwendig ist. Ob ein solches Ereignis vorlag, lässt sich grundsätzlich innerhalb von ein bis zwei Arbeitstagen aufklären. Auch hier empfiehlt sich die Orientierung an der Speicherdauer von maximal 72 Stunden (vgl. DSK, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, S. 22f., https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf).

Längere Speicherintervalle wären nur dann zulässig, wenn Straftaten oder erhebliche Pflichtverletzungen erst bei aufwändigen Überprüfungen entdeckt werden können. In dem zu beurteilenden Fall war eine solche Situation nicht gegeben.

Datenschutzrechtliche Reaktion

Die festgestellten Verstöße erfordern das Ergreifen von Maßnahmen nach Art. 58 Abs. 2 DS-GVO Aufgrund der festgestellten Verstöße wären neben

einem Bußgeldverfahren Maßnahmen nach Art. 58 Abs. 2 Buchst. f DS-GVO in Form einer Untersagungsanordnung in Betracht gekommen. Nach meiner Anhörung und aufgrund meiner rechtlichen Ausführungen setzt die Verantwortliche das System inzwischen nicht mehr ein. Daher wird das Justiziariat meiner Behörde nun das Einleiten eines Bußgeldverfahrens prüfen.

11.3
Active Sourcing zur Gewinnung von Bewerberinnen und Bewerbern

Unter aktiver Personalbeschaffung (Active Sourcing) wird die gezielte Suche von Arbeitgebern oder Personaldienstleistern nach geeigneten Kandidatinnen oder Kandidaten im Internet sowie deren persönliche Ansprache verstanden. Beruflich orientierte Netzwerke, Webseiten, Bewerberdaten oder auch Suchmaschinenanfragen – die Quellen zur Erhebung personenbezogener Daten im Internet sind vielfältig. Active Sourcing kann zulässig sein, wenn die betroffene Person augenscheinlich ihre Daten öffentlich gemacht hat.

Zu Beginn des Berichtszeitraums wandte sich eine Beschwerdeführerin mit der Bitte um datenschutzrechtliche Prüfung und Bewertung im Zusammenhang mit der Kontaktaufnahme eines Personaldienstleisters an mich. Das Recruiting-Unternehmen war an die Betroffene per E-Mail mit sinngemäß folgender Nachricht herangetreten:

> „Sehr geehrte Dame, sehr geehrter Herr,
>
> hiermit informieren wir Sie gemäß Art. 13 bzw. Art. 14 der Datenschutzgrundverordnung (DSGVO), dass wir Ihre personenbezogenen Daten in unsere Datenbank aufgenommen haben. Wir haben Ihre Daten aus sozialen Medien oder einer öffentlichen Datenbank erhalten.
>
> Wir sind ein Personaldienstleister (…). Zu diesem Zweck unterhalten wir eine Datenbank von potenziellen Kandidatinnen und Kandidaten, die ständig aktualisiert und erweitert wird, um Beschäftigte für unsere Kunden zu finden. Ihre Daten werden innerhalb unserer Unternehmensgruppe verarbeitet. Eine Weitergabe personenbezogener Daten erfolgt nicht, es sei denn, es handelt sich um konkrete Projekte, über die wir Sie im Vorfeld informieren. Die Rechtsgrundlage für diese Verarbeitung ist unser berechtigtes Interesse (Art. 6 Abs. (1) f) DSGVO) an der Vermittlung an unsere Kunden.
>
> Verantwortlicher im Sinne der DSGVO ist (…)
>
> Kontakt zu unserem Datenschutzbeauftragten (…)

> Sie haben das Recht, der Verarbeitung zu widersprechen (Art. 21 DS-GVO). Ihre weiteren Rechte und detaillierte Informationen zu unserer Datenverarbeitung finden Sie in der Datenschutzerklärung auf unserer Website: www.(...).de/datenschutz.
>
> Mit freundlichen Grüßen“

Die Betroffene war somit darüber informiert worden, dass ihre personenbezogenen Daten zum Zwecke der Personalvermittlung in die Datenbank des Unternehmens aufgenommen worden sind. Weiterhin enthielt die E-Mail-Nachricht des Personaldienstleisters die Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten und die Betroffene wurde auf ihr Widerspruchsrecht hingewiesen.

Aufgrund der Beschwerde der Betroffenen habe ich das verantwortliche Personalvermittlungsunternehmen angehört. In meiner Anhörung habe ich danach gefragt, woher die Daten der Betroffenen stammten und wie das Unternehmen auf sie aufmerksam geworden war. Der Verantwortliche führte auf meine Anhörung hin umfangreich aus, erläuterte sein Tätigkeitsfeld und den Prozess zur Erhebung und Speicherung potenzieller Kandidatinnen und Kandidaten in der eigenen Datenbank. Bezüglich der Datenverarbeitungsvorgänge rund um die Beschwerdeführerin erklärte der Personaldienstleister, dass er aufgrund einer konkreten Kundenvakanz nach den geforderten Qualifikationen über die Suchmaschine von Google nach passenden Kandidatinnen und Kandidaten gesucht habe. Hierbei sei ein Treffer für eine von der Beschwerdeführerin mit beruflichem Kontext betriebene Webseite erzielt worden. Von dieser Webseite seien sodann die personenbezogenen Daten der Betroffenen erhoben und in der Datenbank des Personalvermittlers gespeichert worden.

Art. 5 Abs. 1 Buchst. a bis f DS-GVO enthält die Grundsätze für die Verarbeitung personenbezogener Daten und stellt in Abs. 2 klar, dass der Verantwortliche für deren Einhaltung verantwortlich ist („Rechenschaftspflicht“). Nach Art. 5 Abs. 1 Buchst. a DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“). Mit Blick auf den durch meine Behörde zu beurteilenden Sachverhalt war vor diesem Hintergrund zum einen zu prüfen, ob die Datenverarbeitungen durch den Personalvermittler auf eine Rechtsgrundlage gestützt werden können, und zum anderen, ob die Informationspflichten des Art. 14 DS-GVO beachtet wurden und das Vorgehen des Verantwortlichen somit ausreichend transparent war.

Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten

Bezüglich der Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Betroffenen scheint es nahezuliegen, die Vorschrift des § 26 Abs. 1 S. 1 BDSG (s. Kap. 11.1) heranzuziehen. Hiernach dürfen personenbezogene Daten in der Bewerbungsphase verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses erforderlich ist. Beim Active Sourcing ist jedoch zu beachten, dass die angesprochene Person an keinem Bewerbungsverfahren teilnimmt und daher noch keine Bewerberin oder Bewerber ist. Es handelt sich beim Active Sourcing vielmehr um ein dem Bewerbungsverfahren zeitlich vorgelagertes Verfahren. Der Anwendungsbereich des § 26 Abs. 1 S. 1 BDSG ist daher weder in persönlicher noch in sachlicher Hinsicht eröffnet.

Hinsichtlich der Rechtmäßigkeit der Verarbeitung war somit zu prüfen, ob eine der in Art. 6 Abs. 1 UAbs. 1 Buchst. a bis f DS-GVO genannten Bedingungen Anwendung findet. Meine Prüfung ergab, dass als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten der Beschwerdeführerin das überwiegende berechtigte Interesse des Verantwortlichen an der Erbringung seiner Personalvermittlungsdienstleistung, mithin Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO, in Betracht kommt.

Art. 6 DS-GVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

(…)

f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (…).

Nach Erwägungsgrund 47 DS-GVO kann die Rechtmäßigkeit der Verarbeitung durch die berechtigten Interessen eines Verantwortlichen, zu denen auch ein wirtschaftliches Interesse zählt, begründet sein. Die vernünftigen Erwartungen der betroffenen Person sind zu berücksichtigen. Dabei ist zu prüfen, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird.

Ausgangspunkt jeder Interessenabwägung im Rahmen des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO sind einerseits das Persönlichkeitsrecht der Betroffenen sowie die Auswirkungen, die eine Verarbeitung der betreffenden Daten für diesen mit sich bringt, und andererseits die Interessen des Verantwortlichen (vgl. BGH Urt. vom 23. Juni 2009 - VI ZR 196/08, NJW 2009, 2888). Bei der Interessenabwägung war insbesondere zu berücksichtigen, dass die Betroffene ihre personenbezogenen Daten auf einer von ihr betriebenen beruflich orientierten Webseite öffentlich zugänglich gemacht hatte. Sie hatte damit ihren Schutzanspruch durch eigenes Tun selbst eingeschränkt.

Öffentlich gemacht sind Daten, soweit diese dem Zugriff einer unbestimmten Anzahl von Personen ohne wesentliche Zulassungsschranke offenstehen (Schulz in Gola/Heckmann, DS-GVO, 3. Aufl. 2022, Art. 9 Rn. 33). Öffentlich gemachte Daten finden sich beispielsweise in frei zugänglich gemachten Bereichen des Internets, auf der eigenen Webseite oder in Meinungsforen. Entscheidend ist, dass die Daten uneingeschränkt frei zugänglich sind und nicht nur innerhalb einer geschlossenen Gruppe zugänglich gemacht wurden.

Selbst wenn die gespeicherten Daten besondere Kategorien personenbezogener Daten (z. B. zur ethnischen Herkunft, zu politischen Meinungen, zu weltanschaulichen Überzeugungen oder zur Gewerkschaftszugehörigkeit) enthielten, wäre das Verbot nach Art. 9 Abs. 1 DS-GVO, solche Daten zu verarbeiten, nach Art. 9 Abs. 2 Buchst. e DS-GVO aufgehoben, wenn es sich um die Verarbeitung öffentlich gemachter personenbezogener Daten handelt.

Art. 9 DS-GVO

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten (…) einer natürlichen Person ist untersagt.

(2) Abs. 1 gilt nicht in folgenden Fällen:

(…)

e) Die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat.

Eine mit Art. 9 Abs. 2 Buchst. e DS-GVO vergleichbare Vorschrift enthält Art. 6 DS-GVO zwar nicht. Wenn aber Art. 9 Abs. 2 Buchst. e DS-GVO eine Ausnahme des Verarbeitungsverbotes für die besonders schutzbedürftigen Datenkategorien des Art. 9 Abs. 1 DS-GVO vorsieht, muss dies erst recht für personenbezogene Daten gelten, die unter den Voraussetzungen des Art. 6 DS-GVO verarbeitet werden können. Der Personaldienstleister konnte die Verarbeitung der personenbezogenen Daten der Betroffenen daher auf Art. 6

Abs. 1 UAbs. 1 Buchst. f DS-GVO, eventuell in Verbindung mit Art. 9 Abs. 2 Buchst. e DS-GVO, stützen. Wer eine eigene, beruflich orientierte Webseite betreibt, muss damit rechnen, dass die bereitgestellten Daten auch von potenziell interessierten Arbeitgebern oder Personalvermittlern für Zwecke einer möglichen Stellenbesetzung oder Personalvermittlungsdienstleistung genutzt werden.

Einhaltung der Informationspflichten nach Art. 14 DS-GVO

Auch ein erheblicher Verstoß gegen den in Art. 5 Abs. 1 Buchst. a DS-GVO enthaltenen Grundsatz der Transparenz, der u. a. durch die Informationspflicht des Art. 14 DS-GVO konkretisiert wird, war nicht gegeben. Art. 14 DS-GVO verpflichtet Verantwortliche, die betroffene Person zu informieren, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden. Dies ist beim Active Sourcing der Fall, da die personenbezogenen Daten – wie im hier zugrundeliegenden Fall – nicht bei der betroffenen Person selbst, sondern aus einer anderen Quelle erhoben werden.

Art. 14 DS-GVO umfasst u. a. die Pflicht zur Information über die gespeicherten personenbezogenen Daten, die Rechtsgrundlage der Verarbeitung, die Kontaktdaten des Datenschutzbeauftragten, die Zwecke der Datenverarbeitung, die Dauer der Speicherung, eine Aufzählung der Betroffenenrechte, das Bestehen eines Beschwerderechts sowie die Quelle, aus der die Daten stammen. Im hier zu prüfenden Fall wurden die Informationspflichten weitgehend beachtet. Es fehlte eine Information zur genauen Herkunft der Daten. Die Datenquelle wurde auf meine Nachfrage hin beauskunftet.

Zusammenfassung und weitere Hinweise für die Praxis

Der Fall zeigt, dass Active Sourcing in Übereinstimmung mit den Bestimmungen des Datenschutzes erfolgen kann. Als Rechtsgrundlage für Datenverarbeitungen kommt insbesondere Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in Betracht; die Vorschriften zum Beschäftigtendatenschutz finden hingegen keine Anwendung.

Sofern Verantwortliche die Datenverarbeitung auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO stützen, ist zwingend eine Interessenabwägung durchzuführen. Hierbei dürfte vor allem relevant sein, ob potentielle Kandidatinnen und Kandidaten ihre personenbezogenen Daten zu beruflichen Zwecken allgemein zugänglich gemacht haben. Die Erwägungen greifen auch für berufsorientierte Netzwerke, sofern die betroffenen Nutzerinnen und Nutzer nicht von der Möglichkeit von Privatsphäre-Einstellungen Gebrauch machen, so dass ihre personenbezogenen Daten allgemein zugänglich sind (Göpfert/

Dußmann, Recruiting und Headhunting in der digitalen Arbeitswelt – Herausforderungen in der arbeitsrechtlichen Praxis, NZA-Beilage 2016, 41, 43). Wurde der Datenzugriff hingegen auf Kontakte beschränkt, mit denen die betroffene Person „vernetzt" ist, kann die Interessenabwägung nur dann zu Gunsten des Verantwortlichen erfolgen, wenn dieser sich bereits bei der „Kontaktanfrage" als Recruiter oder Personalvermittler ausgibt und auf die potenzielle Datenverarbeitung hinweist. Andernfalls ist die Datenverarbeitung auch bei berufsbezogenen sozialen Netzwerken unzulässig, da die Daten nicht „allgemein" zugänglich sind (Auszug aus ArbR Aktuell 2017, 185). Die Verarbeitung von personenbezogenen Daten, die auf einer Webseite oder in einem sozialen Netzwerk zur sozialen Kommunikation veröffentlicht wurden und privaten Charakter haben, stellt hingegen eine Verletzung des Persönlichkeitsrechts dar (vgl. Gola, Das Internet als Quelle der Bewerberdaten, NZA 2019, 654).

Bei Aufnahme der personenbezogenen Daten eines möglichen Bewerbers oder einer Bewerberin in die Datenbank eines Personaldienstleisters treffen diesen die oben beschriebenen Informationspflichten gem. Art. 14 DS-GVO. Ein besonderer Stellenwert kommt hierbei dem Hinweis auf das Widerspruchsrecht (Abs. 2 Buchst. c) und der Nennung der Quelle (Abs. 2 Buchst. f) zu. Ist die Nennung der konkreten Quelle nicht möglich, was bei standardisierten Datenschutzinformationen die Regel sein dürfte, muss zumindest auf Nachfrage des Betroffenen die konkrete Erhebungsquelle benannt werden können. Verantwortliche müssen daher entsprechende Vorkehrungen treffen (s. insgesamt zu den Transparenzpflichten auch die Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 01 der Artikel 29-Datenschutzgruppe).

Das Widerspruchsrecht, auf welches gem. Art. 14 Abs. 2 Buchst. c DS-GVO bei Aufnahme in die Datenbank hinzuweisen ist, regelt Art. 21 DS-GVO. Das Recht auf Widerspruch gegen eine Datenverarbeitung zum Zweck der Personalvermittlung kann jederzeit ausgeübt werden, wobei an die in Abs. 1 geforderte Begründung keine besonderen Anforderungen zu stellen sind. Vielmehr ist der Widerspruch in einer Gesamtschau mit Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO zu betrachten. Äußert eine betroffene Person ein entgegenstehendes Interesse, kann der beabsichtigte Zweck der Personalvermittlung nicht mehr erreicht werden.

12. Internet, Werbung

Die Bedeutung des Internets für das gesellschaftliche Zusammenleben, für die wirtschaftliche Betätigung und die Erfüllung von Verwaltungsaufgaben wird immer wichtiger. Dies gilt nicht nur für die virtuelle Welt, die durch das Internet entstanden ist, sondern durch das Internet der Dinge auch für die körperliche Welt. Grundsätzlich kann jede Tätigkeit in beiden Welten digital erfasst und ausgewertet werden. Dies erhöht die Bedeutung des Datenschutzes zunehmend. Sehr viele Anbieter von Seiten im WWW erfassen Nutzerdaten und erstellen daraus Nutzerprofile (Kap. 12.1). In noch viel stärkerem Maß erfolgt dies durch Anbieter digitaler Plattformen wie z. B. Facebook (Kap. 12.2). Die Profildaten werden für Werbung im Web, aber auch für Werbung durch E-Mail genutzt (Kap. 12.3 bis 12.5). Eine Form des Internets der Dinge sind Sprachassistenten, die besondere Risiken verursachen, wenn sie in Geschäftsräumen genutzt werden (Kap. 12.6). Viele Gewerbetreibende im Internet ermöglichen oder fordern gar die Einrichtung von Online-Accounts, über die sie die Geschäftsbeziehungen abwickeln wollen. Hierdurch entstehen ebenfalls oft unnötige Datenschutzrisiken (Kap. 12.7). Der Betrieb jeder Web-Seite führt zur Verarbeitung personenbezogener Daten. Nicht jedem Betreiber ist aber klar, dass dies für ihn mit Informationspflichten verbunden ist (Kap. 12.8).

12.1 Und täglich grüßt das Nutzerprofil – Datenschutz bei Onlinediensten

Bei vielen Menschen ist der Begriff Datenschutz eng verknüpft mit der Nutzung von Internet- und Telemediendiensten wie z. B. Webseiten, Onlineportalen, Apps oder auch Smart Devices. Entsprechend viele Beschwerden erreichen mich dazu. Die Anbieter solcher Dienste verarbeiten personenbezogene Daten der Nutzer in verschiedenen Konstellationen, besonders häufig geht es dabei um die Erstellung von Nutzerprofilen und die dazu meist erforderlichen Cookies.

Die tagtägliche Nutzung von Internetdiensten geht längst über das „klassische" Surfen auf Webseiten hinaus. Alle mit dem Internet verbundenen Geräte wie z. B. Smartphones, Smart-TV oder auch intelligente Haushaltsgeräte wie z. B. ans WLAN angebundene Heizungsthermostate basieren auf sog. Telemediendiensten. Dass bei der Nutzung solcher Dienste Daten erhoben und verarbeitet werden, die für die Erbringung des jeweiligen Dienstes erforderlich sind, ist für die Nutzer in aller Regel erkenn- und nachvollziehbar. Wer mit einer App die günstigste Reiseverbindung herausfinden möchte, muss

dazu Angaben über Start und Ziel, Reisezeit und ggf. für die Preisbildung relevante Faktoren wie das eigene Alter machen.

Darüber hinaus werden von fast allen solchen Diensten aber auch im Hintergrund Daten erhoben, die nicht für den eigentlichen Zweck des jeweiligen Dienstes benötigt werden und deren Verarbeitung für die Nutzer meist nur schwer erkennbar ist. So erheben viele Diensteanbieter Analysedaten, um herauszufinden, wie genau die Nutzer ihre Dienste verwenden. Anhand dieser Daten können sie ihre Dienste gezielt an die Wünsche der Nutzer und an ihre eigenen Geschäftsinteressen anpassen und beispielsweise Informationen oder Funktionen, die Nutzer besonders häufig suchen oder verwenden, identifizieren und innerhalb einer App prominenter platzieren. Besonders relevant ist vor allem das Sammeln von Daten zur Erstellung von Nutzerprofilen, um auf die persönlichen Interessen des jeweiligen Nutzers zugeschnittene Werbung platzieren zu können. Personalisierte Werbung ist im Internet allgegenwärtig, da damit größere Gewinne erzielt werden als mit nicht personalisierten Anzeigen und sich ein erheblicher Teil der Internetdienste ganz oder teilweise über dieses Geschäftsmodell finanziert.

In aller Regel erheben die Anbieter von Webseiten, Apps oder sonstigen Internetdiensten Nutzerdaten zu diesen Zwecken nicht selbst, sondern bedienen sich dazu spezialisierter Dienstleister, deren Instrumente zur Datenerhebung sie technisch integrieren. Zudem werden häufig auch Tools oder Inhalte von Drittanbietern in die Dienste eingebaut, die vordergründig einen Mehrwert für die Nutzer bieten, im Hintergrund oft aber auch der Erhebung von Daten dienen (z. B. Einbindung von Web-Fonts oder Inhalten aus Social Media- oder Video-Plattformen).

Da schon der Aufruf eines Internetdienstes und alle damit verbundenen Datenverarbeitungen aus technischen Gründen eindeutige Identifikatoren wie z. B. die IP-Adresse des Nutzers erfordern, können die erhobenen Daten immer auch (zumindest potenziell) auf einzelne Personen zurückgeführt werden. Daher sind diese Dienste immer auch datenschutzrechtlich relevant.

Beschwerden, die bei meiner Behörde zu Onlinediensten eingereicht werden, betreffen am häufigsten die Verarbeitung von Nutzerdaten mittels Cookies. Cookies sind auf dem Endgerät des Nutzers gespeicherte Dateien, die in vielen Fällen benötigt werden, um Nutzungsdaten zu sammeln. Auch wenn mittlerweile verschiedene weitere Techniken zu ähnlichen Zwecken verwendet werden und maßgebliche Anbieter wie Google oder Apple an der Ersetzung von Cookies arbeiten, stellen sie noch ein wesentliches Element bei der Verarbeitung von Nutzerdaten im Internet dar und werden von vielen Nutzern auch so wahrgenommen. Im Berichtszeitraum erreichten mich daher Dutzende Beschwerden, die sich gegen den Einsatz von Cookies

generell oder gegen die Gestaltung und die Funktion der allgegenwärtigen Cookie-Banner richteten.

Mit § 25 des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) wurde Ende des Jahres 2021 eine neue gesetzliche Regelung zum Umgang mit Cookies und vergleichbaren Technologien geschaffen, mit deren Umsetzung ich im Berichtszeitraum erstmalig befasst war. Danach erfordert der Einsatz von Cookies in aller Regel eine ausdrückliche Einwilligung der Nutzer, die zumeist beim ersten Aufruf einer Website mit einem Cookie-Banner eingeholt wird. Um den Anbietern von Telemedien Hilfestellungen und Hinweise insbesondere zum rechtmäßigen Einsatz von Cookies zu geben, hat die Datenschutzkonferenz ihre „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien“ (https://www.datenschutzkonferenz-online.de/media/oh/20221130_OH_Telemedien_2021_Version_1_1.pdf) umfassend überarbeitet und an die neue Rechtslage angepasst.

Leider setzen viele Anbieter von Telemedien die Anforderungen aus § 25 TTDSG sowie die datenschutzrechtlichen Anforderungen an die Verarbeitung von Nutzerdaten bisher nur unzureichend um. Entsprechend thematisierten viele Beschwerden fehlende, unzureichende, unverständliche oder technisch nicht korrekt arbeitende Cookie-Banner. Immerhin konnte diesen Beschwerden häufig dadurch abgeholfen werden, dass die Anbieter auf ihre Versäumnisse aufmerksam gemacht wurden und diese daraufhin abgestellt haben.

Unter den häufig in Internetdiensten eingebundenen Tools und Plugins von Drittanbietern stach im Berichtszeitraum besonders der Dienst „Google Fonts“ hervor. Hierbei handelt es sich um verschiedene Schriftarten, die Google unter einer freien Lizenz zur Verfügung stellt. Nicht selten sind diese Schriftarten bereits in Baukästen für Website-Gestaltungen voreingestellt und somit weit verbreitet. Soweit Google Fonts online eingebunden werden, lädt der Browser der Nutzer beim Aufruf der Website diese Schriftarten und nimmt dazu Kontakt mit den Servern von Google auf. Dabei werden personenbezogene Daten der Nutzer an Google übermittelt, so dass hierzu eine Rechtsgrundlage erforderlich ist. Falls daneben eine Übermittlung personenbezogener Daten in die USA stattfindet, sind zusätzlich auch die für Drittlandübermittlungen geltenden Anforderungen zu erfüllen, einschließlich der Anforderungen aus dem Urteil des EuGH in der Rechtssache „Schrems II“ (Urteil vom 16. Juli 2020, C-311/18). Daher empfiehlt es sich, die Schriftarten lokal auf dem eigenen Webserver bereitzustellen. Dies gilt im Übrigen für alle Anbieter von Webfonts.

Im Berichtszeitraum erreichten mich zahlreiche Beratungsanfragen von Websitebetreibern, die Abmahnschreiben erhielten, in denen unter anderem Schadensersatz wegen des Einsatzes von Google Fonts gefordert wurde.

Rechtlich basierten die Abmahnungen auf einem Urteil des Landgerichts München. Dieses hatte den Betreiber einer Website unter anderem zu Schadensersatz in Höhe von 100 Euro wegen des Einsatzes von Google Fonts verurteilt (LG München I vom 20. Januar 2022 – 3 O 17493/20). Zwar konnte ich mangels Zuständigkeit in zivilrechtlichen Streitigkeiten keine individuellen Beratungen durchführen. Die betroffenen Websitebetreiber habe ich jedoch – auch über einen Artikel auf meiner Homepage – auf die oben beschriebene datenschutzrechtliche Problematik sowie mögliche Lösungen hingewiesen.

Inzwischen ermitteln Staatsanwaltschaften gegen mehrere Rechtsanwaltskanzleien, die solche Abmahnschreiben verschickt haben. Es besteht der Verdacht, dass die Abmahnungen in betrügerischer Absicht versandt wurden, ohne dass tatsächlich die Voraussetzungen für einen Schadensersatzanspruch wegen einer Verletzung des Rechts auf informationelle Selbstbestimmung vorgelegen hätten. Auch wenn der Hintergrund dieser Abmahnwelle fragwürdig oder sogar rechtswidrig war, müssen die Betreiber von Webseiten sicherstellen, dass sie Google Fonts in zulässiger Weise einbinden. Andernfalls können Verstöße zwar nicht von unseriösen Abmahnern, aber von den Aufsichtsbehörden verfolgt werden. Daneben setzen sie sich auch der Gefahr berechtigter Schadensersatzforderungen von tatsächlich betroffenen Personen aus.

Nicht selten erreichen mich auch Beschwerden wegen Online-Rezensionen. Auf verschiedenen Plattformen können Kunden, in aller Regel anonym oder unter einem pseudonymen Benutzernamen, Unternehmen bewerten und ihre Erfahrungen aus der Geschäftsbeziehung schildern. Zumeist bieten die Plattformen auch die Möglichkeit an, dass die bewerteten Unternehmen auf Rezensionen antworten und insbesondere bei negativen Bewertungen ihre Sicht der Dinge öffentlich darlegen können. Dabei veröffentlichen immer wieder Unternehmen bewusst Namen oder andere aus dem Geschäftsverhältnis bekannte Daten der Rezensenten, wenn sie Bewertungen anhand ihrer Inhalte auf bestimmte Kunden zurückführen können. Dies dient meist allein dem Zweck, die Rezensentin oder den Rezensenten öffentlich bloßzustellen, und ist datenschutzrechtlich klar unzulässig, wenn die oder der Betroffene seine Identität nicht zuvor bereits selbst öffentlich preisgegeben hat. Auf meine Aufforderung, die Kundendaten umgehend aus ihrer Antwort auf die Rezension zu entfernen und zur Vermeidung empfindlicher Sanktionen vergleichbare Veröffentlichungen zukünftig zu unterlassen, reagieren die angeschriebenen Unternehmen in der Regel schnell.

Mit der hohen Anzahl an Beschwerden aus dem Onlinebereich geht leider auch ein nicht geringer Anteil an missbräuchlichen Beschwerden einher. So erreichen mich immer wieder Eingaben, bei denen klar erkennbar ist,

dass es den Petenten nicht um Verletzungen des Persönlichkeitsrechts, sondern allein um die Verfolgung und Bestrafung eines Kontrahenten (beispielsweise eines Konkurrenten oder ehemaligen Geschäftspartners) durch die Aufsichtsbehörde geht. Zu diesem Zweck wird gezielt nach möglichen Datenschutzverstößen gesucht, wozu sich Websites besonders eignen, da sie von nahezu jedem Unternehmen betrieben werden und stets öffentlich sind. Im Berichtszeitraum hat insbesondere eine Serie von missbräuchlichen Eingaben erheblichen Arbeitsaufwand erzeugt. Dabei wurden unter falschen Identitäten über Monate hinweg dutzende „Beschwerden" gegen verschiedene Websites nach stets ähnlichem Muster eingereicht. Mit ständigen Nachfragen und Drohungen sollte zudem deren zeitnahe Bearbeitung erzwungen werden.

Bei eindeutig missbräuchlichen Beschwerden oder Eingaben von selbst nicht betroffenen Personen liegt es in meinem Ermessen, den (vermeintlichen) Verstößen nachzugehen. Somit ist eine effiziente Aufsicht gewährleistet, die sich nicht instrumentalisieren oder gar ausbremsen lässt. Nichtsdestotrotz kann ich Datenschutzverstöße auch dann verfolgen und abstellen, wenn ich lediglich informelle Hinweise darauf erhalte oder gar durch missbräuchliche Beschwerden darauf aufmerksam gemacht werde.

12.2
Kein Like für Facebook-Seiten

Facebook-Seiten, mit denen sich viele Unternehmen, Vereine, Behörden, Kommunen und andere Stellen in dem sozialen Netzwerk präsentieren, können derzeit nicht datenschutzkonform betrieben werden. Insbesondere die öffentlichen Stellen tragen eine besondere Verantwortung gegenüber den Besucherinnen und Besuchern ihrer Social-Media-Auftritte und sind daher aufgerufen, bei ihrer Öffentlichkeitsarbeit auf datenschutzfreundliche Alternativen zu setzen.

Was sind Facebook-Seiten?

Facebook bietet neben den sog. Profilen, die nur natürliche Personen erstellen und nutzen können, auch sog. Seiten (= Pages, früher Fanpages genannt) an, mit denen Institutionen wie z. B. Unternehmen, Vereine oder staatliche Stellen eigene Präsenzen im Facebook-Netzwerk betreiben können. Sie können darüber insbesondere Mitteilungen und sonstige Inhalte wie Fotos oder Videos teilen, mit Facebook-Nutzern direkt kommunizieren oder interagieren oder Facebook-Werbedienste nutzen.

Auch in Hessen betreiben viele Behörden, Kommunen und andere öffentliche Stellen solche Seiten auf Facebook. Diese werden häufig dazu genutzt,

Informationen aus dem eigenen Geschäftsbereich zu verbreiten, allgemeine Öffentlichkeitsarbeit zu betreiben oder eine niedrigschwellige Kontaktmöglichkeit für Bürgerinnen und Bürger anzubieten.

Warum sind Facebook-Seiten datenschutzrechtlich problematisch?

Mit dem Betrieb von Facebook-Seiten gehen einige datenschutzrechtliche Probleme einher. So können z. B. beim Teilen bestimmter Inhalte oder der öffentlichen Kommunikation auf Facebook personenbezogene Daten gegen den Willen oder sogar ohne das Wissen der Betroffenen weltweit verbreitet werden. Aus datenschutzrechtlicher Sicht weitaus problematischer ist jedoch die Verarbeitung von Nutzerdaten im Hintergrund.

Die Meta Platforms Ireland Ltd. (zuvor: Facebook Ireland Ltd.) als Betreiberin von Facebook sammelt mittels Cookies und ähnlicher Technologien Daten der Nutzer und Besucher von Facebook-Seiten – unabhängig davon, ob sie selbst ein Facebook-Konto besitzen. Ein Teil dieser Daten wird im Rahmen der von Facebook „Insights“ genannten Funktion den Seiten-Betreibern für Zwecke der Webanalyse zur Verfügung gestellt. Diese erhalten so statistische Informationen über die Besucher der jeweiligen Seite. Darüber hinaus erhebt Meta vor allem aber auch für eigene Zwecke Daten, erstellt umfangreiche Nutzerprofile und nutzt sie gewinnbringend, vor allem zur Vermarktung individualisierter Werbung. Der Umfang und das persönlichkeitsrechtliche Risiko dieser Datenverarbeitung sind größer, als den meisten Nutzern und Betreibern von Facebook-Seiten vermutlich bewusst ist. Meta kann mehrere hundert Arten von persönlichen Merkmalen erfassen, speichern, auswerten und zu Werbezwecken nutzen. Schon der Besuch weniger Facebook-Seiten und mit Facebook verknüpfter Webseiten ermöglicht präzise Rückschlüsse auf beispielsweise Alter, Geschlecht, Herkunft, persönlichen Geschmack und möglicherweise sogar sensible Informationen wie sexuelle Orientierung oder politische Einstellung eines einzelnen Nutzenden. Je länger entsprechende Daten gesammelt werden, desto umfassender und genauer werden die Profile zur einzelnen Person.

Dürfen diese Daten erhoben und verarbeitet werden?

Lange war umstritten, ob der Betrieb von Facebook-Seiten/Fanpages gegen datenschutzrechtliche Vorgaben verstößt. Dies zu beurteilen ist nicht zuletzt deshalb schwierig, weil Meta weder den Betreibern und Nutzern von Seiten noch den Aufsichtsbehörden gegenüber offenlegt, welche Datenverarbeitungsvorgänge genau mit Facebook-Seiten verbunden sind.

Inzwischen ist die Rechtslage jedoch durch ein Urteil des EuGH (Urteil vom 5. Juni 2018, C-210/16) sowie mehrere Urteile deutscher Gerichte (insb. BVerwG, Urteil vom 11. September 2019, 6 C 15.18) geklärt. In diesen Verfahren ging es um eine Verfügung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD SH), das einem Unternehmen den Betrieb seiner Fanpage untersagt hatte. Diese Verfügung wurde vom OVG Schleswig-Holstein mit inzwischen rechtskräftigem Urteil schlussendlich für rechtmäßig befunden (Urteil vom 25.11.2021, 4 LB 20/13).

Die ergangenen Urteile beziehen sich grundsätzlich auf den Bescheid des ULD SH aus dem Jahr 2011 und damit auf die zu diesem Zeitpunkt geltende Rechtslage sowie auf den Dienst „Fanpage“, in der Form, in der er damals von Facebook angeboten wurde. Eine von der Datenschutzkonferenz beauftragte Taskforce, bestehend aus spezialisierten Mitarbeitern mehrerer deutscher Datenschutzaufsichtsbehörden, hat jedoch gutachterlich festgestellt, dass sich die in den Urteilen getroffenen Feststellungen auch auf den aktuellen Facebook-Dienst „Seiten“, der den damaligen „Fanpages“ weitgehend entspricht, sowie die heutige Rechtslage übertragen lassen. Obwohl seither mehr als zehn Jahre vergangen sind, hat die Meta Platforms Ireland Ltd. den Dienst nicht an geltendes Recht angepasst.

Von den Gerichten wurde insbesondere festgestellt, dass die datenschutzrechtliche Verantwortung für den Betrieb einer Facebook-Seite nicht alleine bei Meta liegt. Vielmehr sind auch die Betreiber der Seiten gemeinsam mit Meta gem. Art. 26 DS-GVO rechtlich verantwortlich für die damit verbundene Datenverarbeitung.

Aus dieser gemeinsamen Verantwortlichkeit ergeben sich für beide Verantwortliche verschiedene datenschutzrechtliche Pflichten, beispielsweise hinsichtlich der Transparenz und der Rechtmäßigkeit der Datenverarbeitung. Meta kommt seinen diesbezüglichen Pflichten aber weder selbst in ausreichendem Umfang nach, noch stellt es den mitverantwortlichen Seiten-Betreibern die notwendigen Informationen zur Verfügung, die diese benötigen, um wiederum ihren Verpflichtungen nachkommen zu können. So genügt z. B. die von Facebook nach dem Urteil des EuGH bereitgestellte Vereinbarung („Seiten-Insights-Ergänzung bezüglich des Verantwortlichen“) nicht den Anforderungen des Art. 26 DS-GVO (s. auch Beschluss der Datenschutzkonferenz vom 1. April 2019). Auch können die Seiten-Betreiber ihre Informationspflichten nach Art. 13 DS-GVO nicht erfüllen, da Meta auch ihnen gegenüber nicht transparent macht, welche Datenverarbeitung mit dem Betrieb und der Nutzung von Facebook-Seiten genau verbunden ist.

Die von Meta bisher angedachten und teilweise bereits umgesetzten Maßnahmen genügen nicht, um diese Probleme auszuräumen. Auch eine denkbare

Abschaltung der sog. „Insights“ würde nicht dazu führen, dass die datenschutzrechtlichen Anforderungen erfüllt würden. Denn durch die Deaktivierung der Insights-Funktion entfiele nicht die gemeinsame Verantwortlichkeit, die zwischen Meta und den Betreibern einer Facebook-Seite besteht. Die Deaktivierung würde die relevante Datenverarbeitung beim Betrieb einer Fanpage kaum verändern, den Seitenbetreibern würden lediglich aus den – nach wie vor – verarbeiteten Nutzungsdaten keine Statistiken mehr ausgespielt. Weiterhin setzen die Seitenbetreiber durch die Eröffnung ihrer Seite eigenverantwortlich die Ursache für die Erhebung personenbezogener Daten der Besucher ihrer Seite durch Meta, die es ohne den Betrieb der Facebook-Seite wiederum nicht gäbe. Von dieser Datenverarbeitung profitieren die Seitenbetreiber sowie Meta gleichermaßen. Die Seitenbetreiber erhöhen durch die Netzwerkeffekte des sozialen Netzwerkes ihre Reichweite, während Meta basierend auf den Interaktionen der Seitenbesucher spezifische Profile zur zielgerichteten Werbeadressierung anlegen kann. Die Zwecke der Seitenbetreiber und Meta ergänzen sich damit gegenseitig, was für die Annahme eines gemeinsamen Zwecks im Sinn von Art. 26 DS-GVO ausreichend ist.

Zudem ergeben sich auch aus der Übermittlung von Daten in die USA sowie durch den möglichen Zugriff auf Daten europäischer Nutzer durch US-Sicherheitsbehörden datenschutzrechtliche Probleme. Zwar ist die Meta Platforms Ireland Ltd. mit Sitz in der EU Vertragspartner der europäischen Facebook-Kunden, diese ist aber Tochterunternehmen des US-Unternehmens Meta Platforms Inc. (bis 2021: Facebook Inc.). Beide Unternehmen tauschen permanent Daten aus und es ist davon auszugehen, dass dies auch personenbezogene Daten europäischer Nutzender betrifft. Da die weitreichenden Befugnisse amerikanischer Sicherheitsbehörden auch auf Tochterunternehmen von US-Unternehmen mit Sitz im Ausland Anwendung finden, ist zudem ein Zugriff auf bei Meta Platforms Ireland Ltd. gespeicherte Daten durch US-Behörden zumindest möglich. Bisher ist nicht ersichtlich, dass Facebook hinreichende Maßnahmen im Sinn des EuGH (Urteil vom 16.Juli 2020, C 311/18 – „Schrems II“) getroffen hätte, um die Rechte der Betroffenen in einer solchen Konstellation zu schützen.

Auch werden die seit dem 1. Dezember 2021 geltenden Anforderungen an das Setzen und Auslesen von Cookies aus dem TTDSG von den gemeinsam verantwortlichen Seiten-Betreibern und Meta nicht eingehalten. Nach § 25 Abs. 1 S. 1 TTDSG ist u. a. das Setzen und Auslesen von Cookies in der Regel nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen darin eingewilligt hat. Diesen Anforderungen werden Meta und die Fanpage-Betreiber jedoch nicht gerecht, da die von Meta eingeholten Einwilligungen nicht ausreichen und die gesetzlich geregelten Ausnahmen im Falle von Facebook-Seiten nicht einschlägig sind.

Die Verpflichtung aus § 25 TTDSG trifft auch nicht allein Meta, sondern ebenso die Betreiber von Facebook-Seiten selbst, da sie Anbieter von Telemedien im Sinn des § 2 Abs. 2 Nr. 1 TTDSG sind. Sie erbringen zum einen selbst ein Telemedium, da sie eine separat im Netzwerk aufrufbare Seite bereitstellen sowie mit Inhalten befüllen, wirken darüber hinaus durch den Betrieb ihrer Facebook-Seite aber auch am sozialen Netzwerk Facebook mit. Denn dieses lebt gerade davon, dass Facebook-Nutzer mit Facebook-Seiten interagieren und dort Inhalte veröffentlichen. Daher ist auch die inhaltliche Ausgestaltung der Facebook-Seite ein wesentlicher Beitrag zum sozialen Netzwerk.

Alle diese datenschutzrechtlichen Defizite können ohne die aktive Unterstützung durch Meta von den Seiten-Betreibern alleine weder ausgeräumt, noch – beispielsweise durch das Einholen von Einwilligungen – umgangen werden.

Was bedeutet das für die Betreiber von Facebook-Seiten?

Solange Meta die Datenverarbeitung bei Facebook-Seiten nicht

- ausreichend transparent macht,
- den Seiten-Betreibern eine Vereinbarung zur Verfügung stellt, die den Ansprüchen des Art. 26 DS-GVO genügt,
- nachweisbar die Anforderungen des § 25 TTDSG erfüllt,
- sich nachweisbar an die Grenzen zulässiger Datenverarbeitung hält und
- nachweisbar notwendige Schutzmaßnahmen zur Absicherung des Datentransfers in die USA ergreift,

begegnet der Betrieb von Facebook-Seiten erheblichen datenschutzrechtlichen Bedenken.

Die Betreiber von Facebook-Seiten können daher ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nicht nachkommen. Nach der Feststellung des OVG Schleswig-Holstein ist das Betreiben einer Facebook-Seite somit ein „schwerwiegender Verstoß gegen datenschutzrechtliche Vorschriften“.

Die Datenschutzkonferenz hat am 23. März 2022 einen Beschluss getroffen, mit dem die o. g. Punkte festgestellt werden, und ein gemeinsames und einheitliches Vorgehen der Aufsichtsbehörden des Bundes und der Länder vereinbart (https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Facebook_Fanpages.pdf). Der Beschluss folgt auf mehrere Entschließungen und Beschlüsse (u. a. vom 6. Juni 2018, 5. September 2018 und vom 1. April 2019), mit denen die Datenschutzkonferenz seit Jahren immer wieder auf die bestehenden Defizite bei Facebook-Seiten hingewiesen hat.

In dessen Folge habe ich die öffentlichen Stellen in Hessen ausdrücklich auf die nunmehr geklärte Rechtslage hingewiesen und insbesondere gegenüber

der Landesregierung meine Erwartung zum Ausdruck gebracht, dass die öffentlichen Stellen in Hessen keine neuen Facebook-Seiten erstellen und von den Facebook-Seiten, die sie betreiben, zu alternativen, datenschutzrechtlich unbedenklichen Wegen für ihre Öffentlichkeitsarbeit wechseln. Bei einem Wechsel müssen sie sicherstellen, dass die gewählte Alternative keine vergleichbaren Datenschutzprobleme verursacht. Bis dieser Wechsel vollzogen ist, dürfen öffentliche Stellen Informationen nicht exklusiv auf Facebook anbieten, sondern müssen für die Veröffentlichung dieser Informationen immer auch mindestens einen zweiten Kommunikationskanal nutzen, der keine datenschutzrechtlichen Bedenken hervorruft, und auf diesen ausdrücklich hinweisen.

Facebook-Seiten haben für die Öffentlichkeitsarbeit von Behörden und anderen öffentlichen Stellen unbestritten eine große Bedeutung. Dennoch sind die Datenschutzaufsichtsbehörden und damit bin auch ich verpflichtet, dafür Sorge zu tragen, dass die Seitenbetreiber ihrer Verantwortung gerecht werden und die Grundrechte der Besucherinnen und Besucher ihrer Seiten nicht gefährden. Gerade öffentliche Stellen sind an Recht und Gesetz gebunden und erfüllen eine Vorbildfunktion. Daher müssen sie auch in diesem Punkt den Bedenken und der eindeutigen Rechtsprechung Rechnung tragen. Solange internationale Diensteanbieter wie Meta ihren Verpflichtungen aus der DS-GVO nicht gerecht werden, sind die Nutzer von Social-Media-Diensten dazu aufgerufen, für ihre Kommunikation und Veröffentlichungen auf alternative Anbieter und Kommunikationswege zu setzen, die die datenschutzrechtlichen Anforderungen erfüllen.

Der Prozess des Wechsels hin zu datenschutzrechtlich unbedenklichen Alternativen wird dabei durch meine Behörde aktiv begleitet. Dies geschieht insbesondere im Wege der Beratung von Verantwortlichen, aber auch durch direkte Unterstützung der zuständigen Stellen bei der Einrichtung und Etablierung von alternativen Diensten.

12.3
Hohe Hürden für E-Mail-Werbung an Bestandskunden

Für E-Mail-Werbung ist grundsätzlich eine Einwilligung erforderlich. Ausnahmsweise kann bei Bestandskunden stattdessen aber auch eine Interessenabwägung als Rechtsgrundlage dienen. Die aufsichtsbehördliche Praxis zeigt allerdings, dass es vielen Werbetreibenden schwerfällt, die Bedingungen der DS-GVO und des bei der Abwägung ebenfalls zu berücksichtigenden Gesetzes gegen den unlauteren Wettbewerb (UWG) für einwilligungsfreie E-Mail-Werbung zu erfüllen, da hierfür letztlich hohe praktische Hürden zu überwinden sind. Ich empfehle Werbetreibenden daher, stets tragfähige

Einwilligungen für E-Mail-Werbung von Kunden einzuholen und die Ausnahmeregelungen der DS-GVO und des UWG besser nicht in Anspruch zu nehmen.

Für die Verarbeitung einer personenbeziehbaren E-Mail-Adresse zum Versand von E-Mail-Werbung ist grundsätzlich stets eine ausdrückliche, informierte und freiwillige Einwilligung des Adressinhabers nach Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 DS-GVO als Rechtsgrundlage erforderlich. Die Vorschriften der DS-GVO befinden sich hierbei im Gleichklang mit den Regelungen im UWG, wo die Zulässigkeit der Nutzung verschiedener Medien zu Werbezwecken aus wettbewerbsrechtlicher Sicht geregelt wird. Hier ist nach § 7 Abs. 2 Nr. 3 UWG E-Mail-Werbung dann unzulässig, wenn keine vorherige ausdrückliche Einwilligung des Adressaten vorliegt.

Sowohl die DS-GVO als auch das UWG lassen aber bei Bestandskunden unter bestimmten Bedingungen eine Ausnahme von diesem Einwilligungserfordernis zu: Datenschutzrechtlich kann neben der Einwilligung auch die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in Verbindung mit Erwägungsgrund 47 DS-GVO für die Verwendung von E-Mail-Adressen zu Werbezwecken für eigene Produkte oder Dienstleistungen als Rechtsgrundlage dienen, falls es sich um einen Kunden des verantwortlichen Werbetreibenden handelt, mit dem zuvor schon einmal ein Vertrag abgeschlossen wurde und bei dem es möglich ist, dass die E-Mail-Werbung den vernünftigen Erwartungen des betroffenen Kunden entspricht. Damit diese datenschutzrechtliche Abwägung zwischen den berechtigten Interessen des Werbetreibenden und den schutzwürdigen Interessen der betroffenen Person zu Gunsten des E-Mail-Versenders ausgeht, müssen zudem immer auch alle Bedingungen des § 7 Abs. 3 Nr. 1 bis 4 UWG erfüllt sein. Die diesbezüglichen Vorschriften des UWG sind also in die DS-GVO zu integrieren und demzufolge bei der Abwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO zu berücksichtigen.

Werbetreibende, die beim E-Mail-Marketing an eigene Bestandskunden auf eine wirksame Einwilligung verzichten möchten, haben somit folgende Anforderungen des § 7 Abs. 3 Nr. 1 bis 4 UWG kumulativ zu erfüllen, damit die Betroffeneninteressen die berechtigten wirtschaftlichen Interessen an der werblichen Verwendung der E-Mail-Adressen nicht überwiegen:

§ 7 Abs. 3 Nr. 1 UWG

Die zu Werbezwecken verwendete E-Mail-Adresse muss im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden erhoben worden sein.

Viele Unternehmen übersehen, dass diese Vorgabe die werbliche Verarbeitung von E-Mail-Adressen ausschließt, die ein Unternehmen z. B. über eine Interessenten- oder Preisanfrage oder wegen der Anfrage nach einem Kostenvoranschlag oder einem Angebot erhalten hat, da hier kein „Verkauf" stattgefunden hat. E-Mail-Adressen, die aus vorvertraglichen Verhältnissen stammen, sind ohne Einwilligung werblich nicht verwertbar. Und auch bei Verkäufen, die – aus welchen Gründen auch immer – später rückgängig gemacht wurden oder zivilrechtlich unwirksam waren, dürfen die erhobenen E-Mail-Adressen nicht beworben werden. Das Gleiche gilt für E-Mail-Adressen, die nicht direkt vom Kunden stammen, sondern die die Werbetreibenden von Dritten oder aus anderen Quellen erhalten haben.

Als Konsequenz müssen die Verantwortlichen bei der Datenerhebung organisatorische und datenverarbeitungstechnische Vorkehrungen treffen, um in der Lage zu sein, beim E-Mail-Marketing Daten von Kunden mit einer bestehenden Vertragsbeziehung von den Daten anderer betroffener Personen, die aus anderen Kommunikationssituationen erhoben wurden, zu unterscheiden. Nur eine solche Differenzierung, die in den der Aufsichtsbehörde vorliegenden Fällen oftmals unterlassen oder in den zugrundeliegenden edv-technischen Prozessen im Unternehmen nicht korrekt abgebildet wurde, kann gewährleisten, dass nur wettbewerbsrechtlich und damit auch datenschutzrechtlich zulässige E-Mail-Werbung ohne Einwilligung betrieben wird.

§ 7 Abs. 3 Nr. 2 UWG

Die E-Mail-Adresse eines Bestandskunden darf vom verantwortlichen Werbetreibenden nur zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet werden.

Diese Vorschrift verbietet es zum einen, für Waren oder Dienstleistungen anderer Unternehmen E-Mail-Werbung ohne Einwilligung zu betreiben. Dies gilt auch für die Waren oder Dienstleistungen von verbundenen Unternehmen, Geschäftspartnern oder konzernzugehörigen Firmen. Zum anderen ist insbesondere zu beachten, dass in der wettbewerbsrechtlichen Rechtsprechung der Begriff der „Ähnlichkeit" sehr eng ausgelegt wird. Es muss sich dabei letztlich um Waren oder Dienstleistungen handeln, über die zuvor ein Vertrag bestand, oder diese müssen einem sehr ähnlichen Zweck dienen wie die beworbenen. Zulässig ist hier z. B. die Werbung für Güter oder

Dienstleistungen, die austauschbar sind und demselben Zweck dienen. Es darf sich aber auch um Zubehör, Ersatzteile oder Ergänzungen eines bereits gekauften Produkts handeln. Ein Bekleidungsunternehmer darf aber keine Herrenbekleidung per E-Mail bewerben, wenn zuvor Damenbekleidung gekauft wurde, ein Reisebüro darf keine Kulturveranstaltung anpreisen, wenn zuvor nur eine einfache Reise gebucht wurde, und wenn beispielsweise ein Drucker gekauft wurde, darf deswegen nicht automatisch für alle anderen EDV-Produkte eines Unternehmens ohne gesonderte Einwilligung per E-Mail geworben werden.

Um dieser weiteren gesetzlichen Voraussetzung für einwilligungsfreie E-Mail-Werbung gerecht werden zu können, müssen Unternehmen ihr Produkt- und Dienstleistungsportfolio entsprechend bewerten und sehr differenziert nach dem Kriterium der „Ähnlichkeit“ (bzw. „Ersatz“, „Zubehör“, „Ergänzung“) kennzeichnen und vor einer E-Mail-Kampagne mit der jeweiligen Datenherkunft wie unter Nr. 1 dargestellt kombinieren. Nur so kann im Ergebnis für jedes einzelne Werbe-Mailing jeweils eine Empfängerliste zusammengestellt werden, die unter den beiden bisher dargestellten Voraussetzungen per E-Mail einwilligungsfrei beworben werden darf.

§ 7 Abs. 3 Nr. 3 UWG

Der Kunde darf der Verwendung seiner E-Mail-Adresse nicht widersprochen haben.

Diese wettbewerbsrechtliche Bedingung findet sich entsprechend in Art. 21 Abs. 2 und 3 DS-GVO und kann einfach durch das Setzen einer Werbesperre im Datensatz der betroffenen Person in der Kundendatenbank eingehalten werden.

§ 7 Abs. 3 Nr. 4 UWG

Der Kunde muss bei der Erhebung seiner E-Mail-Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen worden sein, dass er der Verwendung für Werbung jederzeit widersprechen kann.

Auch diese Vorschrift hat datenschutzrechtliche Entsprechungen: Nach Art. 13 Abs. 1 Buchst. c DS-GVO muss bei der Datenerhebung über die Verwendungszwecke informiert werden (Datenschutzhinweis) und nach Art. 21 Abs. 4 DS-GVO muss mindestens bei der ersten Werbung auf das Widerspruchsrecht nach Abs. 2 hingewiesen werden. Diese gesetzlichen Anforderungen sind recht einfach zu erfüllen. Auch wenn in Einzelfällen Transparenzdefizite in Datenschutzhinweisen festgestellt wurden, wird über die beabsichtigte werbliche Verwendung erhobener Daten weit überwiegend

korrekt informiert. In Werbe-E-Mails wird üblicherweise mittels eines am Ende der Werbe-E-Mails angebrachten Abmelde-Links auf das Widerspruchsrecht gegen Werbung hingewiesen und Adressinhabern eine einfache Abmeldung vom Werbe-E-Mail-Versand ermöglicht.

Werbetreibende, die auch nur eine der Voraussetzungen des § 7 Abs. 3 UWG nicht erfüllen, können Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO nicht mehr als datenschutzrechtliche Rechtsgrundlage für E-Mail-Werbung in Anspruch nehmen, da ein wirtschaftliches Interesse an ungesetzlicher Werbung nie als berechtigtes Interesse anerkannt werden kann.

Empfehlung

Gerade für größere Unternehmen mit einer umfangreichen Produkt- oder Dienstleistungspalette stellt die Inanspruchnahme der Ausnahmeregelungen von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO und § 7 Abs. 3 UWG für E-Mail-Werbung ohne Einwilligung oftmals eine große Herausforderung dar. Wenn es schon erheblichen organisatorischen und edv-technischen Aufwand bedeutet, die Bedingungen des § 7 Abs.3 Nr. 1 UWG bei der Differenzierung bezüglich der Herkunft von vorhandenen E-Mail-Adressen einzuhalten, gestaltet sich die Kombination mit einer weiteren anschließenden genauen Differenzierung von Produkten oder Produktgruppen nach deren wettbewerbsrechtlichen „Ähnlichkeit“ im Sinn von § 7 Abs. 3 Nr. 2 UWG für breit angelegte und regelmäßige Werbekampagnen noch weitaus problematischer. Die von der Werbewirtschaft gern gesehene Möglichkeit, E-Mail-Adressen ausnahmsweise ohne Einwilligung für Werbung zu verwenden, hält bei genauerem Hinsehen in der Praxis hohe Hürden bereit, die nur mit erheblicher Mühe überwunden werden können.

Zusätzlich ist auch noch zu berücksichtigen, dass Betroffene der E-Mail-Werbung ohne Einwilligung in der Regel ablehnend gegenüberstehen. Sie bringen insbesondere dann keinerlei Verständnis dafür auf, dass ihre E-Mail-Adresse werblich genutzt wird, wenn sie bei ihrer Registrierung als Kunde im WWW-Angebot eines Unternehmens das nicht-vorbelegte Optionsfeld für eine Newsletter-Anmeldung unter dem Registrierungsformular nicht ausgewählt und damit dem Newsletter-Empfang nicht zugestimmt hatten. Diese Kunden legen nach Empfang der ersten nicht ausdrücklich erwünschten Werbe-E-Mail umgehend einen Werbewiderspruch ein. Das Vertrauen zu dem Unternehmen, das bei Neukunden die Grundlage für eine möglichst langfristige Kundenbindung im Interesse des Unternehmens darstellt, wird so schon bei der Erstbestellung durch einwilligungsfreie E-Mail-Werbung empfindlich gestört.

Vor dem Hintergrund der dargestellten rechtlichen und praktischen Schwierigkeiten wird verantwortlichen Werbetreibenden empfohlen, besser auf die Inanspruchnahme der Ausnahmeregelung von dem Einwilligungserfordernis für E-Mail-Werbung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO und § 7 Abs. 3 UWG zu verzichten, als vielfältige rechtliche und praktische Risiken damit einzugehen. E-Mail-Werbung sollte ausschließlich mit ausdrücklicher, informierter und freiwilliger Einwilligung der Adressinhaber betrieben werden.

12.4
Ein Widerspruch gegen Werbung hat kein Haltbarkeitsdatum!

Nach Art. 21 Abs. 2 DS-GVO können Betroffene der Verwendung ihrer Daten zu Werbezwecken widersprechen (Werbe-Widerspruch gegen Direktwerbung). Art. 21 Abs. 3 DS-GVO gibt vor, dass personenbezogene Daten dann nicht mehr zu solchen Zwecken verarbeitet werden dürfen. Ein erneuter Kauf eines Produktes nach Einlegen des Werbewiderspruchs macht diesen nicht unwirksam. Die Wirksamkeit des Widerspruchs hängt auch nicht vom für den jeweiligen Kauf benutzten Vertriebsweg oder dem dahinterstehenden technischen System ab. Die Technik hat sich am Menschen zu orientieren und nicht umgekehrt. Ein einmal gegenüber einem Verantwortlichen eingelegter Werbewiderspruch gilt immer so lange, bis er von der betroffenen Person widerrufen wird.

Im Rahmen meiner Aufsichtstätigkeit wurde ich auf ein Unternehmen aufmerksam, das Kunden in seinen AGB darüber informierte, dass ein eingelegter Werbewiderspruch durch den erneuten Kauf eines Produktes aufgehoben wird. Nach jedem Kauf müsse also erneut ein Werbewiderspruch eingelegt werden, um eine Verwendung der Kundendaten für Werbezwecke nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO zu verhindern.

Das Betroffenenrecht auf Widerspruch gegen die Verarbeitung personenbezogener Daten zu Zwecken der Direktwerbung und die entsprechende gesetzliche Vorgabe für Werbetreibende findet sich in Art. 21 Abs. 2 und 3 DS-GVO:

Art. 21 Abs. 2, 3 DS-GVO

(2) Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.

(3) Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

Ich habe das Unternehmen darauf hingewiesen, dass seine AGB-Informationen und seine darauf basierenden Datenverarbeitungen zu Werbezwecken nicht mit den Vorgaben des Art. 21 Abs. 2 und 3 DS-GVO übereinstimmen und Werbewidersprüche keine Gültigkeitsbegrenzung haben. Insbesondere hebt ein Vertrag über einen Produktkauf die Wirksamkeit des in Anspruch genommenen gesetzlichen Betroffenenrechtes nicht auf.

Im weiteren Verlauf der sich anschließenden Diskussion mit dem werbetreibenden Unternehmen stellte sich zudem heraus, dass es seinen Kunden seine Produkte auf unterschiedlichen Vertriebswegen anbietet und neben einem Ladengeschäft auch noch über einen Online-Shop im WWW und über eine Handy-App verfügt, über die ebenfalls Kundenregistrierungen vorgenommen und Produkte gekauft werden können. Das Unternehmen vertrat hier die rechtsirrige Ansicht, dass ein nach einem Kauf im Online-Shop eingelegter Werbewiderspruch nicht für die Handy-App gelte. Ein Kunde, dessen Daten aufgrund eines Widerspruchs nach einem Kauf im Online-Shop für Werbung gesperrt wurden, dürfe also nach einem Kauf über die Handy-App erneut beworben werden, bis er über die Handy-App ebenfalls einen Werbewiderspruch einlegt. Dies wurde damit begründet, dass für die beiden Vertriebswege zwei unterschiedliche Kundendatenbanken geführt werden, die nicht kompatibel seien und nicht synchronisiert werden könnten.

Ich habe den Verantwortlichen daraufhin verdeutlicht, dass sich die datenschutzrechtlichen Regelungen an den schutzwürdigen Belangen von Betroffenen und deren Inanspruchnahme von gesetzlichen Rechten orientieren und nicht an organisatorischen Defiziten bei verantwortlichen Stellen oder wie vorliegend an der Inkompatibilität technischer Systeme. Wenn es dem Unternehmen aus technischen Gründen nicht möglich ist, eine einheitliche Kundendatenbank für Online-Shop-Kunden und Handy-App-Kunden zu führen, muss das Unternehmen andere technische oder organisatorische Prozesse finden, um die Berücksichtigung von Betroffenenrechten gewährleisten zu können. Das Problem wurde schließlich durch die Einführung einer einheitlichen Sperrdatei gelöst, in die täglich die Werbewidersprüche aus beiden Systemen eingespeist werden und mit der die Versendelisten vor jedem neuen Mailing abgeglichen werden.

12.5
Höflich oder absatzfördernd – E-Mail-Grüße als Werbung

Ein zunächst zuvorkommend erscheinendes „Happy Birthday“, „Frohe Weihnachten“, „Happy Hanukkah“ oder auch „Frohe Ostergrüße“ kann datenschutzrechtlich viele Probleme mit sich bringen, wenn es per E-Mail von Seiten eines Unternehmens versandt wird.

Der Versand von E-Mail-Werbung stellt eine feste Konstante innerhalb des Online-Marketings dar. Die Vorteile des E-Mail-Marketings gegenüber postalischer Werbung sind vor allen Dingen die geringen Kosten und das Potenzial, in kürzester Zeit eine Vielzahl von Personen zu erreichen. Doch häufig kommt bei dieser Form der Werbung der Datenschutz zu kurz.

Zur Beschränkung der E-Mail-Flut, die die eben aufgeführten Vorteile zwangsweise mit sich bringen, und zum Schutz des Persönlichkeitsrechts des Empfängers sind der Kontaktaufnahme mittels Werbe-E-Mails durch den Gesetzgeber enge Grenzen gesetzt.

Datenschutzrechtlich bedeutet dies zunächst, dass zugunsten des Versenders der E-Mail-Glückwünsche eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten vorhanden sein muss. Entscheidend für die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten (wie etwa Geburtsdatum oder Vor- und Zuname und insbesondere E-Mail-Adresse) ist somit nicht das Motiv, sondern ausschließlich, ob eine Rechtsgrundlage besteht.

Die Zulässigkeit von Werbe-E-Mails wird im Wesentlichen bestimmt durch die DS-GVO und das UWG.

Der Versand von Werbe-E-Mails ist unter datenschutzrechtlichen Aspekten zulässig, wenn der Betroffene hierzu eine ausdrückliche, informierte und freiwillige Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 DS-GVO erteilt hat. Die wesentliche wettbewerbsrechtliche Regelung zur Zulässigkeit von E-Mail-Werbung findet sich in § 7 Abs. 2 Nr. 2 UWG. Demzufolge ist E-Mail-Werbung ohne vorherige ausdrückliche Einwilligung grundsätzlich als unzumutbare Belästigung unzulässig.

Liegt ein Verstoß gegen die genannten Regelungen vor, ist die Werbung wettbewerbswidrig. Es besteht sodann ein Unterlassungsanspruch durch die Mitbewerber. Bei dem Betroffenen selbst handelt es sich um einen rechtswidrigen Eingriff in das allgemeine Persönlichkeitsrecht.

Zum Beginn des Berichtszeitraums hat eine in Hessen ansässige Fluggesellschaft Geburtstagsglückwünsche an einen Kunden per E-Mail übermittelt, der bereits im Vorfeld schriftlich jeglicher werblichen Ansprache nach

Art. 21 Abs. 2 DS-GVO widersprochen hatte. Der Betroffene fühlte sein klar geäußertes Widerspruchsrecht missachtet, da seine im Unternehmen gespeicherten personenbezogenen Daten weiterhin zu Zwecken der Direktwerbung verarbeitet wurden.

Die Fluggesellschaft war sich eines Datenschutzverstoßes jedoch gar nicht bewusst, die Übermittlung von Geburtstagsglückwünschen nahm sie nicht als werbliche Handlung wahr.

Was unter den Begriff „Werbung“ fällt, wird von den Gerichten im Zusammenhang mit Direktmarketingmaßnahmen sehr weit verstanden. Werbung ist entsprechend Art. 2 Buchst. a der EU-Richtlinie 2006/114/EG jede direkte oder indirekte Maßnahme, die der Förderung des Absatzes von Produkten und Dienstleistungen oder der Imagepflege des eigenen oder eines fremden Unternehmens dient.

Die Geburtstagsgrüße im vorliegenden Fall enthielten neben den Glückwünschen auch einen Hinweis auf Bonusmeilen, die auf Grund des Geburtstages gutgeschrieben werden könnten, falls in dieser Zeit Reisen über die Fluggesellschaft gebucht würden.

Allein der Versand der Glückwünsche per E-Mail, aber erst Recht der Zusatz zu Bonusmeilen, zielte auf die Absatzförderung des Unternehmens ab und stellt somit Werbung im Sinn der EU-Richtlinie dar. Durch den intensiven Austausch mit der Fluggesellschaft konnte das Verständnis für den Werbeumfang geschärft werden. Folgerichtig wurde die werbliche Ansprache trotz vorliegendem Werbewiderspruch ausdrücklich beanstandet und Maßnahmen nach Art. 58 Abs. 2 DS-GVO in Aussicht gestellt, falls künftig erneut die im Unternehmen zum Betroffenen gespeicherten personenbezogenen Daten zu werblichen Zwecken verarbeitet würden. Auf Grund dessen hat das Unternehmen geeignete technische und organisatorische Maßnahmen getroffen, um den gesetzlichen Anforderungen zukünftig Genüge zu tun.

12.6
Einsatz von Sprachassistenten in Geschäftsräumen

Sprachgesteuerte Assistenzsysteme sind in der Lage, über eine algorithmenbasierte Sprachanalyse menschliche Sprache zu verstehen und sodann entsprechende Assistenzdienste zu erbringen. Gängige Systeme sind etwa Siri von Apple oder Alexa von Amazon. Es ist offensichtlich, dass im Rahmen der Spracherkennung auch eine Verarbeitung personenbezogener Daten unbeteiligter Personen stattfinden kann. Hierbei sind die jeweiligen Vorgaben der DS-GVO zu beachten.

Über eine Beschwerde wurde folgender Fall an mich herangetragen: In einem Ladengeschäft wurde vom Inhaber ein intelligenter Lautsprecher eingesetzt, um Musik abzuspielen. Die betroffene Person äußerte ihr Unbehagen über eine Beeinträchtigung des informationellen Selbstbestimmungsrechts, da unklar sei, inwiefern das gesprochene Wort der Kunden an die Server des Anbieters des Assistenzsystems übertragen wird, um dessen Funktionen anzubieten.

Tatsächlich sendet der Sprachassistent nach seiner Aktivierung durch ein bestimmtes Schlüsselwort die aufgenommenen Sprachdaten an die Server seines Anbieters. Dort transkribiert eine Software die Audiodaten und übermittelt eine Antwort oder setzt eine Funktion um, wie etwa das Abspielen von Musik. Damit findet eine Verarbeitung personenbezogener Daten statt. Je nach Inhalt des gesprochenen Wortes kann es sich sogar um eine Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO handeln, die nach dem Willen des Uniongesetzgebers besonders geschützt sind.

Für den Einsatz eines solchen Assistenzsystems sind daher die Vorgaben der DS-GVO einzuhalten. Hierunter fällt insbesondere das Vorliegen einer Rechtsgrundlage gem. Art. 6 Abs. 1 DS-GVO. Da andere Rechtsgrundlagen nicht ersichtlich sind, kommt eine Einwilligung gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO in Betracht, deren Vorhandensein nach Art. 7 Abs. 1 DS-GVO nachzuweisen ist. Die von der Datenverarbeitung betroffenen Personen sind entsprechend Art. 12 ff. DS-GVO hierüber umfangreich zu informieren. Die Einwilligung muss sich auf sämtliche Verarbeitungsvorgänge beziehen, das gleiche gilt für die Erfüllung der Informationspflichten. Soweit die Server des Anbieters des Assistenzsystems im außereuropäischen Ausland liegen und personenbezogene Daten dorthin übermittelt werden, ist Kapitel V der DS-GVO beachtlich sowie die einschlägige Rechtsprechung, etwa das Urteil des EuGH vom 16. Juli 2020 in der Rechtssache „Schrems II“ (C-311/18).

Im vorliegenden Fall konnte aufgrund entsprechender Hinweise von mir über die nachfolgend dargestellten Konfigurationsmöglichkeiten in den Einstellungen des Sprachassistenten ein angemessenes Schutzniveau erreicht und eine Verarbeitung personenbezogener Daten Betroffener unterbunden werden. Mikrofon und Kamera sollten ausgeschaltet sein. Die vom System erfasste Sprache darf weder gespeichert noch zur Verbesserung des Systems genutzt werden. Ein bereits aufgezeichneter Sprachverlauf ist zu löschen. Daneben bietet sich die Wahl eines seltenen Aktivierungswortes an, um das Risiko einer ungewollten Aktivierung zu minimieren. Soweit das System mittels eines Sprachbefehls aktiviert wird, sollte dies außerhalb der Anwesenheit möglicher betroffener Personen geschehen.

Nachdem der Geschäftsinhaber diese Forderungen umgesetzt hatte, konnte über das System weiter Musik abgespielt werden und die Kunden konnten ohne Beeinträchtigung ihres informationellen Selbstbestimmungsrechts weiter einkaufen.

12.7
Ungenutzte Online-Accounts als Sicherheitsrisiko

Eine immer größer werdende Anzahl von Beschwerden betrifft den Wunsch nach Löschung von Online-Accounts. Denn jedes zusätzliche Onlinekonto erhöht das potenzielle Risiko von Daten- und Identitätsdiebstahl.

In einer zunehmend digitalen Welt bedarf es nicht mehr allein für ein schnelles Shoppingerlebnis eines Online-Accounts, sondern auch für die Reservierung von Tischen in In-Restaurants, das Streaming von Musik und Videos, die Bestellung von Privatfahrten, den Austausch in sozialen Netzwerken oder auch für die Partizipation in Foren.

Bei jeder Registrierung wird ein persönlicher Account angelegt, der einen Benutzernamen und ein Passwort erfordert, um im nächsten Schritt personenbezogene Daten wie den Vor- und Nachnamen zu hinterlegen. Sinn eines solchen Accounts ist die Wiedererkennung des Users und dessen Authentifizierung. Dem Grunde nach stellen Online-Accounts somit vor allen Dingen Sicherheitsmaßnahmen des Websiteverantwortlichen gegenüber seinen Websitenutzern dar. Jedoch hinterlässt der User mit der Einrichtung eines Online-Accounts und der damit einhergehenden Hinterlegung personenbezogener Daten digitale Spuren im World Wide Web (WWW). Weiterhin erhöht sich das Risiko, mit der Anlage immer weiterer Accounts gleiche Benutzernamen und Passwörter für unterschiedliche Dienste zu nutzen.

Entscheidet sich ein User für die Löschung seines Online-Kontos, steht diesem nicht immer die Funktionalität „Account löschen“ in seinen Account-Einstellungen zur Verfügung. Die Anbieter von Webdiensten sind auch nicht dazu verpflichtet, eine einfache Löschung z. B. per eigener Schaltfläche zu ermöglichen. Entsprechend Art. 17 Abs. 1 DS-GVO haben betroffene Personen jedoch das Recht, vom Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden. Das „Wie“ ist allerdings nicht geregelt. Zu beachten ist weiterhin, dass kein Recht auf Löschung von personenbezogenen Daten durch den Verantwortlichen besteht, wenn einer der in Art. 17 Abs. 3 DS-GVO genannten Gründe für eine weitere Speicherung vorliegt. Die Aufbewahrungsfristen für Unternehmen richten sich vornehmlich nach zwei Rechtsgrundlagen, zum einen nach dem Steuerrecht und zum anderen nach dem Handelsrecht. Für Kaufleute

enthält das Handelsgesetzbuch (HGB) entsprechende Vorschriften, z. B. § 257 HGB, und im Bereich des Steuerrechts regelt die Abgabenordnung (AO) überwiegend in § 147 AO die jeweiligen Aufbewahrungspflichten. Somit müssen beispielsweise Unterlagen über getätigte Geschäfte und Zahlungen aufbewahrt werden, soweit diese für die Besteuerung von Bedeutung sind. Jeder Kaufmann ist ferner dazu verpflichtet, Aufzeichnungen über die körperlichen und wertmäßigen Bestandsaufnahmen aller Vermögensgegenstände und Schulden zu führen.

Allerdings unterliegen einige Verantwortliche der irrigen Annahme, dass auch für Online-Konten Aufbewahrungsbestimmungen existieren. Dies ist mitnichten so.

Zu Beginn des Berichtsjahres wandte sich eine Forennutzerin an mich mit der Bitte, sie bei der Durchsetzung ihrer datenschutzrechtlichen Ansprüche zu unterstützen. Nachdem sie sich mit dem Forenbesitzer überworfen hatte, wollte sie ihren Account gelöscht wissen, denn das Forum stellte keine Möglichkeit bereit, eigenständig das einst angelegte Konto zu löschen. Doch statt die Daten der Nutzerin zu löschen, sperrte der Forenbesitzer lediglich das Online-Konto und hielt die hinterlegten personenbezogenen Daten weiter vor. Diese Maßnahme sollte aus Sicht des Forenbetreibers dazu dienen, sein Hausrecht durchzusetzen und sicherzustellen, dass die Forennutzerin keine Möglichkeit mehr hat, auch zukünftig an seinem Forum teilzunehmen. Er sah sich zu dieser Maßnahme veranlasst, da die Forennutzerin seiner Meinung nach gegen die Netiquette-Regeln verstoßen habe.

Aus datenschutzrechtlicher Sicht war der Fall zwar eindeutig und die durchzuführenden Handlungen in Form der Löschung der personenbezogenen Daten und des Accounts selbst zwingend. Allerdings sind in die Betrachtung eines jeden Falles, neben der rein rechtlichen Würdigung, auch die äußerlichen Faktoren und die Bestrebungen und Bedürfnisse der Parteien einzubeziehen und abzuwägen.

Maßnahmen nach Art. 58 Abs. 2 Buchst. c DS-GVO waren somit nicht erforderlich, stattdessen reichte es, dem Beschwerdegegner eine rechtskonforme und für beide Parteien annehmbare Alternative zu empfehlen. Um sein legitimes Bedürfnis, sein Forum zu schützen, durchzusetzen, reichte es, ihm die Führung einer sogenannten „Sperrliste“ anzubieten.

Im Rahmen dieser Sperrliste durfte er die durch die Forennutzerin angegebene E-Mail-Adresse hinterlegen und vorhalten, um im Rahmen von Neuregistrierungen diese abzugleichen und eine unbefugte Neuregistrierung abzuwehren. Somit konnte der Beschwerdegegner den Ausschluss einer zukünftigen Teilhabe durch die Petentin an seinem Forum sicherstellen. Gleichzeitig mit der Einführung der Sperrliste hatte der Beschwerdegegner

alle weiteren personenbezogenen Daten der Beschwerdeführerin samt Account zu löschen.

Alle Parteien waren befriedet und mit der Lösung einverstanden. Die personenbezogenen Daten samt Account wurden gelöscht, die Sperrliste angelegt und die Akte konnte geschlossen werden.

12.8
Datenschutzerklärung für eine Internetseite

Wer im WWW vertreten sein möchte und sich eine Online-Präsenz einrichtet, muss bestimmte Informationspflichten beachten und rechtliche Anforderungen einhalten.

Aufgabe einer Datenschutzerklärung ist es, Nutzer von Online-Diensten darüber zu informieren, in welcher Art und in welchem Umfang Daten von Websitebesuchern verarbeitet werden und welche Rechte sie gegenüber dem Websitebetreiber geltend machen können. Diese Informationen sollen vor allen Dingen für Transparenz sorgen und die informationelle Selbstbestimmung aller betroffenen Personen sicherstellen, selbst zu entscheiden, wie mit seinen Daten umgegangen wird und wer welche Informationen erhält und potenziell auswertet und weiterverarbeitet.

Auf Grund mehrerer bei mir eingegangener Beschwerden schrieb ich einige kleine und mittelständische Unternehmen, aber auch große Holdings innerhalb des Berichtszeitraums an und forderte sie auf, Stellung zu beziehen, wie sie als Anbieter eines Online-Inhaltes und damit als Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO ihrer Informationspflicht nach Art. 13 Abs. 1 und 2 DS-GVO üblicherweise nachkommen, da sie bisher keine solche Datenschutzerklärung vorgehalten hatten.

Häufig führten Verantwortliche aus Unkenntnis heraus aus, dass sie keine Daten im Rahmen ihrer kleinen Online-Präsenz verarbeiten würden und somit keine Datenschutzerklärung benötigten. Doch diese Annahme ist falsch. Die Einbettung eines Kontaktformulars, die Nutzung von Werbebannern, die Entscheidung für Social Media Plugins oder der Einsatz von Cookies haben jedoch die Erhebung und Verarbeitung von personenbezogenen Daten zur Folge. Doch auch bei Verzicht auf diese Anwendungen findet im Hintergrund eine Erhebung personenbezogener Daten statt. Denn bei jedem Aufruf einer Website werden im Hintergrund Metadaten übertragen, um einen technisch reibungslosen Abruf der Inhalte zu ermöglichen. Hierunter fallen auch die IP-Adressen, die auf dem Server des gehosteten Webauftritts in sogenannten Serverlogfiles gespeichert werden. Speichert der Websitebetreiber diese

zusammen mit dem Zugriffszeitpunkt, kann der Anschlussinhaber des Internetzugangs ermittelt werden.

Entsprechend einer Entscheidung des EuGH (vom 19. Oktober 2016, C-582/14) stellen sowohl statische als auch dynamische IP-Adressen personenbezogene Daten dar. Somit werden personenbezogene Daten tatsächlich bereits ab dem Zeitpunkt erhoben, sobald eine Website aufgerufen wird.

Fazit

Jeder Betreiber, der auf seiner Website personenbezogene Daten erhebt, übermittelt, nutzt oder in sonstiger Weise verarbeitet, muss laut DS-GVO eine Datenschutzerklärung auf seiner Seite zur Verfügung stellen. Auch wenn der Verantwortliche selbst auf seiner Website keine Daten der Nutzer abfragt und erfasst, werden personenbezogene Daten durch den im Auftrag des Verantwortlichen tätigen Hostprovider erhoben. Es ist somit beim Betrieb von Websites unmöglich, keine personenbeziehbaren Daten zu erheben, daher ist der Datenschutzhinweis ein Muss.

Achtung

Verantwortlichen, die sich weigern, ihrer Informationspflicht nachzukommen, droht zusätzlich zu möglichen Maßnahmen und Sanktionen durch die Datenschutzaufsicht auch eine Abmahnung durch Mitbewerber. So hat z. B. das OLG Hamburg (Urteil vom 27. Juni 2013; AZ. 3 U 26/12) entschieden, dass eine unzureichende Datenschutzerklärung auf der Website gegen das Wettbewerbsrecht verstößt und damit z. B. durch Mitbewerber abgemahnt werden kann.

Die von mir angeschriebenen Verantwortlichen reagierten nach der Klarstellung zur Notwendigkeit der Einbettung einer Datenschutzerklärung sehr zeitnah, zeigten sich einsichtig und kümmerten sich unmittelbar darum, ihren Informationspflichten nachzukommen.

Eine Holding stellte jedoch die erforderlichen Informationen trotz mehrmaliger Aufforderung nicht bereit und ließ auch keine Bereitschaft erkennen, dies zu tun. Demzufolge habe ich sie nach Art. 58 DS-GVO angewiesen, eine Datenschutzerklärung zu veröffentlichen, und diese Anweisung mit der Festsetzung eines Zwangsgeldes unterstützt. Diese Maßnahmen entfalteten ihre Wirkung. Das Unternehmen besserte nach und bettete eine Datenschutzerklärung in seinen Webauftritt ein.

13. Sozialwesen, Videoüberwachung

Videoüberwachung ist für Unternehmen und öffentliche Stellen sowie Privatpersonen offenbar ein wichtiges Bedürfnis, das der Übersicht und Sicherheit dienen soll. Sie greift aber stark in die Grundrechte erfasster Personen ein und führt daher zu vielen Beschwerden. Ich habe daher immer wieder die Grenzen zulässiger Videoüberwachung zu bestimmen und muss bei ihrer Überschreitung korrigierend eingreifen (Kap. 13.1). Auch im Sozialdatenschutz ergeben sich immer wieder neue Konstellationen der Datenverarbeitung, die datenschutzrechtliche Antworten verlangen. Im Folgenden werden Fragen nach der Befugnis von Jobcentern, die Vorlage von Unterlagen zu verlangen, die auch Daten Dritter enthalten (Kap. 13.2), und Daten über Mietverträge an die Finanzämter weiterzugeben (Kap. 13.3), beantwortet.

13.1
Videoüberwachung – ein Dauerbrenner

Im Jahr 2022 erreichte mich wieder eine Fülle von Beschwerden und Beratungsanfragen zur Videoüberwachung. Im Folgenden resümiere ich die an mein Haus gerichteten Eingaben im Berichtsjahr.

Gesamtschau

Insgesamt gingen zur Videoüberwachung (außer im polizeilichen Bereich) im Berichtszeitraum bei mir 408 Beschwerden und 80 Beratungsanfragen ein. In diesen Fällen war zu prüfen, ob der Anwendungsbereich des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO bei Privatpersonen und Unternehmen oder des Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO in Verbindung mit § 4 HDSIG bei Behörden eröffnet war.

Von den 408 Beschwerden wurden 278 abschließend bearbeitet, bei 130 Beschwerden steht der Abschluss noch aus (Stand: 31.12.2022).

Von den 80 Beratungsanfragen wurden 77 abschließend bearbeitet (Stand: 31.12.2022).

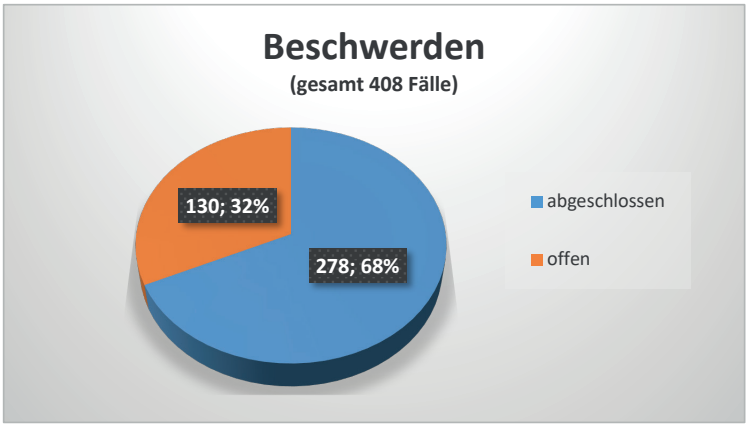

Abbildung 1: Beschwerden Videoüberwachung (Stand: 31.12.2022)

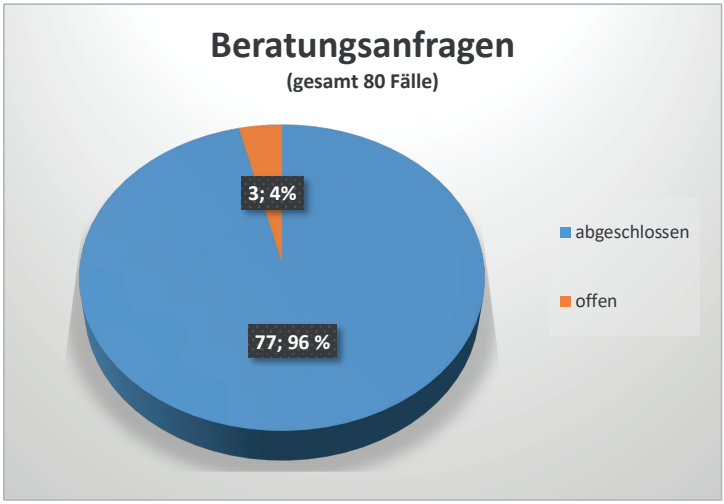

Abbildung 2: Beratungsanfragen Videoüberwachung (Stand: 31.12.2022)

Videoüberwachung im nicht öffentlichen Raum / Zivilsachen:

Für die Prüfung von Videoüberwachungseinrichtungen, die ausschließlich den nicht öffentlichen Raum betreffen (z. B. Videoüberwachung zwischen nachbarschaftlichen Grundstücken, Videoüberwachung, die nicht Gehweg, Straße oder sonstigen öffentlichen Raum betrifft), erfolgt kein datenschut-

zaufsichtsbehördliches Vorgehen durch mich als Ausdruck meines Entschließungsermessens nach Art. 58 Abs. 2 DS-GVO. Nur die Prüfung der Videoüberwachung öffentlicher Räume gehört zum (pflichtigen) Aufgabenbereich der hessischen Datenschutzaufsichtsbehörde nach Art. 57 DS-GVO in Verbindung mit § 4 BDSG und § 4 HDSIG.

Beschwerdeführern steht in Fällen, die ausschließlich den nicht öffentlichen Raum betreffen, der Zivilrechtsweg gegen den Kamerabetreiber nach §§ 823 und 1004 BGB wegen einer möglichen Verletzung des Persönlichkeitsrechts offen. 52 Beschwerden wurden auf den Zivilrechtsweg verwiesen.

Umgang mit Hinweisen

Die auf eine Beschwerde folgende Untersuchung sollte nach Erwägungsgrund 141 zu Art. 77 Abs. 1 DS-GVO so weit gehen, wie dies im Einzelfall angemessen ist. Erforderlich für eine Beschwerde ist eine individuelle Betroffenheit des jeweiligen Beschwerdeführenden.

Trägt ein Beschwerdeführer lediglich vor, dass an einem bestimmten Ort eine Überwachung stattfindet, begründet dies allein keine konkrete Betroffenheit. Es handelt sich dann um einen Hinweis, bei dem kein subjektiver Rechtsanspruch auf eine Befassung und Prüfung durch mich besteht (s. auch VG Wiesbaden, Az. 6K 470/22.WI vom 22. September 2022). Bei etwa zehn Fällen wurde keine konkrete Betroffenheit festgestellt.

Videoüberwachung gastronomischer Betriebe

Häufig werden Videokameras in Restaurants genutzt, um gastronomische Flächen, also Bereiche, in denen sich Besucher aufhalten, zu filmen. Als Gründe werden z. B. Diebstähle und Sachbeschädigungen angeführt, aber auch der schnelle Blick durch die Linse, um Personalmangel zu kompensieren.

Bei der Videoüberwachung gilt – wie auch in anderen Datenschutzbereichen – das Prinzip der Datenminimierung gem. Art. 5 Abs. 1 Buchst. c DS-GVO: Die Datenverarbeitung und die Auswahl und Gestaltung der Technik sind an dem Ziel auszurichten, nur erforderliche Daten zu erheben und so wenig personenbezogene Daten wie möglich zu verarbeiten.

In Restaurants, Cafés und Gastronomieflächen, auch Außengastronomieflächen, ist Videoüberwachung in der Regel unzulässig. Gerade in Bereichen, die man in der Freizeit nutzt und in denen man auch länger verweilt, empfinden Betroffene die Videoüberwachung als störend, was sich in den Beschwerden an mein Haus niederschlägt.

Die Demontage einer Videoüberwachungseinrichtung kann ich – oft leider – nicht anordnen, sondern nur den datenschutzkonformen Betrieb. Hierzu gehört beispielsweise, die Videoüberwachung während der Öffnungszeiten zu untersagen (was in der Regel für die Zwecke „Beweissicherung bei Einbruch/Diebstahl“ ausreicht) oder die Videoeinrichtung beizuschwenken, so dass sie auch nicht den Anschein erweckt, als würde sie während der Öffnungszeiten filmen.

Bedauerlicherweise ist das reine Deaktivieren einer Kamera in der Regel nicht sichtbar, häufig kommt es daher zu Folgebeschwerden. Im Normalfall möchten jedoch Restaurantbetreiber Beschwerden durch ihre Kundschaft vermeiden, so dass auch im Berichtsjahr aus Eigeninteresse Kameras demontiert oder auch eindeutig verdeckt wurden.

So wurde in der Vergangenheit ein Ausflugslokal, welches nachgewiesenermaßen wiederholt von Schäden durch Vandalismus nach Feierabend betroffen war, außerhalb der Öffnungszeiten videoüberwacht. Im Tagesbetrieb wurde die Kamera durch den Wirt verdeckt, so dass die Kamera nicht sichtbar war. Die Hinweisbeschilderung nach Art. 12 ff. DS-GVO wurde entsprechend so angefertigt, dass die Überwachungszeiten transparent angegeben wurden.

Insgesamt 14 Beschwerden richteten sich gegen Gastronomiebetriebe.

Abgaben von Polizeibehörden

Polizeibehörden geben Verfahren an mich ab, bei denen vor Ort festgestellt wird, dass öffentlicher Raum überwacht wird. Auch geben sie Anzeigen an mich ab, bei denen sich Privatpersonen über eine Videoüberwachung des öffentlichen Raumes bei der Polizei beschweren. Hier erfolgt eine Prüfung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO und ggf. die Einleitung weiterer Maßnahmen, möglicherweise auch der Erlass eines Bußgeldbescheids.

Oftmals stoße ich in Prüfverfahren auf Kamerabetreiber, die mir mitteilen, dass Polizeibeamte ihnen nach einem Vorkommnis zu einer Videoüberwachungseinrichtung angeraten haben. Auch ein polizeiliches Anraten einer solchen Einrichtung legitimiert aber datenschutzrechtlich nicht per se die Überwachung des öffentlichen Raumes. Für eine zulässige Videoüberwachung des öffentlichen Raumes bedarf es berechtigter Interessen des Kamerabetreibers, die in einer Abwägung schwerer wiegen als die Interessen der von der Videoüberwachung betroffenen Personen. Dies ist in der Regel nicht der Fall, jedenfalls liegen die Hürden hierfür hoch. Das Recht auf informationelle Selbstbestimmung gewährt jedem Einzelnen grundsätzlich das Recht, sich in der Öffentlichkeit frei bewegen zu können, ohne befürchten zu müssen, zum Gegenstand einer Videoüberwachung zu werden. Regelmäßig ist die

Schutzbedürftigkeit in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise bewegen, aufhalten und miteinander kommunizieren, besonders hoch.

Auch ist zu berücksichtigen, dass die Polizei Bildmaterial einer Videoüberwachung des öffentlichen Raumes durchaus als Beweismittel für z. B. eine Straftat sicherstellen kann. Es erfolgt sodann dennoch eine Abgabe an mich zur Prüfung eines datenschutzrechtlichen Verstoßes, der auch entsprechend einen bußgeldbewehrten Tatbestand erfüllen und geahndet werden kann. Im Berichtsjahr erreichten mich 19 Verfahren, die von der Polizei (+ 53 Verfahren von Ordnungsbehörden) abgegeben wurden.

Videoüberwachung „im Wald und auf der Heide“

Die Videoüberwachung mittels Tierbeobachtungskameras war bereits in vergangenen Tätigkeitsberichten (z. B. ausführlich im 43. Tätigkeitsbericht) Thema. Insgesamt erreichten mich im Berichtszeitraum acht Beschwerden zu diesem Themengebiet.

Im Jahr 2012 wurde in Abstimmung mit dem Hessischen Ministerium für Umwelt, Energie, Landwirtschaft und Verbraucherschutz ein Merkblatt zum Betrieb von Tierbeobachtungskameras erstellt. Dieses Merkblatt wurde im Berichtsjahr überarbeitet und konkretisiert. Mit meiner Unterstützung veröffentlichte das Ministerium mit Stand 1. April 2022 das Merkblatt zum datenschutzkonformen Betrieb von Tierbeobachtungskameras im öffentlich zugänglichen Raum in der freien Landschaft.

Das Merkblatt verfolgt folgenden allgemeinen Grundsatz:

Das Betreten der freien Landschaft auf Straßen und Wegen sowie auf ungenutzten Grundflächen ist zum Zweck der Erholung gem. § 59 des Gesetzes über Naturschutz und Landschaftspflege (Bundesnaturschutzgesetz) allen gestattet. Das Betreten des Waldes ist nach § 15 Abs. 1 Hessisches Waldgesetz und § 14 Abs. 2 Bundeswaldgesetz zum Zwecke der Erholung grundsätzlich jedem erlaubt, so dass der Wald – selbst im Privateigentum – als öffentlich-zugänglicher Raum gilt, sofern kein erkennbares Betretungsverbot besteht.

Für die Überwachung von Flächen in der freien Landschaft (Feldflur und Wald) mittels einer Tierbeobachtungskamera (Wildkamera, Fotofalle, Drohne etc.) gilt Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO. Danach ist die Verarbeitung nur rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person,

die den Schutz personenbezogener Daten erfordern, überwiegen. Das rein private Betreiben von Tierbeobachtungskameras im öffentlich zugänglichen Raum und somit auch in der freien Landschaft, das heißt im Wald und in der Feldflur, ist datenschutzrechtlich grundsätzlich – auch z. B. zum Schutz von Eigentum – nicht erlaubt. Liegt im Ausnahmefall ein berechtigtes Interesse des Überwachenden vor, dem kein überwiegendes schutzwürdiges Interesse der von der Überwachung betroffenen Person entgegensteht, kann eine Überwachung mit einer Tierbeobachtungskamera zulässig sein.

Es gelten folgende spezielle Grundregeln:

1. Für den Bereich des Waldes ist im Hinblick auf die forstliche Bewirtschaftung grundsätzlich davon auszugehen, dass in der Regel kein berechtigtes Interesse für eine Videoüberwachung vorliegt.
2. Im Hinblick auf die Jagdausübung ist überwiegend nicht von einem berechtigten Interesse für eine Videoüberwachung auszugehen. Dies gilt gleichermaßen für Kirrungen, da grundsätzlich mildere Mittel anwendbar sind.
3. Als mögliche Ausnahmen, die ein berechtigtes Interesse rechtfertigen, gelten Forschungsprojekte sowie hilfsweise der Einsatz von Tierbeobachtungskameras zur Verhinderung übermäßigen Wildschadens gem. § 27 Bundesjagdgesetz (Anordnung zur Reduzierung des Wildbestandes durch die zuständige Behörde). Auch zur Seuchenbekämpfung in von Behörden ausgerufenen Gefährdungszonen kann der Einsatz der Tierbeobachtungskameras für eine notwendige Reduktion bzw. für unterstützende Detektionen hilfreich sein. In diesen Fällen sind ebenfalls die nachfolgenden Maßnahmen zu berücksichtigen.
4. Beim Einsatz von Tierbeobachtungskameras im Rahmen von behördlich beauftragten oder genehmigten Untersuchungen wie Monitoring-Projekten u. a. ist von einem berechtigten Interesse auszugehen.
5. Vor Einsatz einer Tierbeobachtungskamera ist immer zu prüfen, ob mildere Mittel in Frage kommen (z. B. Wilduhren). Sofern mildere Mittel möglich sind, sind diese anzuwenden.

Es gelten folgende Umsetzungshinweise für den Einsatz von Tierbeobachtungskameras bei Vorliegen eines berechtigten Interesses:

1. Eine Aufnahme von Menschen sollte wenig wahrscheinlich sein und mit allen verfügbaren Mitteln verhindert werden, z. B. durch
   – den Einsatz von Tierbeobachtungskameras, die selbstständig er-

kennen, ob es sich bei dem Objekt um einen Menschen handelt, und diesen Bereich vollständig aus dem Bild tilgen,

- das Anbringen der Kamera auf maximal 1 Meter Höhe,
- die Ausrichtung direkt auf den Boden,
- die Ausrichtung gegen den Himmel (Vogelerkennungskameras zur Vermeidung von Vogelschlag z. B. an Windenergieanlagen).

2. Bei der Einrichtung der Tierbeobachtungskamera ist auf Datensparsamkeit zu achten (z. B. keine Videosequenzen, Einzelbilder mit einigen Sekunden Abstand aufnehmen, geringe Auflösung der Kamera).
3. Bereiche, die sich in unmittelbarer Nähe zu einer Grillstelle und insbesondere einem Spielplatz befinden, dürfen nicht überwacht werden.
4. In unmittelbarer Nähe zu Wegen (z. B. zur wissenschaftlichen Vogel-, Wolf- oder Luchsbeobachtung) müssen besondere Maßnahmen getroffen werden, um Aufnahmen von Personen zu verhindern (z. B. ggf. Ausrichtung auf den Boden oder in den Himmel, ggf. Überwachung ausschließlich nachts).
5. Ist die Überwachung von Tieren bei Nacht geplant, ist die Kamera tagsüber auszuschalten.
6. Die Hinweisbeschilderung mit den Informationspflichten gem. Art. 13 DS-GVO (u. a. Name und Kontaktdaten des Verantwortlichen, Zwecke und Rechtsgrundlage der Datenverarbeitung) muss gut sichtbar angebracht werden.

Speicherung von Aufnahmen

Gespeicherte Daten sind nach Art. 17 Abs. 1 Buchst. a DS-GVO unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht weiter erforderlich sind oder schutzwürdige Interessen Betroffener einer weiteren Speicherung entgegenstehen. Der EDSA geht von einer Speicherdauer von maximal 72 Stunden aus (Guidelines 3/2019 on processing of personal data through video devices, Adopted on 29 January 2020, Rn. 121).
Ein Verstoß gegen die Rechtmäßigkeit der Verarbeitung sowie eine mangelnde Transparenz (fehlende Hinweisbeschilderung) erfüllen den Bußgeldtatbestand nach Art. 83 Abs. 5 DS-GVO.

Themenverteilung bei der Aufsicht über Videoüberwachung

In der Gesamtschau ergibt sich im Berichtsjahr thematisch folgende Aufteilung:

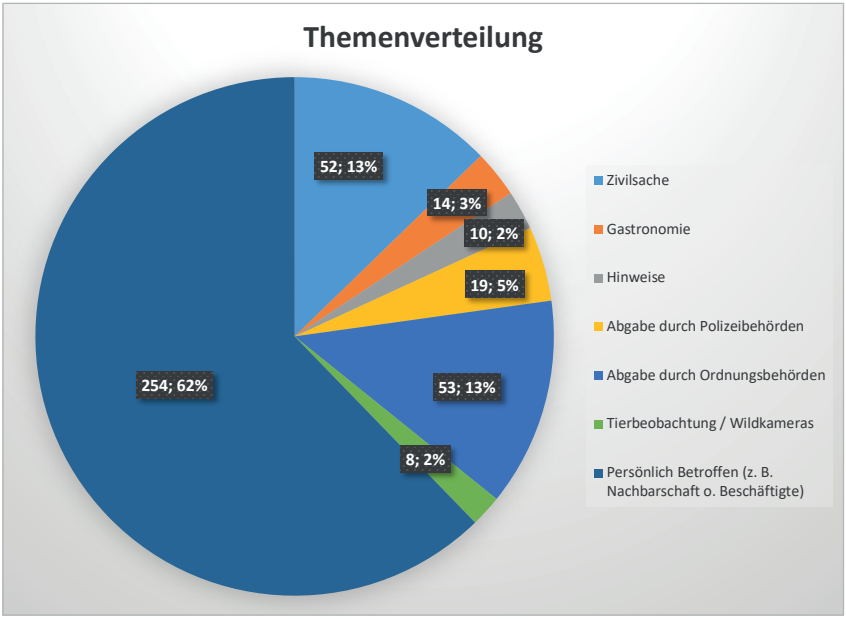

Abbildung 3: Herkunft/Ursachen der Beschwerden in der Videoüberwachung

13.2
(Sozial-)Datenschutz gegenüber selbstständigen SGB II-„Aufstockern“

Im Rahmen der örtlichen Prüfung der Anspruchsvoraussetzungen auf SGB II-Leistungen verlangen hessische Optionskommunen von selbstständigen Anspruchsstellerinnen oder Anspruchsstellern oftmals auch Nachweise in Form von deren Geschäftsunterlagen, mitunter auch von Rechnungen, die diese gegenüber Dritten gestellt haben. Dies kann zur Leistungsprüfung erforderlich sein und stellt dann keinen Verstoß gegen (sozial-)datenschutzrechtliche Vorgaben, wie z. B. eine unbefugte Offenbarung von Daten Dritter, dar, wenn für das Jobcenter die Prüfung und Zuordnung der Einnahmen und Ausgaben der Selbstständigen auf andere, weniger eingriffsintensive Weise nicht möglich ist.

Sachverhalt

Regelmäßig erreichen mich Eingaben von Betroffenen, die als Selbstständige (sog.) aufstockende Leistungen nach dem SGB II beantragen müssen und dann vom für sie zuständigen Jobcenter im Rahmen ihrer Mitwirkungspflichten u. a. mit der Forderung konfrontiert werden, dem Jobcenter Rechnungen vorzulegen, die sie für ihre selbstständigen Tätigkeiten gegenüber Dritten gestellt haben. Die Betroffenen sind in Sorge, ob sie damit nicht einen – ggf. bußgeldbewehrten – Datenschutzverstoß begehen oder gar zu einem solchen aufgefordert würden. Schließlich offenbaren sie Daten von Dritten, nämlich den Empfängerinnen oder Empfängern von Rechnungen (wie z. B. Name, Postadresse, Kundennummer), wenn sie ihre selbst gestellten Rechnungen zum Nachweis ihrer Tätigkeiten vorlegen.

Rechtliche Bewertung

Aufstockende, selbstständige Antragstellerinnen oder Antragsteller oder Leistungsempfängerinnen oder Leistungsempfänger sind grundsätzlich dann nicht zur Vorlage von Daten Dritter verpflichtet, wenn die Prüfung und Zuordnung ihrer Einnahmen und Ausgaben aus ihrer selbstständigen Tätigkeit dem zuständigen Jobcenter (auch) auf andere Weise möglich ist.

Darüber hinaus ist zur Wahrung des Sozialdatenschutzes zu beachten, dass Jobcenter nur die Daten erheben dürfen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Ob es für die Berechnung des Leistungsanspruchs in jedem Fall im Sinn des § 67a Abs. 1 Satz 1 SGB X erforderlich ist, neben den ggf. von der antragstellenden Person eingereichten Kontoauszügen und so nachgewiesenen Ein- und Ausgaben auch einzelne Rechnungen ungeschwärzt vorzulegen, dürfte fraglich sein.

§ 67a Abs. 1 SGB X

(1) Die Erhebung von Sozialdaten durch die in § 35 des Ersten Buches genannten Stellen ist zulässig, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle nach diesem Gesetzbuch erforderlich ist. Dies gilt auch für die Erhebung der besonderen Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679. § 22 Absatz 2 des Bundesdatenschutzgesetzes gilt entsprechend.

Das Jobcenter darf daher die Vorlage der Rechnungen nur dann verlangen, wenn im konkreten Einzelfall andere Unterlagen der antragstellenden Person ohne personenbezogene Daten Dritter unzureichend sind, um die Anspruchsvoraussetzungen nachzuweisen.

Mit Blick auf die antragstellende Person ist zu prüfen, ob sie Geschäftsunterlagen mit Daten Dritter dem Jobcenter vorlegen darf, um zur sachgemäßen Aufklärung des Leistungsanspruchs beizutragen und in den Genuss der Sozialleistungen zu gelangen. Hierfür könnte Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO eine Rechtsgrundlage sein.

Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

(…)

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Die berechtigten Interessen des Verantwortlichen, hier der Antragstellerin oder des Antragstellers auf (die Gewährung von) Sozialleistungen, liegen in der Wahrnehmung des grundrechtlich geschützten Anspruchs auf Wahrung eines menschenwürdigen Existenzminimums. Dieses soll durch die Gewährung der Leistungen nach dem SGB II gesichert werden, so dass die Antragstellerin oder der Antragsteller ein berechtigtes Interesse daran hat, dass die Bewilligungsbehörde (das Jobcenter) in die Lage versetzt wird, anhand der vorgelegten Unterlagen den Anspruch zu prüfen und festzustellen.

Die Offenlegung der Daten muss für die Verfolgung des berechtigten Interesses erforderlich sein. Wenn das Jobcenter die Vorlage der Unterlagen fordert und die Antragstellerin oder der Antragsteller mit einer Ablehnung ihres bzw. seines Antrags rechnen muss, wenn sie oder er diese Forderung nicht erfüllt. Für sie oder ihn stellt sich die Offenbarung der personenbezogenen Daten Dritter als erforderlich dar. Antragsteller sind nicht verpflichtet, eine Ablehnung ihres Antrags in Kauf zu nehmen und dann inzidenter im Rahmen einer Verpflichtungsklage die Erforderlichkeit der verweigerten Vorlage der Daten gerichtlich überprüfen zu lassen.

Im Rahmen der erforderlichen Interessenabwägung ist auch zu berücksichtigen, dass die in den Unterlagen enthaltenen Daten, die dem Jobcenter im Rahmen der Antragstellung bekannt werden, dem Sozialgeheimnis unterliegen. Die weitere Verarbeitung durch den Sozialleistungsträger unterliegt den besonders strengen datenschutzrechtlichen Regelungen des SGB. Aufgabe und Zweck der Verarbeitung durch den Sozialleistungsträger ist ausschließlich die Prüfung des Anspruchs auf Sozialleistungen.

Die Datenverarbeitung durch den Verantwortlichen – hier also: die Übermittlung von Rechnungen der Antragstellerin oder des Antragstellers an den Sozialleistungsträger – kann zur Wahrung der Interessen der Antragstellerin oder des Antragstellers und nach erfolgter Interessenabwägung im Ergebnis demnach als datenschutzrechtlich zulässig eingeordnet werden.

Fraglich bleibt dann noch das mögliche Bestehen einer Pflicht der aufstockenden Leistungsempfängerin oder des aufstockenden Leistungsempfängers, den betroffenen Personen die Weiterleitung ihrer Daten an das Jobcenter gemäß Art. 13 Abs. 1 Buchst. e DS-GVO mitzuteilen.

Art. 13 Abs. 1 lit. e DS-GVO

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

(…)

e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (…).

Zwar könnte danach grundsätzlich eine Informationspflicht bestehen. Zu beachten ist jedoch, dass gemäß Art. 23 Abs. 1 Buchst. i DS-GVO diese Pflicht zum Schutz der Rechte und Freiheiten anderer Personen, zu denen auch der Verantwortliche zählt, beschränkt werden kann.

Art. 23 Abs. 1 lit. i DS-GVO

(1) Durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche oder der Auftragsverarbeiter unterliegt, können die Pflichten und Rechte gemäß den Artikeln 12 bis 22 und Artikel 34 sowie Artikel 5, insofern dessen Bestimmungen den in den Artikeln 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, im Wege von Gesetzgebungsmaßnahmen beschränkt werden, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die Folgendes sicherstellt:

(…)

i) den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen; (…)

Diese Beschränkung findet sich im nationalen Recht in § 32 Abs. 1 Nr. 4 BDSG.

§ 32 Abs. 1 BDSG

(1) Die Pflicht zur Information der betroffenen Person gemäß Artikel 13 Absatz 3 der Verordnung (EU) 679/2016 besteht ergänzend zu der in Artikel 13 Absatz 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

(…)

4. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen (…).

Nach § 32 Abs. 1 Nr. 4 BDSG besteht keine Pflicht zur Information der betroffenen Person. Die Antragsteller könnten gehindert sein, ihren grundrechtlich geschützten Anspruch auf Wahrung eines menschenwürdigen Existenzminimums geltend zu machen, wenn sie dadurch ihren Sozialleistungsbezug gegenüber ihren Kunden, Geschäftspartnern, Lieferanten und Mitarbeitern offenbaren und daraus folgend negative Auswirkungen auf ihre selbstständige Tätigkeit befürchten müssten. Auch hier dürfte die erforderliche Interessenabwägung grundsätzlich zugunsten der aufstockenden Selbstständigen ausfallen. Insofern ist eine Informationspflicht des aufstockenden Selbstständigen zu verneinen.

13.3
Weitergabe von Vermieterdaten an Finanzbehörden durch das Jobcenter oder Sozialamt

Eine Weitergabe von Vermieterdaten an Finanzbehörden in Fällen, in denen Zweifel an tatsächlich existierenden Mietverträgen, insbesondere zwischen Familienangehörigen, bestehen, ist im Regelfall datenschutzrechtlich nicht vertretbar. Ein solches Mittel zur beabsichtigten Feststellung, insbesondere ob tatsächlich Mietzahlungen geleistet werden, steht dem Jobcenter oder dem Sozialamt grundsätzlich nicht zur Verfügung.

Sachverhalt

In einer Beratungsanfrage wandte sich eine hessische Landkreisverwaltung an mich: Dort komme es in der Sozialverwaltung im Anwendungsbereich des SGB XII (3. und 4. Kapitel) vereinzelt vor, dass die Sachbearbeitung erhebliche Zweifel an der Wirksamkeit von geschlossenen Mietverträgen, insbesondere zwischen Familienangehörigen habe.

Gleichzeitig bestehe dabei auf Seiten des Sozialhilfeträgers nicht immer die Möglichkeit, die geforderte Miete abzulehnen. Um zukünftig einen (po-

tenziellen) Leistungsmissbrauch zu verhindern, gebe es Überlegungen, die angegebenen Vermieterdaten bei Verdachtsfällen an die zuständige Finanzbehörde weiterzugeben.

Grundlage hierfür könne § 71 Abs. 1 Nr. 3 SGB X in Verbindung mit § 116 AO (Anzeige von Steuerstraftaten) sein. § 116 AO sieht vor, dass Gerichte und die Behörden von Bund, Ländern und kommunalen Trägern der öffentlichen Verwaltung Tatsachen, die sie dienstlich erfahren und die den Verdacht einer Steuerstraftat begründen, der Finanzbehörde mitzuteilen haben. Problematisch könnte aus Sicht des Landkreises sein, dass zwar Daten weitergegeben würden, die beim Sozialhilfeempfänger erhoben worden seien (z. B. Mietvertrag, Mietbescheinigung), aber dadurch auch die Daten des Vermieters (Dritter) weitergegeben würden, wenn z. B. ein kollusives Zusammenwirken beim Mietvertrag nahe liege oder der Verdacht, dass der Vermieter die Einkünfte aus dem Mietvertrag nicht beim Finanzamt angebe.

Zu dieser Fragestellung hat der Landkreis um meine datenschutzrechtliche Stellungnahme gebeten.

Rechtliche Bewertung

Eine Weitergabe von Vermieterdaten an die Finanzbehörden für die beschriebene Fallkonstellation auf Basis von § 71 Abs. 1 Nr. 3 SGB X in Verbindung mit § 116 AO ist im Regelfall nicht zu vertreten.

Dies ergibt sich datenschutzrechtlich aus der Betrachtung dieser beiden Vorschriften.

§ 71 Abs. 1 Nr. 3 SGB X

(1) Eine Übermittlung von Sozialdaten ist zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Mitteilungspflichten (…),

3. zur Sicherung des Steueraufkommens nach § 22a des Einkommensteuergesetzes und den §§ 93, 97, 105, 111 Absatz 1 und 5, § 116 der Abgabenordnung und § 32b Absatz 3 des Einkommensteuergesetzes, soweit diese Vorschriften unmittelbar anwendbar sind, und zur Mitteilung von Daten der ausländischen Unternehmen, die auf Grund bilateraler Regierungsvereinbarungen über die Beschäftigung von Arbeitnehmern zur Ausführung von Werkverträgen tätig werden, nach § 93a der Abgabenordnung, (…).

§ 116 Abs. 1 AO

(1) Gerichte und die Behörden von Bund, Ländern und kommunalen Trägern der öffentlichen Verwaltung, die nicht Finanzbehörden sind, haben Tatsachen, die sie dienstlich erfahren und die auf eine Steuerstraftat schließen lassen, dem Bundeszentralamt für Steuern oder, soweit bekannt, den für das Steuerstrafverfahren zuständigen Finanzbehörden mitzuteilen.

Soweit die für das Steuerstrafverfahren zuständigen Finanzbehörden nicht bereits erkennbar unmittelbar informiert worden sind, teilt das Bundeszentralamt für Steuern ihnen diese Tatsachen mit. Die für das Steuerstrafverfahren zuständigen Finanzbehörden, ausgenommen die Behörden der Bundeszollverwaltung, übermitteln die Mitteilung an das Bundeszentralamt für Steuern, soweit dieses nicht bereits erkennbar unmittelbar in Kenntnis gesetzt worden ist. (…)

Meine ablehnende Haltung begründet sich vor allem aus dem Wortlaut von § 116 Abs. 1 AO, der von Tatsachen ausgeht, die dienstlich erfahren werden und einen Verdacht auf eine Steuerstraftat begründen. Dem ausdrücklichen Gesetzeswortlaut nach reichen (erhebliche) Zweifel der Sachbearbeitung gerade nicht aus. „Nur" bei Tatsachen ist eine Mitteilung an das Finanzamt (von Amts wegen) angezeigt. Diese Anzeigepflicht setzt das auf festgestellten Tatsachen beruhende Vorhandensein konkreter Verdachtsmomente voraus; bloße Vermutungen begründen keine Mitteilungspflicht.

Dem Landkreis als verantwortlicher Stelle muss (auch in dieser Fallkonstellation) darüber hinaus auch bewusst sein, dass er eine Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO – zumindest mir gegenüber als für ihn zuständige hessische Datenschutzaufsichtsbehörde – hat, die er entsprechend (und objektiv nachvollziehbar) belegen können müsste.

Art 5. Abs. 2 DS-GVO

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Einer dritten Person Steuerhinterziehung oder eine andere Steuerstraftat zu unterstellen, ist ein schwerer Vorwurf, die Hürden hierfür müssen entsprechend hoch gesetzt sein.

Im Übrigen wäre es – einmal vorausgesetzt, in einem Einzelfall könnte eine Übermittlung auf der Grundlage eines auf festgestellten Tatsachen beruhenden Verdachts nach den genannten Vorschriften zulässig sein – der Kreisverwaltung auch nur möglich, „lediglich" eine Datenübermittlung hin zum Finanzamt vorzunehmen. Denn umgekehrt wäre noch nichts darüber gesagt, ob der Finanzverwaltung wiederum eine Übermittlungsbefugnis zur Verfügung stünde, die es ihr gestatten würde, der Sozialverwaltung dann – in etwa – mitzuteilen: „Ja, Frau/Herr XY gibt in ihrer/seiner jährlichen Steuererklärung Mieteinnahmen für die Wohnung ABC von Frau/Herrn DEF an" (oder eben nicht). Die Sozialverwaltung bliebe also weiterhin im Unklaren und erreichte ihr „Ziel" einer ordnungsgemäßen Fallprüfung so nicht.

Ich habe der Kreisverwaltung abschließend angeboten, sollte es aktuell speziell gelagerte und konkrete Einzelfälle in der Sozialverwaltung geben, diese zusammen mit ihr auf ihre datenschutzrechtliche Zulässigkeit hin zu überprüfen. Von diesem Angebot hat die Sozialverwaltung bisher noch keinen Gebrauch gemacht.

14. Wirtschaft, Banken, Auskunfteien, Selbstständige

Der große Bereich der Wirtschaft, der Banken, der Auskunfteien und der Selbstständigen verursacht vielfältige Fragen des Datenschutzes. Auch für den Berichtszeitraum sind Bewertungen zu sehr unterschiedlichen Datenschutzthemen zu berichten. In diesem Kapitel geht es um Steuerberater (Kap. 14.1), Banken (Kap. 14.2), Auskunfteien (Kap. 14.3) und zwei Geschäftsmodelle und deren Datenverarbeitungsvorgänge, die relativ innovativ sind (Kap. 14.4 und 14.5)

14.1
Softwareüberlassung durch Steuerberater

IT-Systeme, die ein Steuerberater seinen Mandanten zur sicheren Übermittlung von personenbezogenen Daten ohne Gewinnerzielungsabsicht zur Verfügung stellt, unterfallen nicht den Anforderungen des Art. 28 DS-GVO.

Mich erreichen immer wieder Anfragen zur Anwendbarkeit des Art. 28 DS-GVO auf konkrete Sachverhalte. Hintergrund ist hierbei immer die Frage, ob für einen konkreten Sachverhalt der Abschluss eines Vertrages im Sinn des Art. 28 Abs. 3 DS-GVO erforderlich ist oder nicht.

Diesmal erreichte mich die Anfrage eines Steuerberaters. Der Steuerberater stellt seinen Mandanten ein System zur Verfügung, mit dem die Mandanten Dokumente in einen Cloud-Speicher laden können. Der Steuerberater übernimmt die vom Mandanten in den Cloud-Speicher geladenen Dateien dann in seine IT-Systeme. Das System dient vor allem der sicheren Übertragung von vertraulichen Unterlagen in einer geschützten und verschlüsselten Umgebung. Zwar wird vom Steuerberater für die Nutzung des Systems durch die Mandanten eine Vergütung verlangt. Diese orientiert sich aber an den Selbstkosten. Eine Absicht der Gewinnerzielung ist damit nicht verbunden.

Der Steuerberater fragte nun, ob für die Überlassung des Systems der Abschluss eines Vertrages im Sinne von Art. 28 DS-GVO erforderlich ist. Die Erforderlichkeit des Abschlusses eines derartigen Vertrages habe ich verneint.

Wann eine Auftragsverarbeitung im Sinn der DS-GVO vorliegt, definiert die DS-GVO selbst nicht. Zwar schreibt die DS-GVO vor, welche datenschutzrechtlichen Anforderungen sie an eine Auftragsverarbeitung stellt. Wann diese vorliegt, ergibt sich jedoch weder aus Art. 28 DS-GVO noch aus der Definition des Auftragsverarbeiters in Art. 4 Nr. 8 DS-GVO. Zwar definiert Art. 4 Nr. 8 DS-GVO den Auftragsverarbeiter, nicht aber die Auftragsverarbeitung. Eine solche liegt allerdings nur dann vor, wenn die personenbezogenen Daten

im Auftrag und auf Weisung des Auftraggebers durch den Auftragnehmer verarbeitet werden. Eine derartige Situation liegt hier nicht vor.

Mandant und Steuerberater können gleichermaßen und zu eigenen Zwecken auf die in den Speicher geladenen Daten zugreifen. Zweck des Systems ist nicht die Verarbeitung der Daten nach Weisung des Mandanten, sondern vielmehr die sichere Übermittlung der Daten an den Steuerberater. Sie ist daher eine Nebenleistung des Steuerberatungsvertrages. Die Steuerberatung selbst ist nach § 11 StBerG keine Auftragsverarbeitung. Gemäß § 11 Abs. 2 S. 1 StBerG erfolgt die Verarbeitung personenbezogener Daten, soweit diese für die Erbringung der Leistungen des Steuerberaters erforderlich ist, weisungsfrei. Daher liegt für die Verarbeitung von Daten im Rahmen der Steuerberatung kein Auftragsverhältnis im Sinn des Datenschutzrechts vor.

Die Übermittlung der Daten auf einem sicheren Weg ist für die Erbringung der Leistungen des Steuerberaters erforderlich und unterfällt daher § 11 Abs. 2 S. 1 StBerG. Selbst wenn dies nicht der Fall wäre, läge eine Auftragsverarbeitung im Sinn des Datenschutzrechts nicht vor, da das System ohnehin ausschließlich zur Übermittlung von Daten und nicht zur Verarbeitung der Daten nach Weisung vorgesehen ist.

14.2
Erhebung von Kundendaten durch Kreditinstitute

Kreditinstitute sind dazu berechtigt, Daten zur Tätigkeit (Berufsgruppe, Branche) ihrer Kundinnen und Kunden oder zur Herkunft von Vermögenswerten zu erheben, um die Anforderungen aus dem Geldwäschegesetz (GWG) erfüllen zu können.

Ein häufiges Thema von Beschwerden im Bereich der Kreditwirtschaft ist die Aufforderung der Kreditinstitute an ihre Kundinnen und Kunden, bestimmte Daten zu übermitteln. Neben den üblichen Daten, wie Name, Vorname, Geburtsdatum und Anschrift, wird auch nach Daten zur Tätigkeit, insbesondere zur Berufsgruppe (oder dem Beruf selbst), sowie zur Branche, in welcher die Tätigkeit erbracht wird, gefragt. In anderen Fällen fordern die Kreditinstitute Nachweise zur Herkunft von Vermögenswerten. In solchen Fällen wird in den bei mir eingereichten Beschwerden häufig nach der Rechtmäßigkeit sowie nach dem zulässigen Umfang der Datenerhebung gefragt.

Grundsätzlich gilt, dass die Erhebung personenbezogener Daten u. a. dann zulässig ist, wenn eine Rechtsnorm die verantwortliche Stelle hierzu verpflichtet (Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO).

Art. 6 DS-GVO

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: (…)

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; (…)

Eine solche rechtliche Verpflichtung enthält das GWG. Es verpflichtet Kreditinstitute, risikobasiert bestimmte Daten zu erheben. Dies ergibt sich aus den Regelungen zu den Allgemeinen Sorgfaltspflichten nach § 10 ff. GWG.

§ 10 GWG

(1) Die allgemeinen Sorgfaltspflichten sind:

1. *die Identifizierung des Vertragspartners und gegebenenfalls der für ihn auftretenden Person nach Maßgabe des § 11 Absatz 4 und des § 12 Absatz 1 und 2 sowie die Prüfung, ob die für den Vertragspartner auftretende Person hierzu berechtigt ist,*
2. *die Abklärung, ob der Vertragspartner für einen wirtschaftlich Berechtigten handelt, und, soweit dies der Fall ist, die Identifizierung des wirtschaftlich Berechtigten nach Maßgabe des § 11 Absatz 5 und des § 12 Absatz 3 und 4; dies umfasst in Fällen, in denen der Vertragspartner keine natürliche Person ist, die Pflicht, die Eigentums- und Kontrollstruktur des Vertragspartners mit angemessenen Mitteln in Erfahrung zu bringen,*
3. *die Einholung und Bewertung von Informationen über den Zweck und über die angestrebte Art der Geschäftsbeziehung, soweit sich diese Informationen im Einzelfall nicht bereits zweifelsfrei aus der Geschäftsbeziehung ergeben,*
4. *die Feststellung mit angemessenen, risikoorientierten Verfahren, ob es sich bei dem Vertragspartner oder dem wirtschaftlich Berechtigten um eine politisch exponierte Person, um ein Familienmitglied oder um eine bekanntermaßen nahestehende Person handelt, und*
5. *die kontinuierliche Überwachung der Geschäftsbeziehung einschließlich der Transaktionen, die in ihrem Verlauf durchgeführt werden, zur Sicherstellung, dass diese Transaktionen übereinstimmen*

a) mit den beim Verpflichteten vorhandenen Dokumenten und Informationen über den Vertragspartner und gegebenenfalls über den wirtschaftlich Berechtigten, über deren Geschäftstätigkeit und Kundenprofil und,

b) soweit erforderlich, mit den beim Verpflichteten vorhandenen Informationen über die Herkunft der Vermögenswerte;

im Rahmen der kontinuierlichen Überwachung haben die Verpflichteten sicherzustellen, dass die jeweiligen Dokumente, Daten oder Informationen unter Berücksichtigung des jeweiligen Risikos im angemessenen zeitlichen Abstand aktualisiert werden.

Zum Umfang der Sorgfaltspflichten fordert § 14 Abs. 2 Satz 2 GWG:

Die Verpflichteten müssen in jedem Fall die Überprüfung von Transaktionen und die Überwachung von Geschäftsbeziehungen in einem Umfang sicherstellen, der es ihnen ermöglicht, ungewöhnliche oder verdächtige Transaktionen zu erkennen und zu melden.

Welche Informationen unter welchen Bedingungen die Kreditinstitute erheben müssen, hat die für das GWG zuständige Aufsichtsbehörde, die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), auf der Grundlage von § 51 Abs. 8 GWG mit ihren Auslegungs- und Anwendungshinweisen vom 8. Juni 2021 festgelegt (https://www.bafin.de/SharedDocs/Downloads/DE/Auslegungsentscheidung/dl_ae_auas_gw.pdf;jsessionid=288F6442B71FBAA666EA309F8F0A6863.2_cid503?__blob=publicationFile&v=17).

Danach ergibt sich für Fragen zur Berufstätigkeit aus der Verpflichtung nach § 10 Abs. 1 Nr. 5 Buchst. a GWG folgende Prüfungsberechtigung: Um ungewöhnliche oder verdächtige Transaktion, z. B. Geldeingänge, identifizieren zu können, muss das Kreditinstitut u. a. einen Abgleich zwischen der Höhe der Geldeingänge und den Angaben zur Tätigkeit (Berufsgruppe) und Branche durchführen. Wenn z. B. ein Kunde eine Helfertätigkeit im Handwerk angibt, monatlich aber Geldeingänge zu verzeichnen sind, die in der Höhe deutlich von den üblichen Eingängen passend zur Tätigkeit abweichen, kann das ein Hinweis auf eine geldwäscherelevante Transaktion sein, die möglicherweise von dem Kreditinstitut dann auch zu melden wäre.

Für Fragen nach der Herkunft von Vermögenswerten ist zu beachten, dass § 10 Abs. 1 Nr. 5 Buchst. b GWG festlegt, dass das verpflichtete Kreditinstitut im Rahmen der kontinuierlichen Überwachung der Geschäftsbeziehung die Transaktionen der Kunden mit Informationen über die Herkunft von Vermögenswerten abgleichen muss. Nach den Auslegungs- und Anwendungshinweisen vom 8. Juni 2021 müssen bei Bartransaktionen die Einzahlenden einen Herkunftsnachweis des einzuzahlenden Bargelds erbringen. Als Herkunftsnachweise dienen hierbei z. B. Kontoauszüge von anderen Banken, von denen das Bargeld abgehoben wurde, Barauszahlungsquittungen, Verkaufs- und Rechnungsbelege und ähnliche Unterlagen. Die in diesem Zusammenhang vorgelegten Herkunftsnachweise sind von dem Kreditinstitut dann nach § 8 GWG aufzuzeichnen und aufzubewahren.

Zusammenfassend ist festzuhalten, dass die Erhebung von Kundendaten nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO in Verbindung mit §§ 10 Abs. 1 Nr. 5 und 14 Abs. 2 Satz 2 GWG datenschutzrechtlich zulässig ist, sofern mit diesen Daten die vom Gesetzgeber auferlegten Prüfpflichten durch das jeweilige Kreditinstitut sichergestellt werden.

14.3
Unterrichtung über Datenempfänger durch Auskunfteien

Die Dritterhebung von personenbezogenen Daten z. B. durch Auskunfteien setzt gemäß Art. 14 DS-GVO eine aktive Information des Verantwortlichen gegenüber der betroffenen Person voraus. Hierbei sind nach Buchstabe e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten zu nennen. Auf die Nennung der konkreten Empfänger darf nur dann verzichtet werden, wenn der Empfänger zum Zeitpunkt der Erhebung noch nicht feststeht.

Mich erreichte eine Beschwerde, in der bemängelt wurde, dass eine Auskunftei nicht ausreichend über die Empfänger der zur jeweiligen Person übermittelten Daten informieren würde.

Bei Auskunfteien handelt es sich um private gewerbliche Unternehmen. Sie erheben Informationen u. a. über die Identität, die Kreditwürdigkeit, die Zahlungswilligkeit und -fähigkeit von Unternehmen und Privatpersonen. Diese Informationen werden gespeichert und an Dritte übermittelt, wenn sie ein berechtigtes Interesse im Sinn des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO an einer solchen Information haben. Auskunfteien können auch als sogenannte Dritterheber für ihre Kunden im Rahmen der Adressrecherche, z. B. im Fall von nicht zustellbaren Schreiben, tätig werden. Hierbei wird die Auskunftei von einem Gläubiger (der ein berechtigtes Interesse glaubhaft machen kann) beauftragt, die aktuelle Adresse des Rechnungsadressaten ausfindig zu machen. Die Auskunftei ermittelt dann die Adresse bei Dritten (etwa bei Einwohnermeldeämtern) und ist aufgrund der Verarbeitung durch sie anschließend verpflichtet, den Betroffenen gem. Art. 14 DS-GVO über die Verarbeitung seiner personenbezogenen Daten zu informieren.

Hintergrund sind hierbei die Transparenzregelungen in den Art. 12 ff. DS-GVO. Die Grundsätze einer fairen und transparenten Verarbeitung erfordern es, die betroffene Person über die Existenz des Verarbeitungsvorgangs und seiner Zwecke zu unterrichten. Werden die Daten an Dritte übermittelt, ist es gem. Art. 14 Abs. 1 Buchst. e DS-GVO erforderlich, der betroffenen Person die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten mitzuteilen.

Im vorliegenden Fall wurde die Auskunftei als sogenannter Dritterheber tätig. Nach Überprüfung der erteilten Auskunft bestätigte sich der Beschwerdeinhalt. In dem Informationsschreiben nach Art. 14 DS-GVO wurde lediglich die „angefragte Anschrift“ sowie die „erhobene Anschrift“ beauskunftet. Mögliche Auskunftsempfänger wurden in einem beigefügten Beiblatt in abstrakter

Weise beschrieben. Die Auskunftei teilte den Betroffenen erst im Rahmen einer weiteren Anfrage den tatsächlichen Empfänger der Daten mit.

Nach Art. 14 Abs. 1 Buchst. e DS-GVO müssen im Falle der Dritterhebung dem Betroffenen die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten mitgeteilt werden. Ob die konkreten Empfänger oder nur die Kategorien von Empfängern mitzuteilen sind, hängt von den jeweiligen Verhältnissen, insbesondere dem Stadium der Datenverarbeitung ab. Steht der Empfänger zum Zeitpunkt der Mitteilung gem. Art. 14 DS-GVO noch nicht fest, kann dieser auch nicht benannt werden. In diesem Fall sind lediglich die Kategorien von Empfängern mitzuteilen. Wenn zum Zeitpunkt der Erhebung der Empfänger der Daten bereits bekannt ist, ist dieser jedoch konkret zu benennen. Da die Auskunftei von einem konkreten Gläubiger beauftragt wird, die Adresse des Betroffenen ausfindig zu machen, ist folglich der Empfänger der Daten als Auftraggeber im Vorfeld bekannt. Mithin ist dieser Empfänger der Daten nach Art. 14 Abs. 1 Buchst. e DS-GVO konkret zu benennen. In der Folge wurde die Auskunftei angewiesen, den Auskunftsinhalt nach Art. 14 DS-GVO anzupassen und somit künftig in allen entsprechenden Fällen den Auskunftsempfänger zu nennen.

14.4
GO-Kart & Gastkonten

Der Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 24. März 2022 hinsichtlich der Verpflichtung, Gastkonten im Onlinehandel einzurichten, ist unter Umständen auch auf Sachverhalte in der analogen Welt anzuwenden. Zur Wahrung des Prinzips der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DS-GVO müssen demnach zwingend bei der einmaligen Nutzung einer Freizeitanlage Gastkontenmodelle angeboten werden. Eine Speicherung von Daten auf Vorrat, für etwaige künftige Nutzungen der Freizeitanlage, ist unzulässig.

Mich erreichte eine Beschwerde, die sich gegen eine Kartbahn in Hessen richtete. Für Kunden existiert am Eingang der Kartbahn ein digitales System zur Nutzerdatenerfassung, das der Benutzer vor Nutzung der Kartbahn selbst über Touchscreen zu bedienen hat. Hierbei wurden umfangreiche personenbezogene Daten abgefragt, ohne deren Eingabe eine Nutzung der Kartbahn nicht möglich war. Insbesondere mussten Besucher Name, Adresse, Telefon und genaues Geburtsdatum angegeben und ein Gesichtsfoto (explizite Aufforderung ohne Gesichtsmaske) zulassen. Durch die Eingaben der Daten erwarb man eine sogenannte „Rennlizenz“, die ein Jahr gültig war. Bei jener „Rennlizenz“ handelte es sich um ein Nutzerkonto.

Auf der Startseite forderte der Betreiber zudem die Bestätigung der Haftungsbedingungen ein. Außer der rudimentären Information, dass die Daten vom Betreiber verarbeitet werden, waren die gem. Art. 13 DS-GVO erforderlichen Angaben nicht enthalten. Eine umfassende Datenschutzbestimmung war weder verlinkt noch waren weitere Angaben zur weitergehenden Nutzung, z. B. durch ein Versicherungsunternehmen, den externen Datenschutzbeauftragten o. Ä., vorhanden. Angaben zur Dauer der Speicherung und eine Möglichkeit zur Verweigerung einer zu erteilenden Einwilligung fehlten ebenfalls.

Ich forderte den Betreiber der Kartbahn nach Anhörung umgehend auf, das Verfahren umzustellen. Im Vordergrund standen hierbei vor allem die Reduzierung der Pflichtangaben, das obligatorische Anfertigen von Gesichtsfotos sowie die fehlenden Informationen. Er sagte die zeitnahe Durchführung der notwendigen Änderungen zu.

Zur Überprüfung der Änderungen fand sodann ein Vor-Ort-Termin durch Mitarbeiter meiner Behörde in der Kartsporthalle statt. Hierbei zeigte sich, dass der Betreiber nach der Verfahrensanpassung zwar die Möglichkeit geschaffen hatte, die datenschutzrechtliche Einwilligung zur Verarbeitung personenbezogener Daten per Kontrollkästchen zu erteilen, ohne Erteilung der Einwilligung konnte der Registrierungsprozess jedoch nicht abgeschlossen werden. Die Erteilung der Einwilligung war daher nach wie vor obligatorisch.

Die Erfassung und Verarbeitung der personenbezogenen Daten im Rahmen der „Rennlizenz“ wurde vom Betreiber u. a. mit dem Eintritt eines etwaigen Haftungsfalles begründet. Daher speicherte er jene Daten ein Jahr lang. Die Kunden mussten sich bei wiederholter Nutzung der Kartbahn nicht mehr registrieren. Das Modell ähnelte somit dem Modell fortlaufender Kundenkonten bei dauerhaften Geschäftsbeziehungen im Online-Handel.

Die Erfassung der zuvor genannten personenbezogenen Daten stellt einen Verstoß gegen den Grundsatz der Datenminimierung gem. Art. 5 Abs.1 Buchst. c DS-GVO dar. Zudem liegt ein Verstoß gegen Art. 7 Abs. 4 DS-GVO vor. Hiernach kann die Freiwilligkeit der Einwilligung in die Verarbeitung personenbezogener Daten nicht vorliegen, wenn die Erbringung der Dienstleistung von der Einwilligung abhängig gemacht wird, diese aber für die Erfüllung des Vertrags nicht erforderlich ist. Der Anwendungsbereich des Art. 7 Abs. 4 DS-GVO ist vor allem im Zusammenhang mit Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO zu sehen, nach dem zur Vertragserfüllung erforderliche Datenverarbeitungen ohne Einwilligung zulässig sind. Die Breite des Anwendungsbereichs für nicht von Art. 7 Abs. 4 DS-GVO erfasste Einwilligungserklärungen ist somit gering, denn gerade zur Vertragserfüllung erforderliche Datenverarbeitungen bedürfen keiner Einwilligung, weshalb es auch für diese an der Erforderlichkeit mangelt (Ingold, in: Sydow/Marsch,

DS-GVO/BDSG, DS-GVO Art. 7 Rn. 30-33). Die vom Betreiber erfassten Daten waren allerdings nicht zur Vertragserfüllung im Sinn des Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO erforderlich und eine Beurteilung im Sinn des Art. 7 Abs. 4 DS-GVO führte zu einer fehlenden Freiwilligkeit der Erteilung einer Einwilligung.

Das Fahren auf der Kartbahn war wiederum nur möglich, wenn die betroffene Person der Verarbeitung personenbezogener Daten zugestimmt hatte. Folglich lag eine Koppelungssituation vor. In Anlehnung an die Leitlinien des EDSA 05/2020 vom 4. Mai 2020 kommt es hierbei gerade nicht auf eine Über- und Unterordnungssituation oder gar Monopolstellung des Verantwortlichen an. Demnach kann eine Einwilligung als nicht freiwillig angesehen werden, auch wenn ein Verantwortlicher argumentiert, dass zwischen seiner Dienstleistung, zu der die Einwilligung in die Nutzung personenbezogener Daten für zusätzliche Zwecke gehört, und einer vergleichbaren Dienstleistung, die von einem anderen Verantwortlichen angeboten wird, eine Wahlmöglichkeit bestehe (zum Meinungsstreit, ob eine Monopolstellung vorliegen muss, s. Stemmer, in: BeckOK DatenschutzR, DS-GVO Art. 7 Rn. 46; Schulz, in: Gola/Heckmann, DSGVO/BDSG, 3. Aufl. 2022, DS-GVO Art. 7 Rn. 19-34).

Im vorliegenden Fall ist zudem noch der Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24. März 2022 zu beachten (DSK, Datenschutzkonformer Online-Handel mittels Gastzugang, https://www.datenschutzkonferenz-online.de/media/dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf). Danach müssen Verantwortliche, die Waren oder Dienstleistungen im Onlinehandel anbieten, ihren Kundinnen und Kunden unabhängig davon, ob sie ihnen daneben einen registrierten Nutzungszugang (fortlaufendes Kundenkonto) zur Verfügung stellen, grundsätzlich einen Gastzugang für die Bestellung bereitstellen. Bei der Kartbahn handelt es sich zwar um keinen Onlineversandhändler. Trotzdem sind die Grundsätze des DSK-Beschlusses anzuwenden. Bei einer einmaligen Nutzung der Kartbahn kann der Verantwortliche nicht per se behaupten, dass er Daten von Kundinnen und Kunden für mögliche weitere, aber ungewisse zukünftige Fahrten auf Vorrat halten darf.

Die Nutzung muss demnach auch ohne Angabe personenbezogener Daten möglich sein. Mithin habe ich den Betreiber angewiesen, die Möglichkeit eines Gastzugangs einzurichten. Dies hat er auch umgesetzt. Zudem hat er die Datenschutzerklärung überarbeitet und eine DS-GVO konforme Einwilligungsmöglichkeit geschaffen.

14.5
360°-Panoramaaufnahmen bei Straßenbefahrungen

Als Rechtsgrundlage für die Erhebung personenbezogener Daten zur Erstellung von 360°-Panoramaaufnahmen, in denen personenbezogene Daten wie Hausfassaden, Kfz-Kennzeichen und Erscheinungsbilder von Personen enthalten sein können, kommt Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in Betracht. Sofern keine Veröffentlichung der Bilder erfolgt sowie nicht erforderliche personenbezogene Daten unkenntlich gemacht werden, besteht seitens der betroffenen Personen kein bedingungsloses Widerspruchsrecht. Die Möglichkeit der betroffenen Personen, Widerspruch gem. Art. 21 Abs. 1 DS-GVO z. B. gegen die Abbildung der Hausfassaden einzulegen, bleibt dagegen unberührt. Dieses Recht ist jedoch zu erläutern und kann vom Verantwortlichen auch verweigert werden, sofern keine ausreichend nachvollziehbaren Gründe vom Antragsteller vorgetragen wurden, die für die Entfernung oder Unkenntlichmachung der Daten sprechen.

Mich erreichen immer häufiger Anfragen von Bürgerinnen und Bürgern, die in ihren Kommunen Straßenbefahrungen von Fahrzeugen bemerken, die mit Kameras ausgestattet sind. Das in diesen Fällen aktive Unternehmen hat seinen Sitz in Hessen, weshalb ich mich mit der damit verbundenen Datenverarbeitung im Berichtszeitraum befasst habe.

Aufnahmen von 360°-Panoramabilder

Das Unternehmen erhebt mit speziell ausgestatteten Fahrzeugen 360°-Panoramabilder vom öffentlichen Raum sowie Laserpunktwolken mittels eines LiDAR-Scanners durch Straßenbefahrungen. So wird ein stadtweites Geoinformationssystem, erweitert durch 360°-Panoramabilder, geschaffen und als „digitaler Zwilling“ über Lizenzverträge den Kommunen sowie weiteren Akteuren und Zielgruppen (hauptsächlich in der Daseinsvorsorge, z. B. Netzbetreiber, Telekommunikationsanbieter) zur Verfügung gestellt. Diese erwerben entsprechende Zugänge und nutzen diese, um ihre Aufgaben effektiver und effizienter direkt vom Büro aus erfüllen zu können, so dass Ortstermine verringert oder sogar ganz entfallen können. Anwendungsbereiche finden sich beispielsweise im Rahmen der Stadtgestaltung, z. B. um die Bausubstanz von Immobilien zu bewerten oder die Durchgrünung und den Zustand von Bäumen und Grünflächen zu dokumentieren. Auch im Bereich der Einsatzplanung, z. B. bei Veranstaltungen oder Feuerwehreinsätzen, werden die Daten herangezogen. Ebenso ist es möglich, im „digitalen Zwilling“ Szenarien wie beispielsweise Starkregenereignisse zu visualisieren, um die dargestellten Auswirkungen in die Katastrophenschutzplanung einzubezie-

hen. Die Daten sind nicht öffentlich, sondern nur durch den genannten und limitierten Anwenderkreis abrufbar.

Neben den Geoinformationen, wie Adressen oder entsprechenden Geokoordinaten, werden bei der Straßenbefahrung weitere personenbezogene Daten wie Abbildungen der Hausfassaden sowie Personen und Fahrzeuge im öffentlichen Raum erfasst, wofür eine Rechtsgrundlage bestehen muss.

Eine rechtmäßige Verarbeitung personenbezogener Daten liegt immer dann vor, wenn eine der Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 Buchst. a bis f DS-GVO erfüllt ist. Insofern gilt im Datenschutzrecht das „Erlaubnisprinzip", denn eine Datenverarbeitung ist immer dann zulässig, wenn ein Erlaubnistatbestand gegeben ist (Roßnagel, NJW 2019, Heft 1-2, S. 5).

Mit Beschluss vom 20. Mai 2020 bestätigte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder auch nach Geltung der DS-GVO ihre Rechtsauffassung, wonach im Rahmen von StreetView und ähnlichen Diensten Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO als Rechtsgrundlage für die Verarbeitung von Straßenansichten, einschließlich teilweiser Abbildungen von Häuserfassaden und privaten Grundstücksbereichen, welche an den öffentlichen Straßenraum angrenzen, in Betracht kommen kann (DSK, Beschluss zu Vorabwidersprüchen bei StreetView und vergleichbaren Diensten, 2020, https://www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_vorabwidersprueche_bei_streetview_und_vergleichbaren_diensten.pdf). Merkmale wie Gesichter und Kfz-Kennzeichen sind dabei jedoch unkenntlich zu machen. Im Rahmen der Interessenabwägung ist bei einer Veröffentlichung der Daten zudem ein Verlangen betroffener Personen auf Unkenntlichmachung ihrer Daten zu berücksichtigen, zu denen auch Abbildungen von Häuserfassaden und private Grundstücksbereiche zu zählen sind.

Interessenabwägung

Sofern danach private Unternehmen Panoramaaufnahmen des öffentlichen Raums anfertigen, kann als Rechtsgrundlage Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO herangezogen werden. Danach ist eine Verarbeitung personenbezogener Daten zulässig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

Das Vorliegen der Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO wird dabei anhand eines dreistufigen Prüfverfahrens geprüft. Zuerst wird das berechtigte Interesse des Verantwortlichen oder eines Dritten ermittelt. Im

Anschluss erfolgt eine Kontrolle, ob die beabsichtigte Datenverarbeitung zur Wahrung des berechtigten Interesses auch erforderlich ist. Zum Schluss wird die eigentliche Abwägung zwischen den festgestellten berechtigten Interessen des Verantwortlichen und des Dritten mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall vorgenommen (DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieterinnen und Anbieter von Telemedien ab dem 1. Dezember 2021, S. 30-31, https://www.datenschutzkonferenz-online.de/orientierungshilfen.html).

Das berechtigte Interesse der Unternehmen, die gem. Art. 4 Nr. 7 DS-GVO als Verantwortliche anzusehen sind, ist ein wirtschaftliches Interesse. Denn die personenbezogenen Daten werden zum Zwecke der Erstellung und gewerblichen Vermarktung sog. „digitaler Zwillinge“ erhoben. In diesem Zusammenhang ist zu berücksichtigen, dass das berechtigte Interesse weit ausgelegt wird (Simitis/ Hornung/ Spiecker gen. Döhmann-Schantz, Datenschutzrecht, DS-GVO Art. 6 Abs. 1 Rn. 98) und das Bestehen wirtschaftlicher Interessen bereits durch den EuGH anerkannt wurde (EuGH, Urteil vom 13. Mai 2014 - C-131/12, Rn. 81).

Der zweite Prüfungsschritt, der zur Erforderlichkeit der Datenverarbeitung, wird im Erwägungsgrund 39 DS-GVO dahingehend erläutert, dass die personenbezogenen Daten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das notwendige Maß beschränkt sein müssen. So sind die Daten nur zu verarbeiten, wenn die Zwecke, die damit verfolgt werden, nicht in zumutbarer Weise durch andere, mildere Mittel erreicht werden können. Im Unterschied zum berechtigten Interesse ist die Erforderlichkeit eng auszulegen (Kühling/Buchner-Buchner/Petri, 3. Aufl. 2020, DS-GVO Art. 6 Rn. 147a).

Die Aufnahme von Häuserfassaden wird explizit bezweckt, um der Kommune als Kundin einen Mehrwert für deren Verwaltungstätigkeit über den digitalen Zwilling anbieten zu können. Exemplarisch wird damit geworben, Verwaltungsvorgänge wie die Erteilung und Durchsetzung verschiedener Genehmigungen oder stadtgestalterische Maßnahmen effizienter und effektiver zu ermöglichen. Ohne die Aufnahme der Häuserfassaden wäre eine solche Nutzung nicht möglich. Ein anderes Mittel ist demnach nicht ersichtlich.

Dagegen sind sowohl die Kfz-Kennzeichen als auch die aufgenommenen Personen keinesfalls erforderlich. Allerdings ist es bei Straßenbefahrungen unvermeidlich, diese personenbezogenen Daten zu erheben. Ein milderes Mittel scheint auch hier nicht zur Verfügung zu stehen. Es gilt jedoch, die Datenverarbeitung in diesen Fällen auf das „absolut Notwendige“ zu begrenzen (EuGH, Urteil vom 4. Mai 2017 - C-13/16, Rn. 30). Daten, die demnach nicht erforderlich sind, sind entsprechend unkenntlich zu machen. Die DSK

hat daher zutreffend bestimmt, dass dies zumindest für die Gesichter und Kfz-Kennzeichen bei der Erstellung von Panoramaaufnahmen erfolgen sollte (DSK-Beschluss von 2020, s. oben). In der Praxis werden diese Daten daher in der Regel noch während der Befahrung durch KI-Technik automatisch verpixelt.

Diese Unkenntlichmachung ist schließlich auch in der dritten Stufe der Interessenabwägung zu berücksichtigen und stellt eine anerkannte Methode dar, um „die häufig widerstreitenden Interessen (…) in einen angemessenen Ausgleich zu bringen“ (OVG Lüneburg, Beschluss vom 19. Januar 2021 – 11 LA 16/20, Rn. 25). Dabei ist eine Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO bereits dann zulässig, wenn die Interessen des Verantwortlichen zu denen der betroffenen Person gleichwertig sind. Nur ein überwiegendes Interesse des Betroffenen führt zu einem entsprechenden Ausschluss.

Bei der Abwägung sind jedoch viele Faktoren einzubeziehen, z. B. der Zweck, das Risiko der Datenverarbeitung und dessen Eingriffsintensität, die Datenkategorie und deren „öffentliche Zugänglichkeit“, die technischen- und organisatorischen Maßnahmen sowie die vernünftigen Erwartungen im Hinblick auf die Datenverarbeitung (Erwägungsgrund 47 DS-GVO) und die Möglichkeit, eine entsprechende Verarbeitung vernünftigerweise absehen zu können (Taeger/Gabel-Taeger, 4. Aufl. 2022, DS-GVO, Art. 6 Rn. 148f.).

Das berechtigte Interesse der betroffenen Person besteht im Schutz ihres informationellen Selbstbestimmungsrechts und ihrer Privatsphäre. Die Unternehmen wiederum können sich auf ihre Wirtschaftsgrundrechte berufen (Art. 12, Art. 14, Art. 19 Abs. 3 GG).

Im konkreten Fall werden Personen, Kfz-Kennzeichen und Hausfassaden in Verbindung mit Geokoordinaten aufgenommen, die sich in der Öffentlichkeit oder in Bereichen befinden, die im öffentlichen Raum, z. B. durch einen Aufenthalt in der entsprechenden räumlichen Umgebung, wahrgenommen werden können. Insofern betrifft es z. B. die Hausfassaden, die zur Straße ausgerichtet sind, und Fahrzeuge, die vor dem Gebäude parken, oder Personen, die sich auf Gehwegen oder in Vorgärten aufhalten. Daten wie das Kfz-Kennzeichen oder die Hausfassade sind demnach öffentlich zugänglich oder einsehbar.

Dennoch sind insbesondere die Hausfassaden und die den Bewohnern des Gebäudes zuzuordnenden Fahrzeuge grundsätzlich dazu geeignet, Aufschluss über die persönlichen Lebensverhältnisse zu geben. So kann etwa das äußere Erscheinungsbild des Hauses und des Gartens in Verbindung mit der Anzahl und dem Zustand der den Bewohnern zuzuordnenden Fahrzeugen Hinweise auf deren finanzieller und familiärer Verhältnisse geben. Ein Blick

in den Vorgarten beispielsweise genügt häufig, um Informationen darüber zu erlangen, ob Kinder in dem Haus leben und in welcher Altersspanne sie sich befinden. Denn typischerweise lassen sich dort Indizien wie Spielzeuge, Schaukeln, Rutschen oder Tret- und Rutschfahrzeuge ausmachen. Ebenso ist es möglich, aufgrund der Lage und der Bausubstanz des Gebäudes Rückschlüsse über dessen wirtschaftlichen Wert zu ziehen.

Allerdings zeigt sich dennoch, dass die in der Öffentlichkeit befindlichen Daten einen geringeren Schutzbedarf aufweisen. So hat auch das Bundesverfassungsgericht bereits 1983 festgestellt, dass solche Daten „ein Abbild sozialer Realität" darstellen und das Recht auf informationelle Selbstbestimmung des Einzelnen in diesen Zusammenhang eingeschränkt werden kann (Urteil vom 15. Dezember 1983 – 1 BvR 209/83, Rn. 156).

Doch gibt es zweifelsohne einen Unterschied zwischen der Möglichkeit, sich über Panoramaaufnahmen oder einen daraus entwickelten digitalen Zwilling in aller Ruhe und unerkannt einen Überblick über das Umfeld zu verschaffen, und der Betrachtung vor Ort.

Berücksichtigung des Adressatenkreises

Innerhalb der Interessenabwägung ist daher eine genauere Betrachtung des Adressatenkreises, dem die Daten zur Verfügung stehen, und deren Zwecke notwendig.

Im Gegensatz zu Google Street View oder Apple Look Around werden die Bilder nicht jedermann offengelegt, sondern über Lizenzen einem bestimmten Personenkreis, insbesondere Behörden, zur Verfügung gestellt, die die Daten wiederum selbst nur für eigene, legitime Zwecke nutzen dürfen. Über entsprechend verpflichtende Datenschutzinformationen ist es somit möglich und erforderlich, der betroffenen Person transparent bewusst zu machen, wer die Daten verarbeitet und wofür. Dies ist bei einer Veröffentlichung weniger klar erkennbar.

Überdies ist weiterhin zu beachten, dass die aufgenommenen personenbezogenen Daten keine hohe Schutzwürdigkeit aufweisen, da sie insbesondere öffentlich sichtbar sind. Ferner muss der Empfänger der Daten – also im Falle der Bereitstellung eines digitalen Zwillings die Kommune selbst – eine Rechtsgrundlage besitzen, die eine Übermittlung der Daten an sie und eine entsprechende Weiterverarbeitung gestattet.

Diese kann in der Regel aus der Aufgabenerfüllung gem. Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO in Verbindung mit § 3 HDSIG und/oder den jeweilig einschlägigen Regelungen der bereichsspezifischen Gesetze bestehen.

Entfällt eine Veröffentlichung und werden die Daten nur für einen begrenzten und bestimmbaren Personenkreis z. B. innerhalb der Kommune für legitime Zwecke verwendet, ist somit innerhalb der Interessenabwägung davon auszugehen, dass die berechtigten Interessen der Betroffenen nicht überwiegen und eine entsprechende Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO rechtlich zulässig ist. Voraussetzung ist natürlich, dass zumindest die Gesichter der aufgenommenen Personen und Kfz-Kennzeichen unkenntlich gemacht werden.

Des Weiteren besteht nach wie vor die Möglichkeit seitens der betroffenen Personen, Widerspruch gem. Art. 21 Abs. 1 DS-GVO z. B. gegen die Abbildung der Hausfassaden einzulegen. Die Gründe zur Wahrnehmung dieses Rechts sind jedoch zu erläutern und die Umsetzung kann vom Verantwortlichen auch verweigert werden, sofern keine ausreichend nachvollziehbaren Aspekte vom Antragsteller vorgetragen wurden, die für die Entfernung oder Unkenntlichmachung der Daten sprechen.

Verbesserung der Transparenz

Im konkreten Fall hat sich herausgestellt, dass Ursache für einige bei mir eingegangen Beschwerden häufig fehlende Transparenz ist. So ist der Befahrungskalender sowie die dazugehörige Datenschutzinformation zwar auf der Website des hessischen Unternehmens sowie auf der Website des Geodatenkodex veröffentlicht, jedoch erreichen diese Informationen die betroffenen Personen häufig nicht, so dass Irritationen und Unsicherheiten entstehen, wenn das Fahrzeug auf der Straße gesichtet wird.

Das in Hessen ansässige Unternehmen sicherte daher zu, dass zukünftig neben der Veröffentlichung der Befahrungstermine auf der eigenen Website sowie ggf. dem Anregen einer Berichterstattung in lokalen Zeitungen zusätzlich gut sichtbare QR-Codes auf den Fahrzeugen angebracht werden, über die Betroffene, welche das Fahrzeug sehen, direkt über den Link des QR-Codes an die entsprechend hinterlegte Datenschutzinformation gelangen. Die Umsetzung soll im folgenden Jahr erfolgen.

15. Gesundheitsbereich

Die Verarbeitung von Gesundheitsdaten ist von doppelter Brisanz: Einerseits geht es darum, Daten zu verarbeiten, um für die Gesundheit von Menschen vorzusorgen, sie zu erhalten oder wiederherzustellen. Andererseits geht es bei Gesundheitsdaten um eine besondere Kategorie von personenbezogenen Daten, für die die informationelle Selbstbestimmung mit besonderer Sorgfalt zu wahren ist. Die Corona-Pandemie, die in den beiden letzten Berichtsjahren eine besondere Aufmerksamkeit der Datenschutzaufsicht gefordert hat, stand in diesem Berichtszeitraum nicht mehr derart im Vordergrund, wenn auch weiterhin ein korrigierendes Eingreifen erforderlich war (s. Kap. 15.2, 15.3 und 15.5). Vielmehr gab es Anlass und Gelegenheit, sich durch Begleitung von Gesetzgebungsverfahren auch um die Bedingungen des Gesundheitsdatenschutzes zu kümmern (s. Kap. 15.1). Schließlich war die Aufgabe der Datenschutzaufsicht, die Einhaltung der Pflichten der Verantwortlichen zu prüfen (s. Kap. 15.4) und die Rechte der betroffenen Person zu wahren, gefragt – am Beispiel der Auskunft (s. Kap. 15.6) und der Berichtigung (s. Kap. 15.7).

15.1
Begleitung von Gesetzesvorhaben im Gesundheitsbereich

Im Berichtszeitraum bildete die Beratung bei Gesetzesvorhaben einen Schwerpunkt meiner Tätigkeit. Um hier einen Einblick zu gewähren, möchte ich im Folgenden von den wesentlichen Ergebnissen meiner Beratungspraxis im Kontext der Novellierung des Hessischen Krebsregistergesetzes (HKRG), des Hessischen Krankenhausgesetzes (HKHG) und des Hessischen Gesetzes über Hilfen bei psychischen Krankheiten (PsychKHG) berichten. In all diesen Bereichen konnte ich auf eine datenschutzfreundliche Ausgestaltung der geplanten Regelungen hinwirken.

Novellierung des HKRG

Im Kontext der Novellierung des Hessischen Krebsregistergesetzes wurde seitens des Hessischen Ministeriums für Soziales und Integration (HMSI) und der forschenden Stellen klar der Wunsch kommuniziert, dass die Möglichkeit der Datenübermittlung an externe Forschende ausgeweitet und Forschungsergebnisse als auch Datensätze für Forschungszwecke besser nutzbar gemacht werden sollen. Ich habe diesen Wunsch unterstützt und dabei ein besonderes Augenmerk auf die Klarheit und Bestimmtheit der geplanten Normen gelegt (s. §§ 9a und 9b HKRG-E).

Die neue Rechtsgrundlage für die Übermittlung anonymisierter und pseudonymisierter Daten enthält Mechanismen und Garantien zur Wahrung der Interessen der betroffenen Personen. Die von der Norm erfassten Vorhaben der Versorgungsforschung müssen sich soweit wie möglich auf die Nutzung anonymisierter Daten beschränken. Die Forschenden müssen zwingend ein aussagekräftiges Datenschutzkonzept bereitstellen. Neben der strengen Zweckbindung soll die Übermittlung der Daten an Dritte und die Identifizierung von betroffenen Personen gesetzlich verboten werden. Auch eine Beteiligung des wissenschaftlichen Beirats ist vorgesehen.

Zudem war es der besondere Wunsch, sich an bereits bestehenden Krebsregistern anderer Länder zu orientieren und es in einem gewissen Umfang zu ermöglichen, trotz eines eingelegten Widerspruchs der betroffenen Personen nach Löschung der Identitätsdaten mit den klinischen und epidemiologischen Daten weiterzuarbeiten (s. § 7a HKRG-E). Da es in Hessen ohnehin die Möglichkeit gibt, das Widerspruchsrecht der betroffenen Personen im Interesse der Forschungszwecke zu beschränken (s. § 24 Abs. 2 S. 1 HDSIG), habe ich auf einen vertretbaren Ausgleich der Interessen hingewirkt. Dementsprechend wurde der verbleibende Datensatz möglichst gering gehalten sowie weitere Korrektive im Sinn des Datenschutzes erreicht. So werden die von einem Widerspruch erfassten Daten nach sieben Jahren vollständig gelöscht. Eine Übermittlung an externe Forschende ist ausgeschlossen. Außerdem soll nach sieben Jahren evaluiert werden, ob diese Einschränkung des Widerspruchsrechts weiterhin für das Krebsregister notwendig ist.

Unterstützt habe ich schließlich auch den Vorstoß, die unterbliebene Meldung durch den meldepflichtigen Arzt zu sanktionieren. Entsprechende Tatbestände für Ordnungswidrigkeiten gibt es bereits in anderen Bundesländern (z. B. Rheinland-Pfalz, Baden-Württemberg, Nordrhein-Westfalen, Schleswig-Holstein), so dass auch Hessen hier durch die Neuregelung nachgezogen ist.

Von einer Verlängerung der bereits sehr langen Aufbewahrungsdauer der Identitätsdaten (zehn Jahre nach dem Tod oder spätestens 130 Jahre nach der Geburt der betroffenen Person, vgl. § 14 HKRG) wurde aufgrund meiner Bedenken Abstand genommen.

Novellierung des PsychKHG

Auch bei der Novellierung des PsychKHG wurde ich seitens des HMSI eingebunden. Der § 14 Abs. 1 S. 2 PsychKHG-E sollte insoweit einen umfassenden Katalog an Daten enthalten, die von den psychiatrischen Krankenhäusern an die Fachaufsicht (HSMI) übermittelt werden. Nach der Gesetzesbegründung handelte es sich nicht um personenbezogenen Daten:

> „Da keine personenbezogenen Daten übermittelt werden, ist die Anonymisierung gewährleistet und Rückschlüsse auf einzelne untergebrachte Personen [sind] nicht möglich."

Diese Perspektive teilte ich nicht. Bereits das Datum des Unterbringungsbeginns und das Entlassungsdatum sollten taggenau erfasst werden und waren damit in der Kombination schon für sich genommen im Regelfall nur einer Person zuzuordnen. Folglich waren sie eindeutig personenbeziehbar. Dies wurde korrigiert und in der Folge geregelt, die Daten nur noch in vergröberter Form zu erfassen (Quartal der Aufnahme und Quartal der Entlassung).

Die nach § 14 Abs. 1 S. 2 Nr. 1 bis 14 PsychKHG-E an das HMSI zu übermittelnden Daten sollten zudem eine große Anzahl an sensiblen Daten gemäß Art. 9 DS-GVO beinhalten (Diagnosen, Behandlungsmaßnahmen, Sicherungsmaßnahmen). Wichtig war es mir daher zudem, dass in § 14 PsychKHG klar geregelt wird, zu welchen Zwecken diese Daten vom HMSI verarbeitet werden und dass eine strikte Zweckbindung der erfassten Daten im Gesetz Erwähnung findet.

Novellierung des HKHG

Auch im Hinblick auf die Novellierung des Hessischen Krankenhausgesetzes konnte eine Neuregelung in § 12 Abs. 5 HKHG erwirkt werden. Danach sind nunmehr die hessischen Krankenhäuser, die dem HKHG unterliegen, dazu verpflichtet, Konzepte für die sichere Aktenverwahrung im Falle ihrer Insolvenz zu erstellen und bereitzuhalten. Näheres hierzu findet sich auch auf meiner Homepage (s. https://datenschutz.hessen.de/datenschutz/gesundheitswesen/schutz-der-patientendaten-bei-schliessung-von-krankenhaeusern).

Ausblick auf die kommenden Gesetzesvorhaben auf Bundesebene

Zu erwähnen ist schließlich auch, dass ich über die neu gegründete Taskforce Forschungsdaten (s. Kap. 16.1) ebenso in die geplanten Neuregelungen auf Bundesebene eingebunden bin. Der Vorsitz der Taskforce Forschungsdaten, bestehend aus BfDI und mir, hat insoweit den Entstehungsprozess des Forschungsdatengesetzes und des Registergesetzes verfolgt und wird auch die weitere Umsetzung begleiten.

15.2
Erlass zur einrichtungsbezogenen Impfpflicht

Zur Einführung der einrichtungsbezogenen Impfpflicht nach § 20a IfSG im März 2022 hat das HMSI einen Erlass zum Vollzug des § 20a IfSG in Hessen veröffentlicht. Im Vorfeld habe ich hierzu das HMSI beraten und mich erfolgreich für datensparsamere Regelungen im Erlass eingesetzt. So konnte sichergestellt werden, dass nur die zur Erfüllung der gesetzlichen Pflichten aus § 20a IfSG erforderlichen personenbezogenen Daten von den Arbeitgebern erhoben und ggfs. an die zuständigen Gesundheitsämter übermittelt werden.

Hintergrund

Am 12. Dezember 2021 trat bundesweit das Gesetz zur Stärkung der Impfprävention gegen COVID-19 und zur Änderung weiterer Vorschriften im Zusammenhang mit der COVID-19-Pandemie (BGBl. I S. 5162) in Kraft. Mit diesem Gesetz wurde u. a. die einrichtungs- und unternehmensbezogene Pflicht zum Nachweis einer Impfung, Genesung oder Kontraindikation in § 20a IfSG eingeführt.

Wie die neue einrichtungsbezogene Impfpflicht durch die Gesundheitsämter in Hessen umzusetzen ist, bedurfte näherer Bestimmungen. Auch aus datenschutzrechtlicher Sicht stellten sich hier einige Fragen, die nicht eindeutig durch den Bundesgesetzgeber vorgegeben wurden. Das federführende HMSI bat mich daher frühzeitig um Beratung in dieser Angelegenheit.

Datenschutzrechtliche Bewertung

Nach § 20a Abs. 2 S. 1 und Abs. 3 S. 1 IfSG hatten Beschäftigte der vom Gesetz erfassten Einrichtungen und Unternehmen der Leitung dieser Unternehmen und Einrichtungen einen entsprechenden Nachweis (Impfnachweis, Genesenennachweis, ärztliches Attest) vorzulegen. Erfolgte dies nicht bis zum 15. März 2022 oder bestanden Zweifel der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises, war das zuständige Gesundheitsamt zu benachrichtigen und es waren personenbezogene Angaben diesem zu übermitteln (§ 20a Abs. 2 S. 2 und Abs. 3 S. 2 IfSG). Die Nachweise selbst durften aber nach dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DS-GVO) nicht von den Arbeitgebern kopiert oder gespeichert werden. Die Arbeitgeber durften nach Kontrolle der Nachweise nur speichern, dass ein gültiger Nachweis vorgelegt wurde und ggfs. das Ablaufdatum des Nachweises, da diese Informationen zur Erfüllung der gesetzlichen Pflichten aus § 20a IfSG ausreichend waren.

In einem amtlichen Muster für eine ärztliche Bescheinigung über eine Kontraindikation als Nachweis gegenüber dem Arbeitgeber durfte aus Gründen der Datenminimierung und mangels Erforderlichkeit die konkrete Diagnose nicht genannt werden. Es reichte vielmehr aus, wenn in einer solchen ärztlichen Bescheinigung festgestellt wurde, dass eine medizinische Kontraindikation gegen eine COVID-19-Impfung vorlag.

Die Übermittlung von Nachweisen an das Gesundheitsamt war nicht gesetzlich vorgesehen und damit unzulässig. Es durften nach dem Grundsatz der Datenminimierung nur der Meldegrund und die personenbezogenen Angaben nach § 2 Nr. 16 IfSG (Name, Anschrift, Kontaktdaten) an das zuständige Gesundheitsamt übermittelt werden.

§ 20a IfSG trat zum 1. Januar 2023 außer Kraft. Somit entfiel die entsprechende Verpflichtung der Einrichtungen und Unternehmen und damit die datenschutzrechtliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Auf der Grundlage von § 20a IfSG erhobene Daten der Beschäftigten waren spätestens zum 31. Dezember 2022 zu löschen oder zu vernichten.

Die DSK hat im Beschluss vom 13. April 2022 „Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht“ diese datenschutzrechtlichen Bewertungen zu § 20a IfSG bestätigt.

Ergebnis

Im Rahmen der Beratung des HMSI konnte ich erreichen, dass die oben genannten datenschutzrechtlichen Anforderungen bei der Umsetzung der einrichtungsbezogenen Impfpflicht in Hessen vollständig berücksichtigt wurden. Auch bei Einrichtung des digitalen Meldeportals zur einrichtungsbezogenen Impfpflicht wurde ich beratend eingebunden und konnte auf datenschutzkonforme Prozesse hinwirken.

15.3
Datenschutz in Testzentren

Im Gesundheitsbereich stellte die Beratung und Überprüfung von COVID-Testzentren einen Schwerpunkt dar. Die von mir festgestellten datenschutzrechtlichen Versäumnisse der Testzentren wurden durch Sensibilisierungen der Beschäftigten, Anpassungen der technischen Prozesse und Überarbeitungen der Dokumente abgestellt. In einigen Fällen habe ich Bußgeldverfahren eingeleitet.

Hintergrund

Im Berichtszeitraum waren COVID-Testzentren häufig Gegenstand von Beschwerden. Auch baten zahlreiche Testzentren um eine Beratung zur datenschutzkonformen Gestaltung ihrer Prozesse. Da es sich bei den COVID-Testergebnissen um nach Art. 4 Nr. 15 und Art. 9 Abs. 1 DS-GVO besonders zu schützende Gesundheitsdaten handelt, unterliegen die Betreiber von Testzentren hohen datenschutzrechtlichen Anforderungen (s. auch Kap. 5.2).

Leider wurden diese gesetzlichen Anforderungen nicht immer erfüllt, so dass mein Einschreiten erforderlich wurde. Hierbei habe ich festgestellt, dass sich die angetroffenen Datenschutzverstöße ähneln und regelmäßig unter einem der folgenden Themen zusammengefasst werden können.

Erhebung nicht erforderlicher Daten

Bei der Online-Registrierung oder der Anmeldung vor Ort dürfen grundsätzlich nur solche personenbezogenen Daten von den zu testenden Personen abgefragt und erhoben werden, die zur Durchführung des COVID-Tests und zur Erfüllung der damit verbundenen rechtlichen Pflichten erforderlich sind.

Manche Testzentren haben im Aufsichtsverfahren vorgetragen, dass Personalausweise kopiert würden, um Angaben zu verifizieren oder um die Pflichten aus der Coronavirus-Testverordnung („TestV“) zu erfüllen.

Die Coronavirus-Testverordnung verlangt aber weder die Anfertigung einer Kopie des Personalausweises noch die Dokumentation der Personalausweisnummer. Nach §6 Abs. 3 Nr. 4 TestV hat die zu testende Person bei einem Bürgertest gegenüber dem Anbieter ihre Identität durch Vorlage eines amtlichen Lichtbildausweises nachzuweisen. Eine Sichtkontrolle mit Datenabgleich ist hierbei ausreichend.

Personalausweiskopien dürfen daher grundsätzlich nicht von den Betreibern der Testzentren erzeugt werden. Im Einzelfall kann aber die Erhebung der Personalausweisnummer zulässig sein, wenn dies erforderlich ist, z. B. bei der Nutzung der Personalausweisnummer für internationale Testzertifikate und wenn die betroffene Person darin eingewilligt hat.

Unzureichende Datenschutzerklärungen

Das Testzentrum hat den zu testenden Personen bei Erhebung ihrer Daten die in Art. 13 DS-GVO genannten Informationen mitzuteilen. Sie müssen insbesondere über den Namen und die Kontaktdaten des Verantwortlichen, die Zwecke und Rechtsgrundlagen der Datenverarbeitungen, die Empfänger von Daten und die Betroffenenrechte informieren. An dieser Stelle sollten

sie auch darstellen, dass sie im Rahmen der Testungen nach Art. 9 Abs. 1 DS-GVO besonders geschützte Gesundheitsdaten verarbeiten.

Die Informationen nach Art. 13 DS-GVO („Datenschutzerklärung“) müssen die Testzentren den zu testenden Bürgerinnen und Bürgern im Testzentrum vor Ort zur Verfügung stellen, insbesondere für die Personen, die sich nicht online anmelden und daher nicht schon bei der Online-Registrierung die Datenschutzerklärung zur Kenntnis nehmen können. Kopien der Datenschutzerklärung müssen vorrätig sein, damit ein Exemplar auf Nachfrage der betroffenen Person mitgegeben werden kann.

Der von einigen Testzentren vorgenommene Verweis auf die allgemeinen Website-Datenschutzerklärungen kann die gesetzlichen Anforderungen aus Art. 13 DS-GVO nicht erfüllen. Denn dabei fehlt es an konkreten Informationen zu den Datenverarbeitungen im Zusammenhang mit der Testdurchführung.

Hier konnte ich Nachbesserungen der Informationstexte erreichen und für mehr Transparenz gegenüber den betroffenen Personen sorgen.

In einem Fall blieb der Betreiber des Testzentrums mangels ordnungsgemäßer Datenschutzerklärung unbekannt und konnte nur durch Unterstützung des Gesundheitsamts ermittelt werden. Durch diesen eklatanten Verstoß gegen Art. 13 Abs. 1 Buchst. a DS-GVO konnten die betroffenen Personen nicht wissen, wer für die Verarbeitung ihrer Daten verantwortlich ist und gegenüber wem sie ihre Rechte ausüben können. Auch in diesem Fall habe ich auf die Erfüllung der Informationspflichten hingewirkt. Darüber hinaus prüfe ich weitere aufsichtsrechtliche Maßnahmen gegenüber dem Verantwortlichen.

Mangelhafte Diskretion und fehlender Zugriffsschutz

Die Betreiber von Testzentren sind nach Art. 5 Abs. 1 Buchst. f und Art. 32 DS-GVO dazu verpflichtet, die personenbezogenen Daten der betroffenen Personen vor unberechtigten Zugriffen und Kenntnisnahmen Dritter zu schützen. Daher sind die Räumlichkeiten der Testzentren so zu gestalten, dass die Kundinnen und Kunden keine Sicht auf die Bildschirme des Testzentrums haben. Die Testergebnisse sind nur der getesteten Person bekanntzugeben, so dass sich das Ausrufen des Testergebnisses vor den wartenden Personen selbstverständlich verbietet. Auch die Dokumentation der Testergebnisse und die Testzertifikate müssen sicher aufbewahrt werden. Entsprechende Papierdokumente sind insbesondere auch außerhalb der Öffnungszeiten des Testzentrums sicher und verschlossen zu verwahren.

Diese grundsätzlichen Regeln zur Diskretion und zum Zugriffsschutz im Testzentrum wurden von einigen Testzentren leider nicht beachtet. In einem Fall wurden die Testzertifikate in einem unverschlossenen Karton in öffentlich

zugänglichen Räumen eines Bürgerhauses aufbewahrt. In einem anderen Fall wurden Teile der schriftlichen Testdokumentation mit personenbezogenen Daten als „Schmierzettel“ verwendet und gegenüber Dritten offenbart (s. Kap. 5.2). Hier waren aufsichtsrechtliche Maßnahmen gegen beide Testzentrumsbetreiber erforderlich.

In einem weiteren Testzentrum hing der interne Leitfaden für die Benutzeroberfläche zur Testverwaltung offen aus. Der Benutzername und das Passwort für den Zugang zu dieser Weboberfläche waren somit für Dritte einsehbar. Dadurch konnten sich unbefugte Dritte anmelden und die personenbezogenen Daten der getesteten Personen abrufen. Aufgrund des generischen Benutzernamens („Testzentrum1“) und des schwachen, leicht zu erratenen Passworts (Straßenname + 2022) ließen sich auch leicht die Zugangsdaten für andere Testzentren des gleichen Anbieters ermitteln. Gegen den Anbieter der Testzentren habe ich ein Bußgeldverfahren eingeleitet.

Sicherheit bei der elektronischen Übermittlung des Testergebnisses

Auch wenn das Testzertifikat den getesteten Personen elektronisch zur Verfügung gestellt wird, müssen die Testzentren die personenbezogenen Daten nach Art. 5 Abs. 1 Buchst. f, Art. 24 Abs. 1 und Art. 32 Abs. 1 DS-GVO durch effektive Authentifizierungsmechanismen ausreichend vor dem Zugriff unberechtigter Dritter schützen. Die Übermittlung der Testergebnisse per E-Mail setzt dabei regelmäßig eine wirksame Inhaltsverschlüsselung voraus. Die Anforderung an eine solche Verschlüsselung habe ich bereits in meinem letzten Tätigkeitsbericht beleuchtet (s. 50. Tätigkeitsbericht, Kap. 17.2., S. 184 ff.). Auch die DSK hat sich in ihrer Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ (https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf) umfassend mit den Anforderungen an eine solche Übermittlung per E-Mail beschäftigt.

In der Praxis kann die notwendige Verschlüsselung von Testzentrumsbetreibern z. B. durch Nutzung eines verschlüsselten Anhangs erfolgen. Als gängiges Verschlüsselungsverfahren empfiehlt sich dabei etwa der Advanced Encryption Standard (AES) mit einer ausreichenden Schlüssellänge (256 Bit oder länger). Verantwortliche können sich bei der Auswahl anderer in Frage kommender Verfahren beispielsweise an der technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102-1) des BSI (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf) orientieren. Eine solche Verschlüsselung kann unter Nutzung allgemein gut verfügbarer

Software, die mitunter auch standardmäßig Teil aktueller Betriebssysteme ist, auf gängige Dateiformate wie etwa ZIP-Dateien angewendet werden.

Das Passwort muss ausreichend komplex sein und darf insbesondere für Dritte nicht leicht zu erraten sein. Daher sollte es sich nicht aus offenkundigen Eigenschaften der Person ableiten lassen. Das Geburtsdatum eignet sich daher nicht als Passwort. Durch einen Bruteforce-Angriff wäre dieses darüber hinaus sehr leicht zu erraten, da die Anzahl der möglichen Kombinationen sehr gering ist. Das BSI hält niederschwellige Informationen zur Auswahl geeigneter Passwörter auf seinem Web-Auftritt bereit (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html). Weitergehende Anforderungen an Passwörter mit Blick auf den breiteren Kontext der IT-Sicherheit finden sich u. a. im Baustein ORP.4 (Identitäts- und Berechtigungsmanagement) des IT-Grundschutz-Kompendiums des BSI (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2021.pdf?__blob=publicationFile&v=2).

Ein solches Passwort darf stets nur auf gesondertem, sicherem Weg an die betroffene Person übermittelt werden. Erfolgt bereits die Übermittlung des inhaltsverschlüsselten Testergebnisses via E-Mail, so kommt E-Mail als Mittel für die Passwortübermittlung daher nicht mehr infrage. Da Art. 32 Abs. 1 DS-GVO von den Verantwortlichen fordert, die Risiken der Verarbeitung personenbezogener Daten zu betrachten, müssten sie hier von dem möglichen Risiko des unbefugten Zugriffs auf das empfangende E-Mail-Postfach ausgehen und daher annehmen, dass ein einziger unbefugter Zugriff gleichzeitig die zu schützenden Daten als auch das schutzgewährende Passwort offenlegen würde. Für die Passwortübermittlung muss daher auf ein alternatives Medium, etwa Telefon oder SMS, ausgewichen werden.

In der Aufsichtspraxis zeigte sich anhand einiger Beschwerden, dass diese Anforderungen bei der Übermittlung der Testergebnisse nicht durchgängig von den Testanbietern beachtet wurden. Daher musste ich hier im Aufsichtsverfahren in vielen Fällen für einen besseren Schutz der Testzertifikate, z. B. durch Nutzung eines zweiten Authentifizierungsfaktors, sorgen. Eine solche Mehr-Faktor-Authentifizierung kann vor allem auch dann erforderlich werden, wenn die verantwortliche Stelle für den Abruf der Testergebnisse einen Online-Dienst nutzt. Bei der Bewertung der Angemessenheit eines solchen Dienstes legt meine Behörde u. a. die Maßgaben der Orientierungshilfe „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“

der DSK (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_anbieter_onlinedienste.pdf) zugrunde.

Häufig konnten die notwendigen Änderungen nur durch die als Auftragsverarbeiter tätigen technischen Dienstleister der Testzentren erfolgen. Dabei hat sich gezeigt, dass ein aufsichtsbehördliches Vorgehen gegen die Anbieter der technischen Lösungen zur elektronischen Bereitstellung der Testzertifikate deutlich effektiver ist als das Vorgehen gegen einzelne verantwortliche Teststellenbetreiber.

In einem Fall musste ich es außerdem unterbinden, dass das Testergebnis schon im Betreff der jeweiligen E-Mail genannt wurde.

Fehlversand von Testergebnissen

Bei dem täglichen tausendfachen Versand von COVID-Testergebnissen ist es nicht ungewöhnlich, dass aufgrund eines Versehens oder eines Tippfehlers ein Testergebnis an die falsche Person gesendet wird. Soweit die technischen Schutzmaßnahmen wie die Verschlüsselung des Testergebnisses (s. oben) eingehalten wurden, hat die fälschlicherweise adressierte Person bei einem Fehlversand per E-Mail dennoch regelmäßig keinen Zugriff auf das Testergebnis. Hier zeigt sich, welche hohe Bedeutung die Wahl angemessener technischer Schutzmaßnahmen hat. Wichtig ist außerdem, dass die Betreiber von Testzentren ihre Pflichten zur Meldung einer Datenpanne nach Art. 33 DS-GVO kennen und entsprechende Prozesse implementiert haben, um bei solchen Vorfällen gesetzeskonform reagieren zu können.

Fazit

Das Geschäftsmodell der COVID-Testzentren besteht nun schon über zwei Jahre, so dass sich hier inzwischen datenschutzkonforme Prozesse etabliert haben müssten. Beim Thema Datenschutz besteht bei den Betreibern jedoch immer noch ein gewisser Nachholbedarf. Die Betreiber von Testzentren in Hessen sollten sich bewusst sein, dass die Feststellung einer schwerwiegenden Datenschutzverletzung zu einem nicht unerheblichen Bußgeld führen kann. Bei einigen Vorgängen habe ich bereits die Eröffnung eines Bußgeldverfahrens veranlasst. In diesem Tätigkeitsbericht werden in Kap. 5.2 mehrere Bußgeldverfahren gegen Testzentrumsbetreiber näher dargestellt.

Auf der Website meiner Behörde habe ich weitere Informationen zum Datenschutz in Testzentren veröffentlicht (https://datenschutz.hessen.de/datenschutz/gesundheitswesen/datenschutz-bei-sars-cov-2-schnelltests). Diese Veröffentlichung soll den Betreibern der Testzentren bei der Erfüllung ihrer datenschutzrechtlichen Pflichten helfen und konnte schon einige Unklarheiten

beseitigen. Sie kann auch jenseits der COVID-Pandemie den Betreibern von Testzentren für andere testrelevante Erkrankungen Hilfestellungen bieten, um ihre datenschutzrechtlichen Pflichten zu erkennen und zu erfüllen.

15.4
Upload medizinischer Bilder in die Cloud zum Abruf durch den Patienten

Der Upload medizinischer Bilder in die Cloud eines Auftragsverarbeiters einer radiologischen Praxis bedarf keiner Einwilligung durch die Patientin oder den Patienten. Die Erstellung der Bilder und die Verarbeitung dieser für eine unkomplizierte Übermittlung an den behandelnden Arzt ist zur Erfüllung der vertraglichen Pflicht der radiologischen Praxis im Sinn des Art. 9 Abs. 2 Buchst. h DS-GVO erforderlich.

Beschwerde gegen den Upload von Bildern

Im Rahmen einer Beschwerde hatte ich die Frage zu beurteilen, ob es sich bei dem Upload von medizinischen Bildern durch eine radiologische Praxis in die Cloud eines Auftragsverarbeiters für den Abruf durch den Patienten oder den behandelnden Arzt um einen zusätzlichen Service ohne geeignete Rechtsgrundlage für die Patientinnen und Patienten handelt und mithin eine Einwilligung erforderlich wäre.

Die beschwerdeführende Person war aufgrund einer Überweisung zur Erstellung medizinischer Bilder in Behandlung in einer radiologischen Praxis. Vor der Behandlung hat sie ausdrücklich erklärt, dass ihre Gesundheitsdaten nicht an Dritte weitergegeben werden dürfen. Sie wollte vor einer eventuell notwendigen Weitergabe informiert und um Einwilligung gebeten werden. Nach ihrer Behandlung wurde ihr zusammen mit einer CD, auf der ihre Untersuchungsbilder gespeichert waren, ein Informationsblatt mit Informationen zur Zugriffsmöglichkeit zur Verfügung gestellt. Damit konnte sie ihre Untersuchungsbilder zusätzlich online abrufen. Hierfür wurden ihre Untersuchungsbilder an einen auftragsverarbeitenden Dienstleister übermittelt. Sollte dies nicht gewünscht sein, bat die Praxis um Rückmeldung. Der Zugriff werde dann deaktiviert und die Bilder damit gelöscht.

Die beschwerdeführende Person bat daraufhin um sofortige Löschung des Online-Zugriffs und ihrer Untersuchungsbilder vom Server des externen Dienstleisters. Diesem Wunsch ist die Praxis umgehend nachgekommen. Da die beschwerdeführende Person der Auffassung war, nicht ausreichend über die Weitergabe der Daten an den externen Dienstleister informiert worden zu

sein und dass eine Übermittlung ohne ihre Einwilligung nicht hätte stattfinden dürfen, wandte sie sich mit einer Beschwerde an mich.

Die Praxis argumentierte, dass das Zurverfügungstellen der Bilder über die Online-Funktionalität des externen Anbieters zu ihrer vertraglichen Pflicht gehöre und dem Aushändigen der Bilder auf einer CD gleiche. Das Erstellen und Zurverfügungstellen der Bilder auf diese Weise gehöre zu ihrem Auftrag, da die Patientinnen und Patienten die Bilder für ihre Behandlung bei einem anderen Arzt benötigten. Zudem wies die Praxis darauf hin, dass immer weniger Patientinnen und Patienten sowie Arztpraxen CDs überhaupt auslesen könnten, da sie kaum noch über CD-ROM-Laufwerke verfügten.

Rechtliche Bewertung

Der Argumentation der Praxis bin ich gefolgt und habe eine Verarbeitung aufgrund von Art. 9 Abs. 2 Buchst. h DS-GVO angenommen.

Die Erhebung, Speicherung und Nutzung von Gesundheitsdaten durch einen behandelnden Arzt ist im Rahmen des Behandlungsvertrages und dem zur Behandlung erforderlichen Umfang nach Art. 9 Abs. 2 Buchst. h letzte Alternative DS-GVO ohne Einwilligungserklärung der Patientin oder des Patienten von Gesetzes wegen zulässig. Danach dürfen insbesondere Name, Kontaktdaten und Versicherungsnummer des Patienten, die Anamnese- und Behandlungsdokumentation, Arztbriefe und Laborberichte auch ohne Einwilligung verarbeitet werden.

Sofern eine Arztpraxis zusätzliche Dienste wie z. B. einen Newsletter oder Recall-Service anbieten will, ist die diesbezügliche Verarbeitung von Patientendaten aufgrund des nicht durch den Behandlungsvertrag gedeckten Zwecks nur mit Einwilligung der Patientin oder des Patienten im Sinn des Art. 9 Abs. 2 Buchst. a DS-GVO zulässig.

In diesem Fall war zu berücksichtigen, dass eine radiologische Praxis im Wesentlichen eine befunderhebende Stelle ist, die weitgehend auf Überweisung von anderen Fachärzten tätig wird. Es handelt sich mithin hauptsächlich um eine mitbehandelnde Einrichtung. Die medizinischen Bilder werden zum Zweck der Weitergabe an die behandelnden Ärzte erstellt. Die Erstellung der Bilder und die Verarbeitung dieser für eine unkomplizierte Übermittlung an den behandelnden Arzt ist somit zur Erfüllung der vertraglichen Pflicht der radiologischen Praxis im Sinn des Art. 9 Abs. 2 Buchst. h DS-GVO erforderlich. Es handelt sich gerade nicht lediglich um einen zusätzlichen Service.

Insoweit war auch die Übermittlung an einen Auftragsverarbeiter nicht zu beanstanden. Der Auftragsverarbeiter ist nicht „Dritter“ im Sinn der DS-GVO (s. Art. 4 Nr. 10 DS-GVO: „außer […] dem Auftragsverarbeiter“). Es

besteht vielmehr zwischen dem den Auftrag erteilenden Verantwortlichen und seinem Auftragsverarbeiter ein „Innenverhältnis“. Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet. Für die Weitergabe von personenbezogenen Daten an den Auftragsverarbeiter und die Verarbeitung durch den Auftragsverarbeiter bedarf es regelmäßig keiner weiteren Rechtsgrundlage im Sinn von Art. 6 bis 10 DS-GVO als derjenigen, auf die der Verantwortliche selbst die Verarbeitung stützt (Datenschutzkonferenz, Kurzpapier Nr. 13, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-08/kurzpapier_nr.13_auftrag.pdf).

Die Möglichkeit der Inanspruchnahme von IT-Dienstleistern durch Berufsgeheimnisträger wurde bewusst durch den Gesetzgeber in § 203 Abs. 3 S. 2 StGB erweitert. In der Gesetzesbegründung wird die Speicherung von Daten in der Cloud ausdrücklich erwähnt (BT-Drs. 18/11936, S. 18):

> „Für sämtliche in § 203 Absatz 1 StGB genannten Personen kann zudem die Speicherung von Daten auf externen informationstechnischen Anlagen (wie z. B. in einer „Cloud“) wirtschaftlich sinnvoll sein. Diese wirtschaftlichen Interessen von Berufsgeheimnisträgern sind grundsätzlich berechtigt, Voraussetzung ist allerdings, dass sie in Einklang gebracht werden können mit den berechtigten Interessen der Inhaber der Geheimnisse an deren rechtlichen Schutz.“

Eine solche Inanspruchnahme externer Dienstleister ist daher nicht per se zu beanstanden, sofern andere datenschutzrechtliche Gründe ihr nicht entgegenstehen, was in dem von mir bearbeiteten Vorgang auch nicht der Fall war. Zu berücksichtigen dabei ist, dass für solche Verarbeitungstätigkeiten schon aufgrund der besonderen Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO ein hohes Schutzniveau erforderlich ist. Für den eingesetzten Online-Dienst sollten die Maßgaben der Orientierungshilfe „Anforderungen an Anbieter von Online-Diensten zur Zugangssicherung“ der DSK (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_anbieter_onlinedienste.pdf) berücksichtigt werden.

Wird dies berücksichtigt, so greift der Verweis der radiologischen Praxis auf den Stand der Technik, der vielerorts bereits den Abschied von physischen Speichermedien wie der CD-ROM und der dazu passenden Auslesetechnik bedeutet hat. Auch aus technischer Sicht macht der Datenschutz ein Festhalten an veralteten Technologien nicht erforderlich, wenn mittels zeitgemäßer Übermittlungswege und Kommunikationsmedien bereits ein vergleichbarer Schutz für die personenbezogenen Daten der betroffenen Personen erreicht werden kann.

15.5
Postalischer Versand der COVID-Impfzertifikate

Mich erreichten einige Beschwerden über die postalisch versandten digitalen Impfzertifikate. Diese Impfzertifikate wurden zusammen mit einem vom Hessischen Ministerium des Innern und für Sport (HMdIS) und dem Hessischen Ministerium für Soziales und Integration (HMSI) gezeichneten Anschreiben versandt. Zur Klarstellung und Förderung der Transparenz habe ich im Dialog mit den beteiligten Ministerien eine Anpassung des Prozesses erreicht.

Nach einer Impfung in hessischen Impfzentren erhielten die Bürgerinnen und Bürger ihr persönliches digitales Impfzertifikat (QR-Code) zusammen mit einem vom HMdIS und vom HMSI gezeichneten Anschreiben. Hierdurch entstand bei einigen Personen der Eindruck, dass die Impfdaten der Bürgerinnen und Bürger in den Ministerien gespeichert würden.

Nach der Stellungnahme des HMdIS wurden die Impfdaten der Bürgerinnen und Bürger nicht von den Ministerien verarbeitet, sondern zur Erstellung und zum Versand der digitalen Impfzertifikate von den Impfzentren an den kommunalen Dienstleister ekom21 übermittelt. Das Anschreiben von HMdIS und HMSI wurde dem jeweiligen Impfzertifikat vor Versand durch die ekom21 lediglich beigelegt, da die Erstellung und der Versand der digitalen Impfnachweise zentral für alle hessischen Impfzentren organisiert wurde.

In dem gemeinsamen Anschreiben von HMdIS und HMSI zu den Impfzertifikaten sind diese als Absender erkennbar. Das Anschreiben enthielt leider keine entsprechende Klarstellung, dass die Erstellung und der Versand der Impfzertifikate im Auftrag der zuständigen Gesundheitsämter als Träger der Impfzentren durch die ekom21 als Dienstleister erfolgte und das Anschreiben der Ministerien nur beigelegt wurde. Daher waren die Bedenken der Bürgerinnen und Bürger hinsichtlich ihrer sensiblen Impfdaten grundsätzlich nachvollziehbar.

Gerade beim Umgang mit den hier betroffenen äußerst schutzbedürftigen Gesundheitsdaten ist besondere Sensibilität erforderlich. Auch im Interesse des Vertrauens der Bürgerinnen und Bürger in die Impfkampagne sollten solche Missverständnisse durch transparente Darstellung von Datenverarbeitungen im Vorfeld verhindert werden.

Falls die Einbindung eines externen Dienstleisters für die Erstellung und den Versand der Impfzertifikate nicht erforderlich ist, sollte dies kritisch überdacht werden. Mit der Übermittlung von sensiblen Gesundheitsdaten an andere Stellen können potenziell neue Risiken verbunden sein.

Auf meine Anregung hin wurden die Prozesse überarbeitet, um für mehr Transparenz gegenüber den Bürgerinnen und Bürgern zu sorgen und Missverständnisse zu verhindern. Nach Anpassung des Verfahrens wurden die digitalen Impfzertifikate direkt von den zuständigen Gesundheitsämtern als Träger der Impfzentren versandt und in deren Namen gezeichnet. Auf die Einbindung der ekom21 wurde verzichtet.

15.6
Elektronische Auskunftserteilung im Gesundheitsbereich

Auch im Gesundheitsbereich muss eine elektronische Auskunft nach Art. 15 Abs. 1 und 3 DS-GVO möglich sein, wenn die betroffene Person dies wünscht. Dafür stehen den Arztpraxen mehrere Wege zur Verfügung.

Anspruch auf elektronische Auskunft?

Ich bekomme immer mehr Eingaben und Anfragen zu dem Thema, dass Arztpraxen die Auskunft nach Art. 15 DS-GVO nur schriftlich erteilen, obwohl die betroffenen Personen den Antrag per E-Mail gestellt und um die Auskunftserteilung „in einem gängigen elektronischen Format“ gebeten haben. Oft wird die Auskunftserteilung dann unter Bezug auf den Datenschutz abgelehnt. Den Patientinnen und Patienten wird angeboten, die Unterlagen entweder abzuholen oder auf dem Postweg zu erhalten.

Gemäß Art. 15 Abs. 3 S. 3 DS-GVO sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, wenn die betroffene Person den Antrag elektronisch stellt und sofern sie nichts Anderes angibt. Auch die Unterrichtung über eine mögliche Verzögerung bei der Auskunftserteilung hat gemäß Art. 12 Abs. 3 S. 4 DS-GVO nach Möglichkeit beim Vorliegen dieser Voraussetzungen auf elektronischem Weg zu erfolgen. Diese Vorgaben und die Möglichkeiten einer sicheren elektronischen Übermittlung an die Patientinnen und Patienten ist den Arztpraxen häufig nicht bekannt.

Anforderungen an eine elektronische Auskunft

Bei der elektronischen Auskunftserteilung ist zunächst zu beachten, dass die Identität der betroffenen Person zweifelsfrei feststehen muss. Ist dies nicht der Fall, kann der Verantwortliche gemäß Art. 12 Abs. 6 DS-GVO zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind. In den mir bekannten Fällen stand die Identität der Antragstellerinnen und Antragsteller fest, weil diese zusätzlich zum elektronischen Antrag unter anderem persönlich in den Arztpraxen vorstellig

wurden, um die elektronische Auskunft zu erbitten, oder auch postalisch mit den Arztpraxen kommuniziert haben.

Insbesondere problematisch bei der Auskunftserteilung im medizinischen Bereich ist, dass nach Art. 9 Abs. 1 DS-GVO besonders schützenswerte Gesundheitsdaten und Daten, die gemäß § 203 StGB der Schweigepflicht unterliegen, übermittelt werden müssen. Arztpraxen haben gemäß Art. 5 Abs. 1 Buchst. f DS-GVO in Verbindung mit Art. 32 DS-GVO hinsichtlich des erforderlichen Schutzniveaus angemessene und geeignete technische und organisatorische Maßnahmen zu treffen, um die Sicherheit der Übermittlung zu gewährleisten. Dies ist auch der Grund dafür, weshalb die elektronische Auskunftserteilung von Arztpraxen oft kategorisch abgelehnt wird.

Dies ist insoweit nachvollziehbar, als bei der Versendung von E-Mails mit Gesundheitsdaten eine Transportverschlüsselung allein, d. h. die häufig von den E-Mail-Anbietern automatisch vorgenommene Verschlüsselung für den Übertragungsweg zwischen den Servern des Senders und des Empfängers, grundsätzlich nicht ausreichend ist. Vielmehr bedarf es hier – um ein angemessenes Schutzniveau zu gewährleisten – bei Berücksichtigung des Standes der Technik zusätzlich zur Transportverschlüsselung auch einer Inhaltsverschlüsselung („Ende-zu-Ende-Verschlüsselung“).

Wie eine Inhaltsverschlüsselung von E-Mails erreicht werden kann, habe ich in meinem letzten Tätigkeitsbericht ausführlich dargestellt (s. 50. Tätigkeitsbericht, Kap. 17.2., S. 184 ff.). Auch die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat sich in ihrer Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ (https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf) umfassend mit den Anforderungen an eine solche Übermittlung per E-Mail beschäftigt.

Bei den Anfragen zur elektronischen Auskunftserteilung durch Arztpraxen verweise ich vornehmlich auf die Möglichkeit der Übermittlung als passwortgeschützte ZIP- oder PDF-Datei im Anhang einer E-Mail. Dies ist aus meiner Sicht die einfachste Möglichkeit, eine sichere elektronische Übermittlung von Gesundheitsdaten zu gewährleisten. Zu beachten ist dabei, dass der Passwortschutz mit einer wirksamen Verschlüsselung verbunden sein muss. Die Wirksamkeit einer Verschlüsselung unterliegt grundsätzlich immer einer zeitlichen Begrenzung durch technologische Fortschritte und entsprechend besser werdenden Angriffen auf verschlüsselte Dateien. Aktuell ist als gängiges Verschlüsselungsverfahren etwa der Advanced Encryption Standard (AES) mit einer ausreichenden Schlüssellänge (256 Bit oder länger) als wirksam zu betrachten. Verantwortliche können sich bei der Auswahl geeigneter

Verfahren z. B. an der technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (BSI TR-02102-1) des Bundesamts für Sicherheit in der Informationstechnik (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf) orientieren.

In jedem Fall hat die Arztpraxis sicherzustellen, dass die Patientin oder der Patient in der Lage ist, die Nachricht zu öffnen. Hierzu sollte vor der Übermittlung stets mit der Empfängerin oder dem Empfänger Rücksprache gehalten werden. Der Austausch eines Passworts zur Entschlüsselung kann ebenfalls im Rahmen einer telefonischen Rücksprache erfolgen. Keinesfalls sollte für die Übermittlung eines Passworts das gleiche Kommunikationsmedium wie für die Übermittlung der verschlüsselten Daten gewählt werden. Durch eine zeitnahe Rücksprache kann auch eventuellen Missverständnissen vorgebeugt werden. So haben sich z. B. einige betroffene Personen in den mir vorliegenden Fällen mit der Bezeichnung „elektronische Auskunft“ auf die Übermittlung von digitalisierten Unterlagen auf einem Datenträger (z. B. CD oder USB-Stick) bezogen. Selbstverständlich kann eine Arztpraxis auch auf diesem Weg ihrer Auskunftspflicht nachkommen, wobei auch in diesem Fall an die Verschlüsselung der übermittelten Daten zu denken ist.

Weiterhin nicht zulässig ist die unverschlüsselte Übermittlung von Gesundheitsdaten aufgrund einer Einwilligung der Patientin oder des Patienten (https://www.datenschutzkonferenz-online.de/media/dskb/20211124_TOP_7_Beschluss_Verzicht_auf_TOMs.pdf). Diese Rechtsauffassung stößt oft auf Unverständnis bei den betroffenen Personen, die meist an einer schnellen und unkomplizierten Auskunftserteilung interessiert sind. Die verantwortlichen Arztpraxen riskieren jedoch einen Verstoß gegen die Vorgaben der Art. 5 Abs. 1 Buchst. f und 32 DS-GVO.

15.7
Berichtigung in der Patientenakte

Dem Patienten steht lediglich dann ein Recht auf Berichtigung nach Art. 16 DS-GVO zu, wenn sich in den Patientenunterlagen objektiv unrichtige oder unvollständige Daten befinden. Der Anspruch auf Berichtigung richtet sich nur auf Tatsachenangaben, die einem empirischen Beweis zugänglich sind.

Ich bekomme regelmäßig Anfragen zur Möglichkeit einer Berichtigung nach Art. 16 DS-GVO in Patientenakten. Hierbei geht es den Eingebenden vor allem darum, dass die Ärztin oder der Arzt ihrer Auffassung nach eine falsche Diagnose erstellt hat.

Grundsätzlich haben Patientinnen und Patienten das Recht, von der Ärztin oder dem Arzt die Berichtigung der sie betreffenden, unrichtigen personenbezogenen Daten nach Art. 16 DS-GVO zu verlangen. Dieses Recht ist u. a. die Ausprägung des Richtigkeitsgrundsatzes aus Art. 5 Abs. 1 Buchst. d DS-GVO.

Allerdings muss hier zwischen Tatsachenangaben, die einem empirischen Beweis zugänglich sind, und Meinungsäußerungen sowie Werturteilen über Personen unterschieden werden. Letztere sind zwar personenbezogene Daten im Sinn des Art. 4 Nr. 1 DS-GVO, deren Berichtigung kann in der Regel aber nicht verlangt werden (vgl. Dix in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 16 Rn. 14.) Den Ärztinnen und Ärzten steht auch im Bereich der Diagnose ein weiter Beurteilungs- und Wertungsspielraum zu. Bei ärztlichen Diagnosen oder anderen Beurteilungen handelt es sich mithin um Wertungen (s. BGH NJW 1989, 774f.). Diese sind einer Bewertung als richtig oder unrichtig nicht zugänglich. Ärztliche Diagnosen oder sonstige Beurteilungen sind daher nicht von dem Berichtigungsrecht erfasst.

Die Eingebenden werden daher regelmäßig von mir darauf hingewiesen, dass der betroffenen Person lediglich dann ein Recht auf Berichtigung nach Art. 16 DS-GVO zusteht, wenn sich in den Patientenunterlagen objektiv unrichtige oder unvollständige Daten befinden. Der Anspruch auf Berichtigung richtet sich nur auf Tatsachenangaben wie z. B. Größe oder Geburtsdatum als auch auf sonstige Angaben wie die Anschrift oder die Kontaktdaten (s. Schröder in: Dochow/Dörfer/Halbe/Hübner/Ippach/Schröder/Schütz/ Strüve, Datenschutz in der ärztlichen Praxis, 2019, S. 158 f.). Die Unrichtigkeit der Daten muss zweifelsfrei festgestellt werden können.

Die Berichtigung muss unverzüglich und unentgeltlich erfolgen, wenn sie berechtigt ist. Aus Gründen der Arzthaftung und der ärztlichen Dokumentationspflicht muss die Berichtigung von Daten immer entsprechend protokolliert werden. So muss nachvollziehbar sein, wer die Berichtigung vorgenommen hat und was genau geändert wurde und was das ursprüngliche Datum war (s. Münchener Anwaltshandbuch Medizinrecht, MedR, § 23 Datenschutz im Gesundheitswesen, Rn. 119, beck-online).

Ein Diagnoseirrtum ist hingegen zivilrechtlich im Rahmen eines Arzthaftungsprozesses geltend zu machen.

Eine alternative Lösung hierzu ist die Aufnahme einer Gegendarstellung (z. B. in Form eines Gutachtens) in die Patientenakte. Dies kann von einem Sperrvermerk begleitet werden. Mit diesem Lösungsansatz habe ich bisher gute Erfahrungen gemacht. Dieser erfordert aber das Einverständnis von beiden Parteien.

16. Wissenschaft und Forschung

Forschung ist Zukunftssicherung. Sie ist nicht nur ein Grundrecht der Forschenden, sondern auch eine Tätigkeit im Allgemeininteresse. Forschungsarbeit muss aber auch die Grundrechte anderer Menschen und andere Interessen des Gemeinwohls berücksichtigen. Soweit sie mit personenbezogenen Daten erfolgt, muss sie die Vorgaben des Datenschutzes beachten. Der Datenschutz darf aber umgekehrt die Forschung nicht so behindern, dass sie nicht mehr oder nur erheblich erschwert möglich ist. Wie dieser Ausgleich erreicht werden kann, war der thematische Schwerpunkt der Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) im Jahr 2022. An der Lösungssuche war ich intensiv beteiligt (Kap. 16.1). Zugleich habe ich im Berichtsjahr wissenschaftliche Institutionen und Verbände in Datenschutzfragen intensiv beraten (Kap. 16.2) und bestehende Kooperationen mit Verbänden im Gesundheitsbereich vertieft und neue begründet (s. Kap. 16.3). Eine große bundesweite Initiative zur C0VID-Forschung war Gegenstand eines von mir mitbetreuten Bewertungsverfahrens (Kap. 16.4).

16.1 Unterstützung der Forschung durch Datenschutz

Vielfach werden Forschung und Datenschutz als gegensätzliche Interessen gesehen. Beide aber, die Forschungsfreiheit und die informationelle Selbstbestimmung, sind Grundrechte. Sie bedürfen einer Zuordnung, die das jeweils andere Grundrecht möglichst wenig einschränkt. Gelingt diese Zuordnung, können sie sich gegenseitig ergänzen und befördern. Forschung ist auf Vertrauen angewiesen, wenn betroffene Personen den Forschenden ihre Daten anvertrauen sollen. Eine wesentliche Grundlage für Vertrauen ist ein überzeugender Datenschutz.

Ausgleich zwischen Grundrechten und Gemeinwohlinteressen

Nach Art. 13 GRCh sind „Kunst und Forschung … frei". Ebenso sind nach Art. 5 Abs. 3 S. 1 GG „Kunst und Wissenschaft, Forschung und Lehre … frei". Als Forschung gilt jede „geistige Tätigkeit mit dem Ziel, in methodischer, systematischer und nachprüfbarer Weise neue Erkenntnisse zu gewinnen" (BVerfGE 35, 79, 112f.). Wissenschaftliche Forschung erfordert Unabhängigkeit und Selbstständigkeit. Die Forschungsfreiheit gilt jedoch nicht schrankenlos. Sie findet ihre Grenzen in den Rechten anderer und in Gemeinwohlbelangen, soweit der Gesetzgeber diese konkretisiert hat.

Ein solches Recht anderer ist das Grundrecht auf Datenschutz gem. Art. 7 und 8 GRCh, das die Entscheidungsbefugnis des Einzelnen über seine personen-

bezogenen Daten gewährleistet. Die gleiche Befugnis schützt das Grundrecht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG. Auch dieses Grundrecht unterliegt Einschränkungen, die im überwiegenden öffentlichen Interesse durch Gesetz festgelegt worden sind. Daher muss der Datenschutz die „Schlüsselfunktion, die einer freien Wissenschaft sowohl für die Selbstverwirklichung des Einzelnen als auch für die gesamtgesellschaftliche Entwicklung zukommt“ (BVerfGE 35, 79, 113), berücksichtigen.

Geraten beide Grundrechte in einen Konflikt, sind beide nach dem Prinzip der praktischen Konkordanz so auszulegen, dass von dem anderen Grundrecht möglichst viel verwirklicht werden kann (s. hierzu Roßnagel, Datenschutz in der Forschung, ZD 2019, 157 ff.). Dieser Ausgleich muss einerseits den betroffenen Personen Schutz gewähren und darf andererseits Fortschritts- und Entwicklungsmöglichkeiten durch wissenschaftliche Forschung nicht übermäßig behindern. Ein solches Ausgleichskonzept versuchen die DS-GVO und das neue deutsche Datenschutzrecht. Sie gewähren der Forschung, um sie zu ermöglichen, vielfältige „Privilegien“ gegenüber anderen Zwecken der Datenverarbeitung und legen ihr aber zugleich auf, in der Durchführung der Datenverarbeitung den betroffenen Personen besondere „Garantien“ für ihre Grundrechte und Freiheiten zu gewährleisten.

Für die Forschung enthält die DS-GVO viele Ausnahmen und Bevorzugungen – z. B. in Art. 5 Abs. 1 Buchst. b eine Ausnahme von der Zweckbindung für die Weiterverarbeitung für Forschungszwecke, in Art. 5 Abs. 1 Buchst. e eine Ausnahme von der Speicherbegrenzung, in Erwägungsgrund 33 eine Ausnahme vom Bestimmtheitsgrundsatz für eine Einwilligung, in Art. 9 Abs. 2 Buchst. j eine Ausnahme vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten, in Art. 14 Abs. 5 Buchst. b eine Einschränkung der Informationspflicht und in Art. 17 Abs. 3 Buchst. d eine Einschränkung der Löschpflicht. Nach Art. 89 Abs. 2 können Mitgliedstaaten weitere Einschränkungen der Rechte der betroffenen Person vorsehen.

Zum Ausgleich dieser „Privilegien“ fordert Art. 89 Abs. 1 DS-GVO „geeignete Garantien für die Rechte und Freiheiten der betroffenen Person“. Diese Garantien sollen durch technische und organisatorische Maßnahmen wie Anonymisierung oder Pseudonymisierung sicherstellen, dass insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird. Soweit jedoch Forschung mit anonymen Daten nicht möglich ist, wie z. B. bei patientenbezogener Forschung, ist diese nach den geltenden Regeln auch mit personenbezogenen Daten möglich.

Forschungsdaten als Schwerpunkt-Thema der DSK

Vor diesem Hintergrund sieht es die DSK als eine wichtige Herausforderung, Wege und Lösungen zu finden, um die Verarbeitung von Forschungsdaten zu wissenschaftlichen Forschungszwecken, die im öffentlichen Interesse liegen, zu ermöglichen und ihre Vorzüge nutzbar zu machen. Gleichzeitig ist den damit verbundenen Risiken konsequent zu begegnen, um den betroffenen Personen einen adäquaten Grundrechtsschutz zu gewährleisten.

Die DSK hat sich daher das Thema „Datenschutz bei Forschungsdaten" zum Schwerpunkt ihrer Arbeiten im Jahr 2022 gewählt. Um die Arbeit an diesem Thema zu befördern und um als einheitlicher Ansprechpartner für bundesweite Forschungsinitiativen zu fungieren, hat sie eine „Taskforce Forschungsdaten" eingerichtet und deren Leitung dem BfDI und mir übertragen. Diese Taskforce hat im Berichtszeitraum sechs Mal getagt und sich in vielfachen Arbeitsgruppensitzungen getroffen, mehrere forschungsbezogene Bewertungsprojekte durchgeführt (s. auch Kap. 16.3), war Ansprechpartner für viele Forschungsinitiativen und -verbände (s. auch Kap. 16.2) und hat zwei Entschließungen der DSK vorbereitet (s. im Folgenden).

In ihrer einstimmigen Entschließung vom 23. März 2022 „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz" (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-08/dsk103_entschliessung_zur_wissenschaftlichen_forschung_0.pdf) unterstrich die DSK, dass wissenschaftliche Forschung und Datenschutz miteinander vereinbar sind. Sie begrüßte Überlegungen der Bundesregierung für ein Forschungsdatengesetz und ein Gesundheitsdatennutzungsgesetz und forderte eine hohe Rechtsklarheit für alle Beteiligten. Sie unterstützt die Erforschung von Methoden, Forschungsdaten so zu verarbeiten, dass Persönlichkeitsrechte bestmöglich geschützt werden. Schließlich forderte sie den rechtlichen Schutz eines Forschungsgeheimnisses.

Unter dem Titel „Stärkung der Forschung durch Datenschutz" veranstalteten die Präsidentin des Hessischen Landtags Astrid Wallmann und ich am 6. Oktober 2022 das „25. Wiesbadener Forum Datenschutz" im Hessischen Landtag (s. näher Kap. 18). Es verfolgte die Fragestellung, wie Forschung und Datenschutz das gemeinsame Ziel eines menschenwürdigen Fortschritts durch verantwortungsvolle Datennutzung erreichen können. Prof. Ulrich Kelber, BfDI, ging in seinem Vortrag „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz" der Frage nach, welcher rechtspolitische Rahmen notwendig ist, um das Ziel einer verantwortungsvollen Datennutzung zu erreichen. Prof. Dr. Franziska Boehm vom Karlsruher Institut für Technologie (KIT) untersuchte in ihrem Vortrag „Der besondere Schutz der Forschung in der Datenschutz-Grundverordnung", welche besondere

Berücksichtigung von Forschungsinteressen die DS-GVO vorsieht und wie diese Sonderregeln in der Praxis zur Anwendung kommen können. Prof. Dr. Dr. Eric Hilgendorf von der Universität Würzburg erweiterte durch seinen Vortrag „Der Datenschutz in der künftigen Regulierung europäischer Forschungsdatenräume“ die Diskussion um die europäische Perspektive und Prof. Dr. Hannes Federrath, Universität Hamburg, von 2018 bis 2021 Präsident der Gesellschaft für Informatik, betrachtete in seinem Vortrag „Datenschutzwahrende Methoden der Forschungsdatenverarbeitung“ die Fragestellung der Tagung aus technischer Sicht.

Am 3. November 2022 führte der BfDI in der Kaiserin-Friedrich-Stiftung in Berlin das Symposium „Forschung mit Gesundheitsdaten – Herausforderungen im Zeichen der Datenschutz-Grundverordnung“ durch. Vorträge aus dem Bundesministerium für Gesundheit, aus dem Kreis der Datenschützer, der medizinischen (Verbund-)Forschung, der Medizininformatik und der Rechtswissenschaft steckten die Problemkreise ab, die bei einem praktischen Ausgleich zwischen medizinischer Forschung und Datenschutz beachtet werden müssen. Einigkeit bestand insoweit, als die Aufgabe darin besteht, den normativen Rahmen, die Strukturen der Entscheidungsfindungen und die Praktiken der Kooperation fortzuentwickeln.

Die DSK führte am 21. November 2022 im alten Plenarsaal des Bundesrates in Bonn ein Symposium „Gesundheitsforschung trifft Datenschutz“ durch, dessen Höhepunkt ein von Frederik Richter von der Stiftung Datenschutz moderiertes Streitgespräch zwischen Prof. Dr. Sylvia Thun, Digitale und Interoperabilität am Berlin Institute of Health in der Charité Berlin, und mir war. In diesem ging es vor allem um die Notwendigkeit der Verarbeitung personenbezogener Daten für die medizinische Forschung und die Möglichkeiten zum Schutz der Datensouveränität der betroffenen Patienten durch Gestaltung der Datenverarbeitungsprozesse. Einigkeit bestand darin, dass der Gesetzgeber für mehr Einheitlichkeit und Rechtssicherheit hinsichtlich der relevanten Rechtsregeln sorgen muss. Differenzen blieben hinsichtlich der notwendigen informationstechnischen Schutzmaßnahmen in der medizinischen Forschung sowie der Bedeutung des Zweckbindungsprinzips und des Prinzips der Minimierung des Personenbezugs.

Petersberger Erklärung

Auf ihrer 104. Konferenz auf dem Petersberg bei Bonn beschloss die DSK am 23. November 2022 ihre „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“ (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/06_entschliessung_-_petersberger_erklaerung.pdf). Sie gibt

mit ihr Empfehlungen an die Gesetzgeber in Deutschland und der Union für die Regelung der Forschung mit Gesundheitsdaten. Wesentliche Aspekte sind die folgenden:

In der Union und in Deutschland besteht ein Bedarf, die Regelungen für die Nutzung von Forschungsdaten näher zu spezifizieren und kohärent auszugestalten. Ziel dabei sollte eine länderübergreifende, einheitliche Regelung zur Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken sein, die Forschungsverbünden mit Partnern in unterschiedlichen Bundesländern das Einhalten der datenschutzrechtlichen Anforderungen erleichtert.

Der Gesetzgeber sollte die im Allgemeininteresse liegende Forschung mit Gesundheitsdaten ermöglichen, aber auch ihre Grenzen festlegen und die Interessen der betroffenen Personen wahren. Er darf diese komplexen Fragestellungen nicht vollständig auf die betroffenen Personen und die Forschenden verlagern. Mit einer solchen Regelung kann er bei der Nutzung von Daten aus anderen Quellen, beispielsweise Behandlungsdaten aus Krankenhäusern, aus medizinischen Registern oder auch aus anderen Forschungsprojekten (sog. Sekundärnutzung) datenschutzkonforme Forschung ermöglichen oder erleichtern, wenn das Einholen einer ausdrücklichen Einwilligung nicht durchführbar wäre oder das Forschungsvorhaben ernsthaft beeinträchtigt würde. Dabei sollte er aber auch festlegen, welche Forschung inhaltlich im Gemeinwohlinteresse liegt und welchen weiteren Anforderungen an das Verfahren und die Durchführung die Forschung entsprechen muss.

Mit Blick auf den Schutz betroffener Personen gilt der Grundsatz: Je höher der Schutz durch geeignete Garantien und Maßnahmen ist, desto umfangreicher und spezifischer können die Daten genutzt werden. Soweit der Forschungszweck mit anonymisierten Daten erreicht werden kann, dürfen nur anonymisierte Daten verarbeitet werden. Dabei bestehen hohe Anforderungen an die Anonymisierung personenbezogener Daten. Soweit der Forschungszweck eine vollständige Anonymisierung verhindert, sind effektive Maßnahmen der Pseudonymisierung vorzusehen. Diese sollte gesetzlich an unabhängige und eigenverantwortliche Vertrauensstellen übertragen werden. Darüber hinaus sind technische und organisatorische Schutzmaßnahmen entsprechend der bei Gesundheitsdaten gesteigerten Anforderungen gemäß dem Stand der Technik zu treffen wie z. B. die Verschlüsselung der Daten. Anonymisierung, Pseudonymisierung und Verschlüsselung sollten vom Gesetzgeber präzisiert werden.

Will der Gesetzgeber die Verarbeitung zu Forschungszwecken nicht auf eine Einwilligung, sondern auf eine gesetzliche Grundlage stellen, sollte er die Einbindung der betroffenen Personen durch Regelungen zu einer aus-

reichenden Transparenz und zu einer voraussetzungslosen Widerspruchsmöglichkeit vorsehen.

Sofern eine gesetzliche Grundlage geschaffen werden sollte, um Datensätze aus verschiedenen Quellen, z. B. aus medizinischen Registern, zu verknüpfen, sind besondere Sicherheits- und Schutzmaßnahmen vorzusehen. Dies kann z. B. besondere Record-Linkage-Verfahren umfassen, die nur eine anlassbezogene und temporäre Zusammenführung zulassen sollten. Die betroffenen Personen sollten über ein Einwilligungsmanagementsystem die Gelegenheit haben, in Kenntnis der Risiken der Zusammenführung aktiv zuzustimmen. Alternativ müssen technische Methoden oder Maßnahmen sicherstellen, dass die Re-Identifizierung der betroffenen Person trotz der Verkettung ausgeschlossen ist. Außerdem sollten die Daten – soweit dies vom Forschungszweck her möglich ist – am Ort der Speicherung ausgewertet werden, so dass den Ort der sicheren Speicherung nur anonyme Ergebnisse der Datenauswertung verlassen. Dabei ist eine Mehrfachspeicherung zu vermeiden.

Durch Regelung eines Forschungsgeheimnisses soll die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe gestellt, deren Beschlagnahme verboten und ein Zeugnisverweigerungsrecht für wissenschaftlich Forschende und ihre Berufshelfer geschaffen werden.

16.2
Datenschutzberatung in Wissenschaft und Forschung

Neben der Bearbeitung von Eingaben macht auch die Beratung von Forschungsprojekten einen großen Bestandteil meiner Arbeit aus. Von forschenden Studierenden bis hin zur Universität oder größeren Unternehmen aus dem Gesundheitsbereich sind dabei alle Bereiche und Stellen vertreten.

Beratungsbedarf

Gerade in der Planungs- und Anfangsphase von Forschungsprojekten ist es oft wichtig, im Hinblick auf den Datenschutz die richtigen Impulse zu setzen, um das Projekt in die richtige Richtung zu lenken. Wie ich beobachten konnte, fehlt es insoweit an Anlaufstellen für junge und erfahrene Forschende in Hessen. In der Vergangenheit habe ich diese Lücke daher sehr gerne gefüllt.

Bei einer Vielzahl an Projekten fällt dabei auf, dass oft einige Aspekte vernachlässigt werden, die aus Sicht des Datenschutzes wichtig sind. Dies sind stichpunktartig die folgenden Punkte:

– Ausführliche Überlegungen und Begründungen hinsichtlich der Ausgestaltung der Verantwortlichkeiten, gerade dann, wenn mehrere Stellen

beteiligt sind (getrennte oder gemeinsame Verantwortlichkeit oder Auftragsverarbeitung).
– Klare Bestimmung der Rechtsgrundlagen für die Verarbeitung personenbezogener Daten.
– Ausreichende Transparenz gegenüber den betroffenen Personen, insbesondere Informationen über die Datenverarbeitung nach Art. 13 oder 14 DS-GVO.
– Rechtzeitige Einbindung des oder der internen Datenschutzbeauftragten und ggfs. der Aufsichtsbehörde.
– Aussagekräftiges Datenschutzkonzept, wie es auch viele Fördermittelgeber voraussetzen.
– Berücksichtigung der besonderen datenschutzrechtlichen Anforderungen, die an eine Verarbeitung von Gesundheitsdaten (als besondere Kategorien gem. Art. 9 DS-GVO) oder an eine automatisierte Entscheidungsfindung – Stichwort algorithmenbasierte Entscheidungsunterstützungssysteme (KI) – gestellt werden. Dazu kann beispielsweise die Notwendigkeit einer Datenschutz-Folgenabschätzung gehören.
– Eine risikobasierte und am Schutzbedarf der personenbezogenen Daten orientierte Technikgestaltung, die schon bei der Festlegung der Mittel beginnt und die Grundsätze der Datenverarbeitung – wie z. B. Vertraulichkeit, Datenminimierung, Zweckbindung – umsetzt und entsprechend geeignete und angemessene technisch-organisatorische Maßnahmen vorsieht.

Sofern an die genannten Punkte gedacht wird, ist dies erfahrungsgemäß zugleich ein Motor für die Umsetzungsgeschwindigkeit.

Beispiele aus der Praxis

Zu den erfolgreichen Projekten, die unter der genannten Beratungspraxis hervorgegangen sind, gehört das Projekt TeleCOVID Hessen. Hierdurch wurden in sehr kurzer Zeit krankenhausübergreifende Konsile und ein fachlicher Austausch zu COVID-Erkrankungen während der Hochphase der Corona-Pandemie ermöglicht. Realisierbar war dies auch aufgrund der vorbildlichen und rechtzeitigen Einbindung meiner Behörde durch das Hessische Ministerium für Soziales und Integration (HMSI): Eine Zusammenarbeit, wie ich sie mir weiter wünsche. Das Projekt ist mittlerweile ausgebaut worden und hat nicht mehr nur COVID-Erkrankungen zum Gegenstand (s. hierzu 50. Tätigkeitsbericht, Kap. 17.5; https://soziales.hessen.de/presse/telecovid-app-hessen-vernetzt-krankenhaeuser-0).

Darüber hinaus gibt es aktuell eine Reihe von interessanten Projekten aus dem Rettungsdienstbereich, in die ich eingebunden bin. Hier wäre etwa das

SAN-Projekt zu nennen, mit dem die Notfallstationen der Krankenhäuser durch örtliche, nahe gelegene Arztpraxen entlastet werden sollen. Gerade in Zeiten der Pandemie ist dies wieder ein Projekt von besonderer Bedeutung.

Ebenso bin ich beim sogenannten ETA/ETN-Projekt beteiligt, bei dem rettungsdienstspezifische Messenger-Dienste zum Einsatz kommen sollen.

Auch wenn diese Projekte zum Teil noch nicht abgeschlossen sind, ist auch hier rechtzeitig an die Einbindung der Datenschutzaufsicht gedacht worden, so dass früh entscheidende Weichen für die Projekte gestellt werden konnten.

Vielleicht ist hier noch der Wunsch angebracht, dass der E-Health-Beirat des HMSI seine Tätigkeit wiederaufnimmt und in einer höheren Frequenz und Regelmäßigkeit tagt. Aktuell gibt es genügend Projekte, die auch dort erörtert werden könnten und bezüglich derer es hilfreich ist, wenn man Entscheidungsträger aus dem Gesundheitsbereich in Hessen an einem Ort zusammenbringt. Eventuell kann diese Lücke auch durch die in diesem Jahr neu gegründete IGH AG Gesundheitsdaten geschlossen werden. Diese bringt Unternehmen aus dem Gesundheitsbereich und Vertreter der Ministerien zusammen, um Hessen als datenschutzfreundlichen und der Digitalisierung zugewandten Standort den Rücken zu stärken.

Abschließend noch der Hinweis auf ein länderübergreifendes Projekt, dessen Projektkoordinatoren ihren Sitz in Hessen haben. Bei dem Projekt geht es um die Erforschung der Auswirkungen der COVID-Erkrankung auf die Lunge. Hier habe ich im Rahmen der Taskforce Forschungsdaten der DSK eine koordinierende Funktion und werde auf ein einheitliches Votum durch alle Aufsichtsbehörden hinwirken (s. hierzu näher Kap. 16.4).

16.3
Kooperationen zum Datenschutz im Gesundheitsbereich

Bereits in der Vergangenheit war es mir ein wichtiges Anliegen, in den Bereichen Gesundheit, Wissenschaft und Forschung in einen Austausch mit den in diesen Bereichen aktiven Stellen und Verbänden zu kommen. Die aktuellen geplanten Gesetzesvorhaben auf nationaler und europäischer Ebene machen diesen Dialog wichtiger denn je. In meiner Funktion als Vorsitzender des AK Wissenschaft und Forschung der DSK sowie im Rahmen des Co-Vorsitzes der Taskforce Forschungsdaten führe ich diesen Dialog sowohl auf Landes- als auch auf länderübergreifender Ebene.

Dialog mit Fachverbänden im Rahmen des AK Wissenschaft und Forschung

Eine wichtige Rolle im Forschungskontext spielt die klinische Forschung. Hier freut es mich besonders, dass ich bereits im Jahr 2018 einen ständigen Austausch des AK Wissenschaft und Forschung der DSK mit dem Verband der forschenden Arzneimittelhersteller (v.f.a. e. V.) ins Leben rufen konnte. Die Konsultationsgruppe Datenschutz im Bereich der klinischen Forschung tagte in diesem Jahr bereits zum neunten Mal. Themen, die in den vergangenen neun Sitzungen auf der Agenda standen, reichten von Fragen rund um die Anonymisierung bis hin zu Konstellationen, die die Verantwortlichkeit der an klinischen Prüfungen beteiligten Stellen betreffen. Auch der Entwurf einer Verordnung der Europäischen Kommission zu einem European Health Data Space (EHDS) war von starkem Interesse für die forschenden Unternehmen und stellte daher einen Schwerpunkt in diesem Jahr dar.

Soweit dies die klinische Forschung betrifft, ist zudem auch der Bundesverband der Pharmazeutischen Industrie (bpi e. V.) zu erwähnen, der sich ebenfalls immer wieder in einem Austausch mit dem AK Wissenschaft und Forschung befindet.

Dialog mit Fachverbänden im Rahmen der Taskforce Forschungsdaten

Eine der Hauptaufgaben der Taskforce Forschungsdaten ist es, die Medizininformatik-Initiative (MII) und den dazugehörigen Austausch mit der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF) intensiv zu begleiten.

Ein Schwerpunkt war es im vergangenen Berichtszeitraum und wird es im kommenden Berichtszeitraum sein, den Dialog zu den Mustertexten der MII zur Einwilligung in die medizinische Forschung fortzuführen und das Modul Drittstaatentransfer abzustimmen. Hierzu ist bereits ein Workshop in Planung, der dazu dienen soll, die Interessen des Datenschutzes und der Forschenden in einen interessengerechten Ausgleich zu bringen.

Darüber hinaus steht die Taskforce Forschungsdaten aber auch auf Anfrage anderen Gremien und Fachverbänden für einen Austausch zum Thema Forschungsdaten zur Verfügung. So fand beispielsweise im Jahr 2022 ein Treffen mit der AG Bio-IT, Big Data und E-Health der BIO AG Deutschland e. V. statt. Es stellte sich heraus, dass das Thema der Sekundärnutzung von Daten von besonderem Interesse ist und eine weitere Befassung der Taskforce mit diesem Thema stark von den Vertretern der BIO AG Deutschland e. V befürwortet wird.

Dialog mit Fachverbänden auf Landesebene

In der Vergangenheit gab es auch immer wieder kritische Stimmen zur Rolle des Datenschutzes im Kontext von Gesundheitsversorgung und Forschung im Medizinbereich. Hier war es für mich von besonderer Bedeutung, dass im Jahr 2022 erstmalig ein Austausch mit der Deutschen Gesellschaft für Innere Medizin (DGIM e. V.) stattfand, der größten medizinisch-wissenschaftlichen Fachgesellschaft in Europa (s. auch https://datenschutz.hessen.de/presse/zu-einem-besseren-verstaendnis-zwischen-medizin-und-datenschutz).

Bei den beiden stattgefundenen Treffen war es ein wichtiges Anliegen, Verständnis für die Belange des Datenschutzes zu wecken und zugleich die Erforderlichkeiten und Bedürfnisse aus den Bereichen Medizin und Forschung zu besprechen. Auch wurden Forderungen der DGIM und der DSK in ihrer Petersberger Erklärung (s. Kap. 16.1) gemeinsam abgeglichen. Es besteht die Erwartung, dass dieser fruchtbare Dialog im nächsten Berichtsjahr fortgesetzt wird.

Von gleichermaßen großer Bedeutung auf Landesebene ist auch die Teilnahme an der IGH AG Gesundheitsdaten. Diese setzt sich aus forschenden Gesundheitsunternehmen aus Hessen, Vertretern des Hessischen Ministeriums für Soziales und Integration und des Hessischen Ministeriums für Digitale Strategie und Entwicklung zusammen. Hier ist es die Bestrebung, Hessen als Standort für Gesundheitsunternehmen unter Beachtung datenschutzrechtlicher Grundsätze weiter zu stärken und noch attraktiver zu machen. Als Vorbild dient hier insbesondere die Roadmap Gesundheitsdatennutzung aus Baden-Württemberg (s. https://www.forum-gesundheitsstandort-bw.de/download_file/force/21093/84221). Ein Papier nach diesem Vorbild ist in Arbeit und wird voraussichtlich im kommenden Jahr finalisiert werden.

Ausblick

Für die Zukunft wird es wichtig, den Dialog auch auf europäischer Ebene zu intensivieren und über die dort bereits vorhandenen Gremien Einfluss auf die kommenden Entwicklungen zu nehmen. Für die Bereiche Gesundheit sowie Wissenschaft und Forschung ist besonders die „Compliance, eGovernment und Health Expert Subgroup“ des EDSA relevant. Hier habe ich mich bereits an der Prüfung von Verhaltensregeln nach Art. 40 DS-GVO (Code of Conduct – CoC) beteiligt und werde auch die Erstellung der Leitlinien für die wissenschaftliche Forschung begleiten.

16.4
Forschungsinitiative RACOON

Als Co-Vorsitzender der Taskforce Forschungsdaten der DSK habe ich die Beratung der Forschungsinitiative RACOON federführend koordiniert. Bei einem solchen länderübergreifenden Forschungsprojekt verschiedener Universitätskliniken müssen die Verantwortlichen ihre jeweiligen landesspezifischen datenschutzrechtlichen Regelungen beachten. Bei dieser herausfordernden gesetzlichen Ausgangslage habe ich auf eine konstruktive Beratung durch die Taskforce Forschungsdaten hingewirkt.

Hintergrund

Durch die bundesländerübergreifende Forschungsinitiative RACOON, an der alle radiologischen Universitätskliniken Deutschlands beteiligt sind, soll eine neuartige Forschungsinfrastruktur zur strukturierten Erfassung und Auswertung radiologischer Daten von COVID-19-Fällen geschaffen werden. Dabei sollen die radiologischen Daten zunächst lokal in dem jeweiligen Universitätsklinikum strukturiert und analysiert werden. In einem zweiten Schritt sollen die Daten nach Entfernung von personenbeziehbaren Informationen über eine zentrale Instanz auch den anderen beteiligten Universitätskliniken für bestimmte Forschungsprojekte zur Verfügung gestellt werden.

Hierbei ist aufgrund der föderalen Struktur der datenschutzrechtlichen Regelungen und der Zuständigkeit der jeweiligen Datenschutzaufsichtsbehörden eine enge Beteiligung und Abstimmung zwischen den Aufsichtsbehörden erforderlich. Die im Herbst 2021 gegründete Taskforce Forschungsdaten der DSK ermöglichte eine effektive und schnelle Zusammenarbeit.

Datenschutzrechtliche Herausforderungen

Die verantwortlichen Universitätskliniken sind von einer gemeinsamen Verantwortlichkeit der beteiligten Universitätsklinken ausgegangen und haben hierzu ein entsprechendes Vertragswerk erstellt. Die Charité in Berlin und die Universitätsklinik in Frankfurt haben die Projektkoordination der Forschungsinitiative übernommen.

Die datenschutzrechtlichen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten mussten klar bezeichnet werden. § 287a S. 1 des Fünften Sozialgesetzbuches (SGB V) enthält eine Regelung zur Rechtsgrundlage bei länderübergreifenden Vorhaben der Versorgungs- und Gesundheitsforschung, an denen Stellen aus zwei oder mehr Ländern als Verantwortliche beteiligt sind. Hiernach ist auf solche Vorhaben § 27 BDSG anwendbar. Durch

die Benennung der Universitätsklinik in Frankfurt als Hauptverantwortliche konnten die formalen Voraussetzungen dieser Vorschrift erfüllt werden.

Aufgrund von Bedenken hinsichtlich der Bundeszuständigkeit und der systematischen Stellung im SGB V bestanden aber Zweifel an der Anwendbarkeit des § 287a SGB V auf das Projekt RACOON. Daher wurden auch die landesrechtlichen Regelungen, insbesondere die Landeskrankenhausgesetze, als Rechtsgrundlagen herangezogen. Die sich wesentlich unterscheidenden Regelungen in den Landesgesetzen hatten auch unterschiedliche Bewertungen durch die Landesaufsichtsbehörden zur Folge.

Auch die datenschutzrechtlichen Anforderungen an die Anonymisierung von radiologischen Bilddaten stellte für die Projektverantwortlichen eine Herausforderung dar.

Die Projektverantwortlichen haben der Taskforce Forschungsdaten umfangreiche datenschutzrechtliche Dokumente zur Verfügung gestellt und das Projekt in einer Sondersitzung der Taskforce Forschungsdaten vorgestellt. Hinweise aus dem Kreis der Taskforce-Mitglieder wurden berücksichtigt und Nachbesserungen sind erfolgt.

Zum Ende des Berichtszeitraums konnten sich die beteiligten Aufsichtsbehörden mehrheitlich auf eine positive Bewertung des Vorhabens einigen

Fazit

Die Vorgehensweise der Taskforce Forschungsdaten kann als Vorbild für die Begleitung zukünftiger länderübergreifender Forschungsprojekte dienen.

Es hat sich gezeigt, dass in Hessen für die Forschung im Krankenhausbereich durch den Verweis in § 12 Abs. 3 HKHG auf § 24 HDSIG eine gute Gesetzeslage besteht. In anderen Ländern konnte hingegen im Rahmen der Beratung zum Projekt RACOON ein Änderungsbedarf hinsichtlich der landesspezifischen Regelungen festgestellt werden.

Die Beachtung unterschiedlicher landesrechtlicher Rechtsgrundlagen stellt die Forschenden vor Herausforderungen. Im Interesse der Forschung sollten die datenschutzrechtlichen Regelungen zur länderübergreifenden Forschung unter Beachtung der verfassungsrechtlichen Vorgaben weiter harmonisiert werden.

17. Technik und Organisation

Die Umsetzung des Datenschutzrechts wird vielfach durch mangelhafte Technik und ungenügende Organisation verursacht. Daher ist es für die Wahrnehmung meiner Aufgaben wichtig, ein IT-Laboratorium zu betreiben, das die erforderlichen technischen Untersuchungen durchführen kann (Kap. 17.1). Datenschutzverstöße sind mir als Aufsichtsbehörde zu melden (Kap. 17.2). Dies ist von besonderer Bedeutung, wenn Auftragsverarbeiter angegriffen werden, weil davon viele Verantwortliche betroffen sind (Kap. 17.3). Die Fehlerfreiheit von Technik und Organisation kann auch Gegenstand einer systematischen Prüfung sein (Kap. 17.4). Für den Datenschutz relevante Schwachstellen kommen insbesondere bei selbst entwickelter Software vor (Kap. 17.5). Nach Datenschutzverstößen können die betroffenen Personen zu benachrichtigen sein, was an einem Fall des Missbrauchs von E-Mail-Konten erläutert wird (Kap. 17.6). Die nachteiligen Folgen von Angriffen auf IT-Systeme können stark gemindert werden, wenn die Verantwortlichen oder Auftragsverarbeiter über ein funktionierendes Backup verfügen und die verlorenen Daten wiederherstellen können (Kap. 17.7)

17.1 Technische Datenschutzprüfungen im IT-Laboratorium

Nicht zuletzt aufgrund der fortschreitenden Digitalisierung in allen Lebensbereichen befasst sich meine Behörde mit unterschiedlichsten technischen Sachverhalten. Ist eine rein dokumentenbasierte Überprüfung nicht ausreichend, führen die Mitarbeitenden meiner technischen Abteilung technische Datenschutzüberprüfungen im eigens hierfür eingerichteten IT-Laboratorium meiner Behörde durch. Diese technischen Datenschutzüberprüfungen müssen verschiedenen Anforderungen genügen, um rechtskonform durchgeführt werden zu können.

Eingaben zu technischen Sachverhalten

Im Berichtszeitraum erreichten mich regelmäßig Eingaben, die sich auf technische Sachverhalte richteten oder solche als Hintergrund hatten. Beispiele hierfür waren

– Beschwerden gemäß Art. 77 DS-GVO über Websites, in die in vermeintlich unzulässiger Weise externe Ressourcen eingebunden wurden, z. B. Schriftarten, welche von Servern eines Unternehmens mit Sitz in den USA nachgeladen wurden,
– Eingaben zu vermuteten Verletzungen des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12 DS-GVO, etwa im Zusammenhang mit

potenziellen Schwachstellen in Web-Anwendungen oder mobilen Applikationen und der damit verbundenen unbeabsichtigten Offenlegung personenbezogener Daten, sowie

– Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO aufgrund von Hackerangriffen und der Veröffentlichung von personenbezogenen Daten durch die Angreifer.

Schon diese exemplarischen Sachverhalte liefern einen ersten Eindruck vom breiten Spektrum technischer Fragestellungen, mit denen sich die Mitarbeitenden aus der technischen Abteilung meiner Behörde befassten und befassen.

Die Detailtiefe und technische Fundiertheit der im Berichtszeitraum an mich gerichteten Eingaben variierte stark. Sie reichte von knappen und allgemein gehaltenen Schilderungen bis hin zu einer detaillierten Beschreibung des Sachverhalts inklusive des schrittweisen Vorgehens zum Nachvollziehen.

Technische Datenschutzüberprüfung

Bei Eingaben zu technischen Sachverhalten bestand häufig der Bedarf nach einer Überprüfung der übermittelten Angaben sowie einer Bewertung und Beurteilung der Ergebnisse dieser Überprüfung. Diese bildeten die Grundlage für das etwaige weitere Tätigwerden meinerseits, etwa der Ergreifung von Maßnahmen gemäß Art. 58 Abs. 2 DS-GVO.

Meine Behörde ist gemäß Art. 58 Abs. 1 Buchst. b DS-GVO befugt, Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen. Diese Befugnis wurde vom Gesetzgeber bewusst allgemein formuliert und schließt insbesondere auch die Durchführung technischer Datenschutzüberprüfungen mit ein. Hierbei handelt es sich um die Überprüfung technischer Sachverhalte mittels geeigneter technischer Prüfwerkzeuge. Derartige technische Datenschutzüberprüfungen müssen nicht zwingend in den Räumlichkeiten von Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO oder Auftragsverarbeitern gemäß Art. 4 Nr. 8 DS-GVO durchgeführt werden. Die Untersuchungsbefugnis meiner Behörde gemäß Art. 58 Abs. 1 Buchst. b DS-GVO bietet mir vielmehr die Möglichkeit, in meiner Dienststelle oder aus dieser heraus technische Datenschutzüberprüfungen durchzuführen (s. näher Bruhn/Roßnagel/Wachhaus/Zimmer, Datenschutzüberprüfungen im IT-Labor von Aufsichtsbehörden, DuD 2022, 685 ff.). Hiervon habe ich im Berichtszeitraum insbesondere Gebrauch gemacht, wenn zu prüfende technische Sachverhalte in Zusammenhang mit über das öffentliche Internet zugänglichen IT-Systemen oder -Diensten standen. Hierbei mussten technische Datenschutzüberprüfungen immer gemäß den allgemeinen Grundsätzen des behördlichen Handelns im Rechtsstaat erfolgen. Bei der Durchführung mussten somit die entsprechenden Anforderungen erfüllt werden. Aufgrund der in der DS-GVO gegebenen

Rechtsgrundlage agieren meine Mitarbeitenden im Rahmen ihres dienstlichen Handelns damit immer in befugter Weise, weshalb mögliche Straftatbestände, wie etwa das Ausspähen von Daten gemäß § 202a Strafgesetzbuch (StGB), hierfür nicht einschlägig sind.

Als Voraussetzung für die Durchführung technischer Datenschutzüberprüfungen müssen die Mitarbeitenden der technischen Abteilung meiner Behörde mit angemessenen und geeigneten Prüfwerkzeugen ausgestattet sein. Auch müssen sie über eine entsprechende Infrastruktur verfügen, um die jeweiligen Prüfwerkzeuge effektiv und effizient einsetzen zu können. Um diese Voraussetzungen zu erfüllen, wurde in meiner Behörde schon vor dem Berichtszeitraum ein IT-Laboratorium eingerichtet und im Berichtszeitraum weiter ausgebaut.

Interessenabwägung im Rahmen technischer Datenschutzüberprüfungen

Im Rahmen der Durchführung einer technischen Datenschutzüberprüfung wird in der überwiegenden Mehrzahl der Fälle mit IT-Systemen und -Diensten von Verantwortlichen und Auftragsverarbeitern interagiert. Hierdurch werden in der Regel deren rechtlich geschützte Interessen berührt. Art, Umfang und Ausmaß dieses Eingriffs hängen hierbei vom zugrundeliegenden Sachverhalt, von den eingesetzten Prüfwerkzeugen und vom konkreten Ablauf der technischen Datenschutzüberprüfung ab. All diese Faktoren sind somit im Rahmen der Ausübung meines pflichtgemäßen Ermessens bei der Konzeption und Durchführung einer technischen Datenschutzüberprüfung angemessen zu berücksichtigen. Hierbei muss ich entgegenstehende Interessen berücksichtigen, diese Interessen mit meinem Prüf- und Schutzauftrag abwägen sowie die Vertretbarkeit und Verhältnismäßigkeit des Mitteleinsatzes gewährleisten.

Grundsätzlich dürften diejenigen Prüfschritte einer technischen Datenschutzüberprüfung vertretbar und verhältnismäßig sein, bei denen Form und Intensität der Interaktionen mit IT-Systemen und -Diensten von Verantwortlichen oder Auftragsverarbeitern für diese erwartbar sind. Derartige Prüfschritte wurden und werden im IT-Laboratorium meiner Behörde aus Gründen der Verhältnismäßigkeit in der Regel ohne Einbeziehung von Verantwortlichen oder Auftragsverarbeitern durchgeführt, etwa im Rahmen von Vorermittlungen.

Es kann jedoch zu Situationen kommen, in denen die Vertretbarkeit einzelner Prüfschritte einer technischen Datenschutzüberprüfung fraglich erscheint. Dies kann zum Beispiel in einer nur rudimentären oder unklaren Informationslage in Bezug auf die zu prüfenden IT-Systeme und -Dienste begründet sein. Auch könnte die Art eines geplanten Prüfschritts in bestimmten Fällen

zu Schäden an geprüften IT-Systemen und -Diensten führen. In solchen Fällen werden die jeweiligen Verantwortlichen und Auftragsverarbeiter über die geplanten Schritte informiert. Hierbei werden in der Regel weitere, für die Prüfung erforderliche Informationen erfragt, und es wird Verantwortlichen und Auftragsverarbeitern die Möglichkeit zur Stellungnahme und zum Vorbringen von Vorbehalten eingeräumt. Die Rückäußerungen werden im Anschluss derart berücksichtigt, dass im Bedarfsfall eine Anpassung einzelner Prüfschritte erfolgt. Auch kann es erforderlich werden, dass Prüfschritte gemeinsam mit Verantwortlichen und Auftragsverarbeitern durchgeführt oder verworfen werden.

Technische Datenschutzüberprüfung im Verwaltungsverfahren

Technische Datenschutzüberprüfungen werden häufig im Vorfeld eines Verwaltungsverfahrens oder als dessen Bestandteil durchgeführt. Im ersten Fall dienen sie der Aufklärung von Sachverhalten im Rahmen von Vorermittlungen, um festzustellen, ob und mit welchem Ziel ein Verwaltungsverfahren eröffnet werden soll. Im zweiten Fall kommen technische Datenschutzüberprüfungen häufig zum Einsatz, um technische Sachverhalte aufzuklären und Beweismittel sicherzustellen.

In beiden Fällen ist eine generelle Verpflichtung zur Vorabinformation von Verantwortlichen oder Auftragsverarbeitern über die Durchführung technischer Datenschutzüberprüfungen ebenso wenig gegeben wie eine Pflicht zur Information im Nachgang. Eine solche Beteiligtenöffentlichkeit ist in den Rechtsvorschriften zur Beweisaufnahme im Verwaltungsverfahren, wie etwa § 26 Verwaltungsverfahrensgesetz (VwVfG), nicht vorgesehen. Eine Vorabinformation ist jedoch, wie oben beschrieben, weiterhin mindestens erforderlich, wenn die Durchführung einer technischen Datenschutzüberprüfung ansonsten als nicht vertretbar erscheint.

Über die Eröffnung eines Verwaltungsverfahrens selbst müssen Verantwortliche und Auftragsverarbeiter ebenfalls nicht zwingend informiert werden. Sie gilt unabhängig von der Durchführung einer technischen Datenschutzprüfung als Bestandteil des jeweiligen Verwaltungsverfahrens.

Die Durchführung einer technischen Datenschutzüberprüfung ist von der Nutzung ihrer Ergebnisse im Rahmen eines Verwaltungsverfahrens unabhängig. So können Prüfergebnisse z. B. als Grundlage für das Erlassen eines Verwaltungsakts dienen, etwa einer Anordnung gemäß Art. 58 Abs. 2 DS-GVO. In diesem Fall ist dem Verantwortlichen oder Auftragsverarbeiter aufgrund von § 28 VwVfG die Gelegenheit zu geben, vor dem Erlass des Verwaltungsakts zum zugrundeliegenden Sachverhalt Stellung zu nehmen. Hierzu sind ihm auch die Ergebnisse einer technischen Datenschutzüberprü-

fung mitzuteilen. Daher kommt der Beweiseignung der Prüfungsergebnisse und der zugehörigen Dokumentation eine besondere Bedeutung zu.

Ausgewählte Prüfschritte

Im Folgenden werden einige ausgewählte, repräsentative Prüfschritte aus technischen Datenschutzüberprüfungen im Berichtszeitraum skizziert, um einen ersten, konkreteren Eindruck von den Gegenständen technischer Datenschutzüberprüfungen zu vermitteln.

Im Rahmen technischer Datenschutzüberprüfungen werden häufig Recherchen auf Webseiten im Internet, in Social-Media-Kanälen oder im sogenannten „Darknet“ durchgeführt. Hierbei werden öffentlich zugängliche Informationen ermittelt und ausgewertet. Diese können sich beispielsweise auf Schwachstellen in IT-Systemen und -Diensten oder auf die Veröffentlichung personenbezogener Daten beziehen. Internet-Archive und ähnliche Dienste können im Bedarfsfall dazu genutzt werden, um zu ermitteln, in welchem Zeitraum eine Veröffentlichung voraussichtlich vorlag. Das Spektrum der Informationsbeschaffung kann sich somit auf unterschiedliche Fragestellungen beziehen. Informationsquellen müssen allerdings in jedem Fall auf ihre Vertrauenswürdigkeit hin analysiert, bewertet und beurteilt werden. Bei Recherchen handelt es sich in der Regel um die am wenigsten invasivste Art von Prüfschritten. Die Durchführung dürfte somit in der Regel vertretbar sein.

Eingaben zu konkreten Websites können aus unterschiedlichen Gründen bei mir eingehen. Beispiele hierfür sind Beschwerden über

– die Ausgestaltung von Cookie-Bannern,
– die rechtswidrige Veröffentlichung personenbezogener Daten,
– die rechtswidrige Nutzung personenbezogener Daten für den Versand von Werbung,
– nicht funktionierende Abmeldeverfahren von Newslettern oder
– konkrete Schwachstellen in Web-Anwendungen.

Zur Aufklärung der zugrundeliegenden technischen Sachverhalte wird aus dem IT-Laboratorium heraus mit den betroffenen Websites und Web-Anwendungen im Rahmen des vom Betreiber erwartbaren Benutzerverhaltens interagiert. Hierzu zählen, je nach konkretem Gegenstand einer Beschwerde, beispielsweise

– der Aufruf der Website, um ein Cookie-Banner näher zu analysieren oder eine beschwerdegegenständliche Veröffentlichung zu inspizieren,
– die Erstellung eines Benutzerkontos, um einen etwaigen rechtswidrigen Werbe-E-Mail-Versand zu bestätigen,

– die Registrierung und nachfolgende De-Registrierung für einen Newsletter, um das Funktionieren der entsprechenden Funktionalitäten zu prüfen, oder
– das manuelle Nachvollziehen des in einer Beschwerde beschriebenen Vorgehens, um das Vorliegen einer Schwachstelle zu verifizieren.

Diese Prüfschritte sind in der Regel vertretbar, da sie alle auf Basis der vom Betreiber vorgesehenen und bereitgestellten Funktionen durchgeführt werden. Besondere Sorgfalt ist aber insbesondere beim letzten Prüfschritt geboten. Hier gilt es, etwaige unerwartete Seiteneffekte und hiermit verbundene Schadenswirkungen zu vermeiden.

Eine weitere Gruppe von Prüfschritten im Rahmen von technischen Datenschutzüberprüfungen beziehen sich auf mobile Applikationen (Apps). Hierbei kann grob zwischen statischer und dynamischer Analyse unterschieden werden. Bei einer statischen Analyse werden die Bausteine der zu prüfenden App analysiert, etwa hinsichtlich der Einbindung sogenannter Tracker oder des Vorhandenseins sicherheitskritischer Informationen im Quellcode. Hierzu ist eine Ausführung der geprüften App nicht erforderlich. Daher nehmen diese Prüfschritte auch eine besondere Rolle ein, denn eine Interaktion mit IT-Systemen und -Diensten von Verantwortlichen und Auftragsverarbeitern findet nicht statt. Dynamische Analysen kommen zum Einsatz, wenn das Verhalten einer App im Rahmen der Nutzung Gegenstand eines oder mehrerer Prüfschritte ist. Diesen Prüfschritten können unterschiedliche Fragestellungen zugrunde liegen, etwa in Hinblick auf die tatsächliche Übermittlung personenbezogener Daten an unterschiedliche Akteure. Derartige Prüfschritte dürften vertretbar sein. Es ist jedoch besondere Sorgfalt geboten, falls Apps im IT-Laboratorium zur Herstellung der Prüfbarkeit manipuliert werden mussten. Hier gilt es ebenfalls, unerwünschte Seiteneffekte mit Schadenswirkung zu vermeiden.

Bei der technischen Datenschutzüberprüfung von Websites und bei der dynamischen Analyse von Apps wird in der Regel der Netzwerkverkehr aufgezeichnet. Hierdurch wird zum einen eine vertiefende Analyse der ausgetauschten Daten ermöglicht. Zum anderen erhöht die lückenlose Aufzeichnung des Netzwerkverkehrs in der Regel die Beweiskraft der Ergebnisse einer technischen Datenschutzüberprüfung. Häufig kommt im Rahmen der Netzwerkkommunikation eine Verschlüsselung zum Einsatz. Diese muss zusätzlich aufgebrochen werden, um Zugriff auf die unverschlüsselten Daten zu erhalten. Sowohl die Aufzeichnung des Netzwerkverkehrs als auch das Aufbrechen der Verschlüsselung sind in der Regel vertretbare Prüfschritte. Dies gilt insbesondere, wenn beide Prüfschritte passiv erfolgen und keine Manipulation der ausgetauschten Daten durchgeführt wird.

Auch die Analyse von über das Internet zugreifbaren IT-Systemen hinsichtlich offener Netzwerk-Ports oder unterstützter Verschlüsselungsverfahren dürften

vertretbar und verhältnismäßig sein. Schließlich müssen Verantwortliche und Auftragsverarbeiter damit rechnen, dass derartige Analysen im Internet regelmäßig von unterschiedlichen Akteuren durchgeführt werden. Sie gehören somit ebenfalls zu den erwartbaren Interaktionsmustern.

Fazit

Eine grundlegende Aufgabe meiner Behörde ist gemäß Art. 57 Abs. 1 Buchst. a DS-GVO die Überwachung und Durchsetzung der Vorschriften des Datenschutzrechts. Zu diesem Zweck verfügt meine Behörde gemäß Art. 58 Abs. 1 Buchst. b DS-GVO über die Untersuchungsbefugnis, Datenschutzüberprüfungen durchzuführen. Hierzu zählen insbesondere auch technische Datenschutzüberprüfungen. Als Voraussetzung für deren Durchführung verfügt meine Behörde über ein entsprechend ausgestattetes IT-Laboratorium.

Technische Datenschutzüberprüfungen müssen immer gemäß den allgemeinen Grundsätzen des behördlichen Handelns im Rechtsstaat durchgeführt werden. Im Rahmen der Durchführung werden in der Regel rechtlich geschützte Interessen von Verantwortlichen und Auftragsverarbeitern berührt. Daher müssen bei der Konzeption und Planung einer technischen Datenschutzüberprüfung im Rahmen des pflichtgemäßen Ermessens unterschiedliche Einflussfaktoren angemessen berücksichtigt, Interessen abgewogen sowie die Vertretbarkeit und Verhältnismäßigkeit des Mitteleinsatzes gewährleistet werden.

Technische Datenschutzüberprüfungen werden häufig im Rahmen von Vorermittlungen oder als Teil von Verwaltungsverfahren durchgeführt. Spätestens wenn Prüfergebnisse als Grundlage für den Erlass von Verwaltungsakten verwendet werden sollen, muss betroffenen Verantwortlichen und Auftragsverarbeitern die Möglichkeit zur Stellungnahme eingeräumt werden. Hierzu ist ihnen auch Einblick in die Prüfergebnisse zu gewähren. Hierbei sind ihre Beweiseignung und ihre Dokumentation von besonderer Bedeutung.

17.2
Meldungen von Datenschutzverletzungen

Die Zahl der Meldungen von Datenschutzverletzungen blieb im Berichtsjahr auf einem hohen Niveau. Anlässlich der zugenommen Cyberangriffe auf Dienstleister rückten die Rolle und die Pflichten der für verantwortliche Stellen tätigen Auftragsverarbeiter verstärkt in den Fokus.

Überblick und Entwicklungen

Nachdem im Jahr 2021 mit insgesamt 2.016 Meldungen ein Rekordhoch in Bezug auf Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO, § 65 BDSG in Verbindung mit § 500 StPO und § 60 HDSIG zu verzeichnen war, ging die Anzahl der im Jahr 2022 eingereichten Meldungen etwas (ca. 13 %) zurück. Mit 1.754 Meldungen blieb die Zahl der gemeldeten Datenschutzvorfälle jedoch auch im Berichtsjahr auf einem hohen Level. Die Bearbeitung von Datenpannenmeldungen stellte damit weiterhin einen großen Teil der täglichen Arbeit meiner Behörde dar.

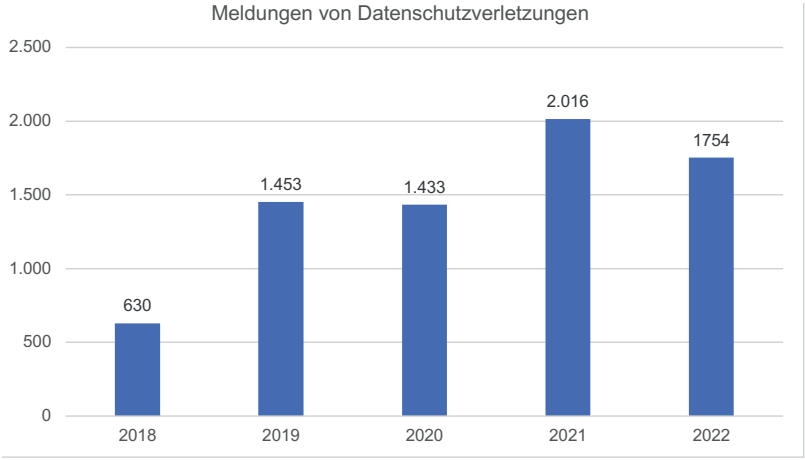

Abbildung: Entwicklung der Anzahl der Meldungen von Datenschutzverletzungen beim HBDI seit Wirksamwerden der DS-GVO

Die Palette der gemeldeten Datenschutzvorfälle war insgesamt sehr bunt. Das Ranking der am häufigsten gemeldeten Verletzungen führten, wie auch in den letzten Jahren, wiederholt die Vorfälle im Zusammenhang mit fehlerhaftem Versand und falscher Zuordnung von Daten sowie Cyberkriminalität an. Die meisten Meldungen erreichten meine Behörde aus dem Wirtschaftssektor einschließlich Kreditwirtschaft, Inkasso, Dienstleister, Handel und Gewerbe. Darüber hinaus waren die Bereiche Beschäftigtendatenschutz sowie Gesundheit und Pflege stark betroffen.

Meldungen im Zusammenhang mit der Corona-Pandemie

Insbesondere im Gesundheitssektor gingen im Berichtsjahr diverse Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit der Corona-Pandemie ein. Bei einem Großteil davon handelte es sich um Fehlübermittlungen von positiven Testergebnissen durch die Teststellen sowie Fehlversand entsprechender Informationen bei einer festgestellten Corona-Infektion durch die Gesundheitsämter. Die Ursachen lagen in diesen Fällen hauptsächlich in individuellen Fehlern von Mitarbeitenden und waren unter anderem auf das akut erhöhte Infektionsgeschehen und die damit verbundene Arbeitsüberlastung zurückzuführen.

In einem Fall brachte mir eine Wiesbadener Arztpraxis zur Kenntnis, dass eine Mitarbeiterin mutmaßlich zahlreiche gefälschte Covid-19-Impfzertifikate ausgestellt hatte. Die Meldung ging auf einen Hinweis der Kriminalpolizei zurück, die in dem Fall umfangreich ermittelte. Um den weiteren Missbrauch zu unterbinden, reagierte die verantwortliche Stelle umgehend mit der Freistellung der Beschäftigten sowie weiteren Maßnahmen, wie Änderung der Passwörter und erneuter Sensibilisierung aller Mitarbeitenden.

In einem weiteren Fall meldete ein Krankenhaus, dass im Rahmen von Zugangskontrollen von Patienten und Besuchern statt eines Scans und der Überprüfung die vorgelegten Corona-Impfzertifikate und Ausweisdokumente mittels dienstlicher Smartphones abfotografiert worden waren. Nach Kenntnis der Datenschutzverletzung wurden die erhobenen Daten gelöscht und das Verfahren zur Durchführung der Zugangskontrollen unverzüglich umgestellt.

Meldungen im Zusammenhang mit dem Zensus 2022

Darüber hinaus erreichten mich im Berichtszeitraum einzelne Meldungen von Datenschutzverletzungen, die sich im Kontext des Zensus 2022 ereigneten.

So meldete zum Beispiel eine hessische Stadt den Verlust von umfangreichen Zensusunterlagen durch eine Erhebungsbeauftragte. Betroffenen waren die Bewohner eines Mehrfamilienhauses. Die verantwortliche Stelle reagierte mit entsprechenden Maßnahmen wie der zusätzlichen Sensibilisierung der Mitarbeitenden und der Erhebungsbeauftragten und der Information gegenüber den Betroffenen nach Art. 34 DS-GVO. Von Seiten meiner Behörde wurde der Stadt im Rahmen der umfassenden Beratung darüber hinaus empfohlen, gegebenenfalls erhöhte Kontrollen durchzuführen.

In einer anderen Stadt wurden die im Rahmen der Zensusdurchführung erhobenen Daten einer Person missbräuchlich zu privaten Zwecken verwendet. Dabei kontaktierte der Erhebungsbeauftragte im Nachgang des stattgefundenen Gesprächs eine auskunftspflichtige Bürgerin per Telefon und sendete ihr

dabei anzügliche Nachrichten. Anlässlich des geschilderten Vorfalls trennte sich die Stadt mit sofortiger Wirkung von diesem Erhebungsbeauftragten.

Insgesamt kann in diesem Bereich eine positive Bilanz gezogen werden. Im Verhältnis zu den Datenmengen, die im Zusammenhang mit der Volkszählung erhoben und verarbeitet werden, wurden nur sehr wenige Einzelfälle als Datenschutzverletzungen gemeldet. Ich gehe daher davon aus, dass sich diesbezüglich der weit überwiegende Teil der Verantwortlichen und der Erhebungsbeauftragten datenschutzkonform verhielt (s. hierzu auch Kap. 9).

Hackerangriffe

Cyberkriminalität war auch im Jahr 2022 ein Dauerbrenner bei den Datenschutzverletzungen. Insbesondere hervorzuheben ist eine neue, mit einer großen Gefahr einhergehende Entwicklung, die im Berichtszeitraum beobachtet werden konnte. Immer häufiger werden Dienstleister aus verschiedenen Bereichen von Hackern angegriffen. So wurden im Berichtsjahr mehrere hessische Dienstleister Opfer von intensiven Cyberattacken. Darüber hinaus waren zahlreiche in Hessen ansässige verantwortliche Stellen durch Hackerangriffe auf Dienstleister aus anderen Bundesländern beeinträchtigt. Insgesamt waren sowohl Unternehmen als auch öffentliche Einrichtungen, unter anderem auch kritische Infrastrukturen und Unternehmen der Daseinsvorsorge, von solchen Angriffen betroffen. Bei Attacken auf IT-Dienstleister mit Tätigkeitsschwerpunkten in der Personal- und/oder Altersversorgungsverwaltung waren erhebliche Datenmengen von Beschäftigten betroffen.

Mit dieser dynamischen Entwicklung nimmt die Problematik der Cyberkriminalität insgesamt neue Dimensionen an. Erfolgreiche Cyberangriffe auf Dienstleister, die in der Regel im Auftrag mehrerer Verantwortlicher erhebliche Datenmengen verarbeiten, erreichen zwangsläufig ein großes Ausmaß und verursachen gravierende bereichs- und branchenübergreifende Schäden. Insbesondere Störungen im Betrieb von kritischen Dienstleistungen könnten die Versorgungssicherheit der Bürgerinnen und Bürger bemerkbar gefährden.

Darüber hinaus stellen Angriffe auf Dienstleister aufgrund ihrer Komplexität alle Beteiligten vor besondere Herausforderungen bei der Bewältigung und Aufarbeitung der Vorfälle. Unter anderem muss aufwendig identifiziert werden, welche Daten welcher Verantwortlichen in welchem Umfang betroffen sind. Die beschriebene Entwicklung spiegelte sich auch im Rahmen der Zusammenarbeit der deutschen Datenschutzaufsichtsbehörden wider. So mussten im Berichtsjahr in mehreren Fällen die Fragen der Zuständigkeit sowie des Informationsflusses gemeinsam geklärt werden. Darüber hinaus erforderten die Ereignisse einen ständigen Austausch bei der Aufklärung

und der Bewertung der Fälle. Dies gestaltete sich im Berichtsjahr in allen Fällen einwandfrei, zielgerichtet und konstruktiv.

Die Rolle und die Pflichten der Auftragsverarbeiter

Anlässlich des beschriebenen Anstiegs der Cyberangriffe auf Dienstleister aus verschiedenen Bereichen im vergangenen Jahr ist es mir ein großes Anliegen, nochmals auf die Wichtigkeit der datenschutzkonformen Gestaltung der Auftragsverarbeitung und der gelungenen Zusammenarbeit zwischen den verantwortlichen Stellen und den Auftragsverarbeitern hinzuweisen.

Auftragsverarbeiter sind wichtige Akteure, die im Zusammenhang mit Datenschutzvorfällen eine entscheidende Rolle spielen können. Eine erfolgreiche Umsetzung der Pflichten und der effektive Schutz vor Hackerangriffen kann nur gelingen, wenn verantwortliche Stellen, Auftragsverarbeiter, zuständige Datenschutzaufsichts- sowie andere betroffene Behörden kooperativ zusammenarbeiten (s. auch Kap. 17.3).

Liegt eine Auftragsverarbeitung gemäß Art. 28 DS-GVO vor, müssen auch im Kontext der möglichen Datenschutzverletzungen zusätzliche Regelungen berücksichtigt werden. Unter anderem unterstützt der Auftragsverarbeiter gem. Art. 28 Abs. 3 Buchst. f DS-GVO den Verantwortlichen bei der Erfüllung seiner Melde- und Benachrichtigungspflichten.

Art. 28 DS-GVO

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter (…)

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt; (…)

Diese Vorschrift wird in Art. 33 Abs. 2 DS-GVO konkretisiert. Danach ist der Auftragsverarbeiter verpflichtet, den Verantwortlichen unverzüglich zu informieren, sofern ihm eine Datenschutzverletzung bekannt wird.

Art. 33 DS-GVO

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich. (…)

Dies bedeutet insbesondere, dass der Auftragsverarbeiter seinen Auftraggeber über jede Verletzung des Schutzes personenbezogener Daten im Sinn von Art. 4 Nr. 12 DS-GVO unverzüglich – also ohne schuldhaftes Zögern im Sinne von § 121 BGB – informieren muss. Eine eigene Risikoanalyse führt er dabei nicht durch. Das bedeutet, selbst wenn eine Datenschutzverletzung kein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt, ist diese dem Verantwortlichen in jedem Fall zur Kenntnis zu bringen. Es obliegt dann dem Verantwortlichen, mit Unterstützung des Dienstleisters eine Risikobewertung durchzuführen und anschließend zu entscheiden, ob eine Meldung an die Aufsichtsbehörde und eine Benachrichtigung von betroffenen Personen erforderlich sind. Ich empfehle den Auftragsverarbeitern, sofern unklar ist, welche Daten von der Verletzung betroffen sind, vorsorglich alle Kunden zu unterrichten, in deren Auftrag sie tätig sind. Die jeweiligen Verantwortlichen entscheiden anschließend unter Berücksichtigung aller Umstände des jeweiligen Falles über die weitere Vorgehensweise.

In diesem Kontext rege ich an, dass bereits im Rahmen der Ausgestaltung einer Vereinbarung über die Auftragsverarbeitung klare Regelungen für den Fall eines möglichen Datenschutzvorfalls getroffen werden. Diese sollen u. a. den gesamten Meldeprozess nebst den zuständigen Ansprechpartnern und Abwesenheitsvertretern sowie den Umfang der seitens des Dienstleisters mitzuteilenden Informationen beinhalten (z. B. detaillierte Sachverhaltsschilderung, zeitlicher Ablauf, Anzahl und Kategorien von betroffenen personenbezogenen Daten und Personen, die vom Auftragsverarbeiter ergriffenen Maßnahmen zur Eindämmung der Datenschutzverletzung sowie alle weiteren Umstände, die im Einzelfall von Bedeutung sein könnten) (s. auch Kap. 17.3).

Den Auftragsverarbeiter trifft keine eigene Meldepflicht aus Art. 33 DS-GVO gegenüber der Aufsichtsbehörde. Unabhängig hiervon kann jedoch der Verantwortliche den Auftragsverarbeiter bevollmächtigen, für ihn eine Meldung an die Datenschutzaufsichtsbehörde zu erstatten. In diesem Fall muss die Meldung alle erforderlichen Informationen gemäß den Vorgaben des Art. 33 DS-GVO umfassen. Ungeachtet dessen kann vereinzelt eine zusätzliche Meldung durch den Auftragsverarbeiter an die für ihn zuständige Aufsichtsbehörde – zum Beispiel aus Gründen der Transparenz oder bei Beratungsbedarf – sinnvoll sein. Eine solche Meldung ist in jedem Fall dann angezeigt, wenn auch eigene Daten des Dienstleisters, wie zum Beispiel

Beschäftigtendaten, betroffen sind, für die er als datenschutzrechtlicher Verantwortlicher und nicht als Auftragsverarbeiter fungiert.

Da der Verantwortliche generell die Sicherheit der ihm anvertrauten Daten gewährleisten muss, ist er nach Art. 28 Abs. 1 DS-GVO verpflichtet, im Falle einer Auftragsverarbeitung mit der nötigen Sorgfalt einen zuverlässigen Dienstleister auszuwählen. Diese Pflicht endet nicht mit der Erteilung des Auftrags, sondern erstreckt sich auf die gesamte Dauer der Vertragsbeziehung. Auch im Zusammenhang mit Datenschutzvorfällen beim Auftragsverarbeiter obliegt es dem Verantwortlichen, kontinuierlich zu überprüfen, ob der Dienstleister die gebotenen Anforderungen erfüllt. Dabei ist im Nachgang eines Vorfalls unter anderem durch den Verantwortlichen zu überprüfen, ob die technischen und organisatorischen Maßnahmen des Auftragsverarbeiters den aktuellen Standards entsprechen und im gebotenen Umfang angepasst wurden. Darüber hinaus untersucht der Verantwortliche, ob seitens des Dienstleisters ausreichende Maßnahmen eingeleitet wurden, um die Wiederholung eines Vorfalls zu verhindern oder zu minimieren.

Der Auftragsverarbeiter muss seinerseits jederzeit hinreichende Garantien im Hinblick auf geeignete technische und organisatorische Maßnahmen bieten. Dies gilt umso mehr vor dem Hintergrund, dass bei Datenschutzverstößen Auftragsverarbeiter neben den Verantwortlichen haftbar gemacht werden können. Darüber hinaus können sich auch datenschutzrechtliche Aufsichtsmaßnahmen gemäß Art. 58 DS-GVO an Auftragsverarbeiter richten. Im Falle von Verstößen sind weitreichende Sanktionen sowohl gegenüber Auftragsverarbeitern als auch gegenüber Verantwortlichen möglich. Im Berichtsjahr wurden durch meine Behörde keine Maßnahmen im Sinn von Art. 58 Abs. 2 DS-GVO gegen Auftragsverarbeiter ergriffen.

Fazit und Empfehlung

Trotz der hohen Anzahl an gemeldeten Datenschutzverletzungen musste ich im Berichtszeitraum lediglich bei wenigen Fallkonstellationen von meinen Abhilfebefugnissen im Sinn von Art. 58 Abs. 2 DS-GVO Gebrauch machen. In den meisten Fällen verfuhren verantwortliche Stellen und Auftragsverarbeiter im Umgang mit und bei der Bewältigung von Datenschutzvorfällen entsprechend der datenschutzrechtlichen Anforderungen. Im Berichtsjahr habe ich einzelne Unternehmen wegen einer nicht oder nicht fristgerecht gemeldeten Datenschutzverletzung gemäß Art. 58 Abs. 2 Buchst. b DS-GVO verwarnt. Ein Unternehmen wurde gemäß Art. 58 Abs. 2 Buchst. e DS-GVO zur Benachrichtigung von betroffenen Personen nach einem Hackerangriff angewiesen. Gegen ein weiteres Unternehmen wurde gemäß Art. 58 Abs. 2 Buchst. i DS-GVO eine Geldbuße wegen unterbliebener Dokumentation der

Datenschutzverletzung gemäß Art. 33 Abs. 5 DS-GVO verhängt. Darüber hinaus war es erforderlich, gegenüber einer hessischen Stadt nach einem Datenschutzereignis mit umfangreichen schützenswerten Daten eine förmliche Anweisung mit dem Ziel der Unterrichtung von betroffenen Personen zu erlassen.

Bei einer Vielzahl von gemeldeten Datenschutzverletzungen können die Ereignisse letztendlich auf einen menschlichen Fehler zurückgeführt werden. Dies gilt für den klassischen Fehlversand und den offenen E-Mail-Verteiler, aber auch für die illegalen Phishing-Attacken sowie andere Formen der Cyberkriminalität. Auch wenn solche Datenschutzverletzungen sich nicht vollkommen vermeiden lassen, appelliere ich an alle datenverarbeitenden Stellen, in diesem Bereich noch stärker präventiv tätig zu werden und vor allem durch entsprechende Schulungen ihre Mitarbeitenden zu sensibilisieren. Neben den weiteren technischen und organisatorischen Maßnahmen können ein versierter und sicherer Umgang mit der Technik sowie ein geschärftes Bewusstsein im Umgang mit den Fragen der IT-Sicherheit dazu beitragen, dass diverse Verdachtsmomente und Unregelmäßigkeiten besser wahrgenommen und entsprechend identifiziert sowie jegliche Angriffsversuche frühzeitig unterbunden werden und Hackern somit keine Chance für ihr kriminelles Handeln gegeben wird.

17.3
Datenschutzverletzungen bei Auftragsverarbeitern

Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO bei Auftragsverarbeitern stellen für Verantwortliche eine Herausforderung dar. Defizite bei der Abstimmung und Bereitstellung relevanter Informationen zwischen Auftragsverarbeitern und Verantwortlichen führen häufig zu vermeidbaren Verzögerungen im Ablauf der gemeinsamen Behandlung von Datenschutzverletzungen und damit letztlich auch zu einer verspäteten Benachrichtigung der betroffenen Personen. Dieser Beitrag skizziert auf Basis der Anforderungen der Art. 33 und 34 DS-GVO den Ablauf der Behandlung von Verletzungen des Schutzes personenbezogener Daten anhand eines idealtypischen Szenarios eines Ransomware-Angriffs auf einen Auftragsverarbeiter. Anschließend werden typische Problemfelder aus der aufsichtsbehördlichen Praxis umrissen, die im Berichtszeitraum zu Verzögerungen und Defiziten in der Vorfallbehandlung führten. Daraus werden Erwartungen an Verantwortliche und Auftragsverarbeiter hinsichtlich der Umsetzung übergreifender Prozesse zum angemessenen Umgang mit Datenschutzverletzungen abgeleitet.

Notwendiges Zusammenwirken von Verantwortlichen und Auftragnehmern

Kommt es zu Verletzungen des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12 DS-GVO bei Auftragsverarbeitern gemäß Art. 4 Nr. 8 DS-GVO, dann sind häufig auch Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO hiervon betroffen, die personenbezogene Daten durch die Auftragsverarbeiter verarbeiten lassen. Dementsprechend besteht für diese Verantwortlichen auch die Pflicht, Verletzungen des Schutzes personenbezogener Daten nach Art. 33 Abs. 1 DS-GVO an die zuständige Datenschutzaufsichtsbehörde zu melden. Dies gilt, sofern durch den Vorfall voraussichtlich mindestens ein Risiko für Rechte und Freiheiten der betroffenen Personen entstanden ist. Damit Verantwortliche dieser Verpflichtung nachkommen können, muss der Auftragsverarbeiter seinerseits seiner Verpflichtung gemäß Art. 33 Abs. 2 DS-GVO nachkommen und den Verantwortlichen den Vorfall unverzüglich melden (s. auch Kap. 17.2). Mit steigender Anzahl beteiligter Stellen steigt auch die Wahrscheinlichkeit, dass es in der Abstimmung zwischen Auftragsverarbeitern und Verantwortlichen zu Problemen und vermeidbaren Verzögerungen kommt. Im Berichtszeitraum wurde mir eine signifikante Anzahl von Verletzungen des Schutzes personenbezogener Daten gemeldet, bei denen es in dieser Konstellation tatsächlich auch zu nicht unerheblichen Verzögerungen in der Behandlung der Vorfälle kam. Auch musste ich in mehreren Fällen Defizite in der Informationsbereitstellung feststellen. Dies galt sowohl für Auftragsverarbeiter gegenüber den Verantwortlichen als auch von diesen gegenüber den betroffenen Personen und gegenüber meiner Behörde. Immer wieder gab es auch Fälle, bei denen Verantwortliche Vorfälle unzureichend behandelt haben und damit ihren datenschutzrechtlichen Verpflichtungen nur auf Drängen meiner Behörde in ausreichendem Maße nachgekommen sind. Vor allem bei Datenschutzverletzungen, bei denen es zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen kommt, sind schnelle Reaktionen und eine angemessene Bereitstellung von relevanten Informationen von besonderer Bedeutung. Dies ist insbesondere notwendig, um die negativen Auswirkungen des Vorfalls zu mindern und betroffenen Personen ihrerseits die Möglichkeit zu bieten, angemessen auf den Vorfall zu reagieren.

Im Folgenden werden zunächst die gesetzlichen Anforderungen der Art. 33 und 34 DS-GVO an Auftragsverarbeiter und Verantwortliche im Zusammenhang mit Verletzungen des Schutzes personenbezogener Daten zusammengefasst. Danach wird ein idealtypischer Ablauf der gemeinsamen Behandlung von Verletzungen des Schutzes personenbezogener Daten durch einen Auftragsverarbeiter und mehrere Verantwortliche skizziert. Hierzu wird ein exemplarisches Szenario eines erfolgreichen Ransomware-

Angriffs auf einen Auftragsverarbeiter verwendet, bei dem alle Beteiligten angemessen reagieren und ihren datenschutzrechtlichen Verpflichtungen bei der Bewältigung des Vorfalls gerecht werden. Danach wird anhand dieses Ablaufs erläutert, wo im Berichtszeitraum typischerweise Probleme oder Verzögerungen entstanden sind.

Datenschutzrechtliche Anforderungen der DS-GVO

Die Verantwortlichen und Auftragsverarbeitern im Rahmen von Verletzungen des Schutzes personenbezogener Daten obliegenden Pflichten sowie die hierbei einzuhaltenden Fristen sind in Art. 33 und 34 DS-GVO geregelt. In Art. 5 Abs. 2 DS-GVO ist festgelegt, dass Verantwortliche für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich sind und deren Einhaltung nachweisen können müssen. Nach Art. 12 DS-GVO sind die Verantwortlichen auch die Schnittstelle für die betroffenen Personen und dafür verantwortlich, diesen die Ausübung ihrer Rechte zu ermöglichen. Die grundlegenden Anforderungen an die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter sind in Art. 28 DS-GVO festgelegt. Die Verarbeitung durch einen Auftragsverarbeiter ist in einem Auftragsverarbeitungsvertrag (AVV) zu regeln, der den Anforderungen des Art. 28 Abs. 3 DS-GVO genügt. Spezifisch ist darin nach Art. 28 Abs. 3 Buchst. f DS-GVO vorzusehen, dass der Auftragsverarbeiter

Art. 28 Abs. 3 Buchst. f DS-GVO

(3) (…)

f) unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Artikeln 32 bis 36 genannten Pflichten unterstützt; (…).

Dies umfasst somit auch die in den Art. 33 und 34 DS-GVO geregelten Pflichten. In Art. 33 DS-GVO sind diese wie folgt definiert:

Art. 33 DS-GVO

(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

d) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen.

Damit ein Verantwortlicher seinen Pflichten nachkommen kann, sind Auftragsverarbeiter nach Art. 33 Abs. 2 DS-GVO in jedem Fall verpflichtet, dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten unverzüglich zu melden. In Verbindung mit Art. 28 Abs. 3 Buchst. f DS-GVO muss der Auftragsverarbeiter einem Verantwortlichen dabei diejenigen Informationen bereitstellen, die dieser benötigt, um seinen Pflichten nachkommen zu können.

Alle Verletzungen des Schutzes personenbezogener Daten sind nach Art. 33 Abs. 5 DS-GVO unabhängig vom Risiko durch den Verantwortlichen zu dokumentieren. Nach Art. 33 Abs. 1 DS-GVO muss ein Verantwortlicher mit Sitz in Hessen Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden an meine Behörde melden, sofern die Datenschutzverletzung voraussichtlich mindestens zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Nach dem Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten liegen jedoch nicht immer unmittelbar alle relevanten Informationen vor. In diesem Fall hat eine erste, gegebenenfalls unvollständige Vorabmeldung binnen 72 Stunden zu erfolgen, sofern die Bedingungen des Art. 33 Abs. 1 DS-GVO erfüllt sind. Nach Art. 33 Abs. 4 DS-GVO sind Nachmeldungen an

meine Behörde möglich. Diese müssen jedoch ohne unangemessene weitere Verzögerung erfolgen (s. hierzu auch 50. Tätigkeitsbericht, Kap. 18.1).

Sollte durch Verletzungen des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen entstehen, so hat ein Verantwortlicher diese nach Art. 34 Abs. 1 DS-GVO unverzüglich zu benachrichtigen. Die den betroffenen Personen mindestens bereitzustellenden Informationen sind in Art. 34 Abs. 2 DS-GVO festgelegt. Auch bei der Erfüllung dieser Pflicht des Verantwortlichen hat der Auftragsverarbeiter diesen gemäß Art. 28 Abs. 3 Buchst. f DS-GVO zu unterstützen.

Szenario für Datenschutzverletzungen durch einen Ransomware-Angriff

Der Ablauf der Behandlung einer Verletzung des Schutzes personenbezogener Daten, der die hier thematisierten datenschutzrechtlichen Anforderungen erfüllt, wird im Folgenden anhand eines Szenarios für einen Ransomware-Angriff exemplarisch dargestellt. Den üblichen Ablauf von Ransomware-Angriffen habe ich bereits in meinem 50. Tätigkeitsbericht für das Jahr 2020 in Kap. 18.2 skizziert.

Für das hier betrachtete Szenario wird von einem mittelständischen Auftragsverarbeiter ausgegangen, der Verantwortlichen eine Reihe von Dienstleistungen anbietet. Zur Erbringung und zur vertraglichen Abwicklung dieser Dienstleistungen verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag der Verantwortlichen. Darüber hinaus verarbeitet er auch personenbezogene Daten in eigener Verantwortung, z. B. Beschäftigtendaten der eigenen Angestellten. Die Verarbeitung der personenbezogenen Daten erfolgt auf verschiedenen IT-Systemen des Auftragsverarbeiters.

Ein Ransomware-Angriff könnte in diesem Szenario wie folgt ablaufen: An einem Freitagnachmittag stellen Beschäftigte des Auftragsverarbeiters fest, dass es bei IT-Systemen und -Diensten vermehrt zu Fehlverhalten kommt und diese sukzessive ausfallen. Parallel melden sich Kunden, die sich beschweren, dass IT-Dienste nicht mehr erreichbar sind. Die eingeschaltete IT-Administration stellt fest, dass ein Ransomware-Angriff stattfindet. Die zuständigen Beschäftigten informieren weitere Kolleginnen und Kollegen und führen erste Maßnahmen durch, die für einen solchen Fall im erprobten Notfallplan festgelegt sind. Dazu gehört auch die frühzeitige Einbindung des betrieblichen Datenschutzbeauftragten.

Auf konkrete technische und organisatorische Maßnahmen wird im Folgenden nicht näher eingegangen, da diese im Rahmen dieser Darstellung nicht relevant

sind. Anhaltspunkte und weiterführende Informationen im Zusammenhang mit der Informationssicherheit lassen sich beispielsweise im Arbeitspapier des BSI „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“ finden (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf).

In dem hier betrachteten Szenario stellt der Auftragsverarbeiter in einer ersten Bilanz fest, dass eine große Anzahl von Daten verschlüsselt wurden – darunter auch Datenbanken und Inhalte von Netzlaufwerken mit Daten von Kunden. Auch wurde das Online-Backup verschlüsselt und damit unbrauchbar gemacht (s. auch Kap. 17.7). Der Auftragsverarbeiter informiert gemäß Art. 33 Abs. 2 DS-GVO unverzüglich seine Kunden in ihrer Rolle als Verantwortliche über den Vorfall und fasst dazu den aktuellen Sachstand zusammen. Die übermittelten Informationen ermöglichen den Verantwortlichen eine Einschätzung des Ausmaßes und der möglichen Auswirkungen des Vorfalls sowie eine eigene Risikobewertung. Weiterhin meldet der Auftragsverarbeiter die Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 1 DS-GVO innerhalb von 72 Stunden in seiner Rolle als Verantwortlicher an die für ihn zuständige Datenschutzaufsichtsbehörde, da auch eigene Beschäftigte vom Vorfall betroffen sind und von einem Risiko für deren Rechte und Freiheiten ausgegangen werden muss.

Auch wenn es zu diesem frühen Zeitpunkt noch nicht möglich ist, den Sachverhalt abschließend zu erfassen, ist die erste unverzügliche Benachrichtigung der Verantwortlichen erforderlich. Nur so haben diese die Möglichkeit, ihrerseits zu reagieren und ggf. notwendige technische und organisatorische Maßnahmen zu ergreifen. Die Verantwortlichen führen daraufhin entsprechend dem mitgeteilten Sachstand eine erste Risikobewertung durch (DSK, Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-08/kp_18_risiko.pdf). Zu den von den Verantwortlichen ergriffenen Maßnahmen gehört beispielsweise die Trennung etwaiger Verbindungen zu IT-Systemen und -Diensten des Auftragsverarbeiters. Da die genutzten IT-Dienste des Auftragsverarbeiters und die dort verarbeiteten Daten daraufhin nicht mehr verfügbar sind, werden entsprechende Notfallpläne umgesetzt. Falls die Verantwortlichen aufgrund der Risikobewertung zu dem Schluss kommen, dass die Verletzungen des Schutzes personenbezogener Daten voraussichtlich mindestens zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führen, melden sie die Datenschutzverletzungen ihrerseits gemäß Art. 33 Abs. 1 DS-GVO unverzüglich und binnen 72 Stunden jeweils ihren zuständigen Datenschutzaufsichtsbehörden. Darin beschreiben sie den Vorfall nachvollziehbar und geben auch den Auftragsverarbeiter an, damit die Meldungen unterschiedlicher Verantwortlicher demselben Vorfall zuge-

ordnet werden können. In diesem Szenario handelt es sich dabei um eine erste, vorläufige Meldung, die bei neuen Erkenntnissen oder geänderten Risikobewertungen ohne unangemessene weitere Verzögerungen durch Nachmeldungen ergänzt werden. Dies teilen sie der jeweiligen Aufsichtsbehörde in ihrer ersten Meldung mittels eines entsprechenden Hinweises mit. In Fällen, in denen die erste Risikobewertung der Verantwortlichen zu dem Ergebnis kommt, dass die Verletzung des Schutzes personenbezogener Daten ein hohes Risiko für die Rechte und Freiheiten betroffener Personen zur Folge hat, benachrichtigen sie diese gemäß Art. 34 DS-GVO unverzüglich. Für weitere Informationen zu der Meldung von Verletzungen des Schutzes personenbezogener Daten sei auf die Leitlinie 2016/679 des EDSA (WP250rev.01 – Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, Stand: 6. Februar 2018, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/wp250rev01_de.pdf) und die Beispiele für die Meldung von Verletzungen des Schutzes personenbezogener Daten in der Leitlinie 01/2021 (EDSA, Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Version: 2.0, Stand: 14. Dezember 2021, https://edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_de.pdf) verwiesen.

Im Rahmen des Szenarios ist der Auftragsverarbeiter weiter mit der Bewältigung des Ransomware-Angriffs beschäftigt. Für die Untersuchung des Vorfalls wird ein spezialisierter IT-Forensik-Dienstleister beauftragt. Dieser wird auch explizit beauftragt festzustellen, auf welche personenbezogenen Daten die Angreifer Zugriff hatten und ob und wenn ja welche Daten durch die Angreifer exfiltriert wurden.

Die Angreifer nehmen nach einiger Zeit Kontakt mit dem Auftragsverarbeiter auf und teilen ihm mit, dass sie in großem Umfang personenbezogene Daten kopiert haben. Sie drohen mit der Veröffentlichung dieser Daten, falls kein Lösegeld gezahlt wird. Der Auftragsverarbeiter folgt den Empfehlungen des BSI und des Bundeskriminalamtes (BKA) und kommt der Forderung nicht nach (Bundesvereinigung der kommunalen Spitzenverbände, BKA und BSI, Umgang mit Lösegeldforderungen bei Angriffen mit Verschlüsselungstrojanern auf Kommunalverwaltungen, Stand: 3. März 2020 https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/EmpfehlungenRansomware.pdf). Die Drohung der Angreifer sowie der Umgang mit dieser sind relevante Informationen, die den Verantwortlichen unverzüglich mitgeteilt werden, damit diese ihrerseits ihre Risikobewertung aktualisieren können. Auch wenn im Rahmen der weiteren Analysen des Vorfalls klar wird, welche Systeme vom Vorfall betroffen waren und welche Daten aus einem vorhandenen Offline-Backup wiederhergestellt werden

können, werden die Verantwortlichen entsprechend informiert. Je nach Betroffenheit und Änderung der Risikobewertung melden die Verantwortlichen wiederum ohne unangemessene weitere Verzögerung den neuen Sachstand zusammengefasst an ihre zuständige Datenschutzaufsichtsbehörde und aktualisieren ihre Dokumentation gemäß Art. 33 Abs. 5 DS-GVO. Weiterhin benachrichtigen die Verantwortlichen betroffene Personen erstmals gemäß Art. 34 DS-GVO, wenn durch die aktualisierte Risikobewertung nunmehr von einem hohen Risiko für deren Rechte und Freiheiten auszugehen ist. Auch bereits benachrichtigte Personen werden erneut informiert, sofern eine aktualisierte Informationslage dies erforderlich macht, etwa aufgrund neu identifizierter Risiken.

Die Angreifer veröffentlichen nach einem Monat einzelne Dokumente aus den exfiltrierten Daten im „Darknet“. Dies dient als Nachweis, dass die Angreifer tatsächlich Daten exfiltriert haben, und soll den Druck auf den Auftragsverarbeiter erhöhen, das geforderte Lösegeld zu zahlen. Wenig später beginnen die Angreifer damit, sukzessive größere Datenmengen zum Download bereitzustellen. Diese bestehen jeweils aus einem Konglomerat an Dokumenten, E-Mail-Archiven und Datenbankauszügen. Während des gesamten Veröffentlichungsprozesses beobachtet der vom Auftragsverarbeiter für diese Zwecke beauftragte IT-Dienstleister die Veröffentlichungsplattform der Angreifer und analysiert die veröffentlichen Daten fortlaufend, insbesondere auch hinsichtlich personenbezogener Daten. Er bereitet die Analyseergebnisse für den Auftragsverarbeiter auf, so dass dieser seinerseits die Verantwortlichen angemessen informieren und die eigene Risikobewertung anpassen kann. Der Auftragsverarbeiter informiert jeweils die Verantwortlichen über den neuen Sachstand, die entsprechend ihrerseits ihre Risikobewertung aktualisieren und im Bedarfsfall aktiv werden.

Nach Abschluss des Vorfalls analysieren der Auftragsverarbeiter und die Verantwortlichen die Ursachen des Vorfalls und überprüfen kritisch die Abläufe und die Zusammenarbeit im Rahmen der Vorfallbewältigung. Im Rahmen von sogenannten „Lessons Learned“ werden die bisher getroffenen technischen und organisatorischen Maßnahmen und Prozesse angepasst.

Dieses Szenario beschreibt einen Ablauf, bei dem alle Beteiligten ihren Verpflichtungen zur Bewältigung der Datenschutzverletzungen umgehend nachkommen. Damit entstehen keine unnötigen Verzögerungen. Hierdurch sind alle Beteiligten zeitnah über den relevanten Sachstand informiert und können entsprechend reagieren. Dies unterstützt die zeitnahe Ergreifung von Maßnahmen durch den Auftragsverarbeiter, die Verantwortlichen und auch die betroffenen Personen zur Behebung oder Abmilderung der möglichen nachteiligen Auswirkungen der Datenschutzverletzungen.

Exemplarische Problemfelder aus der aufsichtsbehördlichen Praxis

Auf Basis der mir im Berichtszeitraum gemeldeten vergleichbaren Verletzungen des Schutzes personenbezogener Daten konnte ich feststellen, dass die Zusammenarbeit zwischen Auftragsverarbeitern und Verantwortlichen während der Behandlung dieser Art von Vorfällen in verschiedenen Bereichen Verbesserungspotenzial besitzt. Im Folgenden werden einige dieser Möglichkeiten zur Verbesserung der Abläufe beschrieben.

Die ersten vermeidbaren Verzögerungen und Defizite entstehen häufig in der initialen Informationsversorgung der Verantwortlichen durch den Auftragsverarbeiter. Die Beendigung eines IT-Sicherheitsvorfalls hatte in der Regel eine hohe Priorität für Auftragsverarbeiter. Die datenschutzrechtlichen Pflichten wurden daher immer wieder nachrangig behandelt. Am Anfang der Behandlung eines Vorfalls war oftmals noch nicht bekannt, was genau geschehen war und welche Ausmaße der Vorfall hatte. Es kam daher vor, dass Auftragsverarbeiter das Informieren der Verantwortlichen vorerst zurückstellten, etwa um die eigenen Kunden nicht unnötig zu beunruhigen. Hierdurch kam es jedoch dazu, dass datenschutzrechtlich Verantwortliche zu spät informiert wurden und ihrerseits nur verspätet reagieren konnten.

Auch unzureichende Vorbereitungen und Notfallplanungen machten sich bei erfolgreichen Ransomware-Angriffen negativ bemerkbar. So gab es beispielsweise Auftragsverarbeiter, die Schwierigkeiten hatten, Verantwortliche zu kontaktieren, da sie den Zugriff auf die Kontaktinformationen der Kunden und ihre Kommunikationsinfrastruktur verloren hatten und für diesen Fall keine Alternativen vorgesehen hatten. Auch gab es vereinzelt Fälle, in denen Auftragsverarbeiter den Verantwortlichen zunächst Informationen bereitstellten, die nicht das tatsächliche Ausmaß des Vorfalls widerspiegelten. Hierdurch wurden Verantwortliche in falscher Sicherheit gewogen.

Wie an dem Szenario gezeigt wurde, kann sich die Informationslage bei komplexen Datenschutzverletzungen wie Ransomware-Angriffen sukzessive ändern. Diese Änderungen waren eine weitere Quelle für Verzögerungen, wenn der Auftragsverarbeiter den neuen Sachstand nicht zeitnah und entsprechend aufbereitet an die Verantwortlichen kommunizierte, etwa im Falle der Ankündigung der Veröffentlichung exfiltrierter Daten. Wenn bei Ransomware-Angriffen die Websites der Angreifer im Darknet nicht aktiv beobachtet wurden, führte dies in der Regel dazu, dass die tatsächliche Veröffentlichung von Daten nicht oder erst verspätet bekannt wurde.

Bei einer Veröffentlichung von Daten müssen diese in der Regel analysiert werden, um darin enthaltende personenbezogene Daten und die betroffenen Personen zu identifizieren. Da veröffentlichte Daten aber durch die Angreifer kompromittiert sein können, beispielsweise mittels der Infektion mit Schad-

programmen, sollten diese Daten nicht ohne entsprechende Vorkehrungen geöffnet oder anderweitig verarbeitet werden. Weiterhin können der Aufwand und damit verbunden die Kosten für eine solche Analyse sehr hoch ausfallen. Wenn der Auftragsverarbeiter und die Verantwortlichen sich nicht auf eine Zuständigkeit für die Analyse einigen können, kann dies große Verzögerungen hervorrufen oder gar dazu führen, dass die Analyse ganz unterbleibt. Weitere Verzögerungen können entstehen, wenn ein Auftragsverarbeiter das endgültige Ergebnis der Analyse der veröffentlichten Daten abwartet, bevor er die Verantwortlichen informiert, dass eine Datenveröffentlichung überhaupt stattgefunden hat.

Auch auf Seiten der Verantwortlichen traten vermeidbare Verzögerungen auf. Wenn aus den ersten Informationen des Auftragsverarbeiters z. B. nicht klar hervorging, ob oder in welchem Umfang ein Verantwortlicher konkret betroffen war, entschlossen sich Verantwortliche teilweise, zunächst weitere Informationen abzuwarten und nicht selbst aktiv zu werden. Es war jedoch die Aufgabe der Verantwortlichen, die bereitgestellten Informationen des Auftragsverarbeiters über die Verletzung des Schutzes personenbezogener Daten auszuwerten und darauf basierend eigene Risikobewertungen vorzunehmen. Im Falle einer unzureichenden Informationsversorgung müssen sie weitere, erforderliche Informationen aktiv einfordern. Selbst wenn am Anfang der Vorfallbewältigung noch wenige Informationen verfügbar sind, kann ein Verantwortlicher eine erste Risikobewertung vornehmen, da ihm zumindest bekannt ist, welche personenbezogenen Daten der Auftragsverarbeiter für ihn verarbeitet. Ein Verantwortlicher muss seine Risikobewertung beim Vorliegen neuer Informationen überprüfen und bei Bedarf anpassen. Bei relevanten Änderungen ist zu prüfen, ob weitere Maßnahmen getroffen werden müssen.

Ein wiederkehrendes Problem im Rahmen der Bearbeitung der mir gemeldeten Verletzungen des Schutzes personenbezogener Daten war, dass Verantwortliche mir diese zwar gemäß Art. 33 Abs. 1 DS-GVO direkt meldeten, mir aber fehlende oder relevante neue Informationen erst auf explizite Rückfragen hin zur Verfügung stellten. Art. 33 Abs. 4 DS-GVO sieht vor, dass Informationen nachgereicht werden können, allerdings soll dies ohne unangemessene weitere Verzögerung geschehen.

Die Bearbeitung der Vorgänge in meiner Behörde wurde teilweise auch dadurch erschwert, dass Verantwortliche jede Mitteilung des Auftragsverarbeiters ohne jede Aufbereitung oder Bewertung an mich weitergeleitet haben. Insbesondere bei Vorfällen mit vielen Verantwortlichen kam es daher vor, dass ich dieselbe E-Mail eines Auftragsverarbeiters mehrfach kommentarlos weitergeleitet bekam. Verantwortliche sollten in einer Nachmeldung die neuen Informationen in einen Kontext zu ihrer Meldung setzen und insbesondere auf

Änderungen in Bezug auf ihre Risikobewertung, auf getroffene technische und organisatorische Maßnahmen sowie auf etwaige Benachrichtigungen betroffener Personen eingehen. Zum vertiefenden Verständnis können hierzu ergänzend die vom Auftragsverarbeiter neu bereitgestellten Informationen beigefügt werden.

Fazit und Bewertung

Anhand des betrachteten Szenarios wurde aufgezeigt, wie die Kommunikation zwischen dem Auftragsverarbeiter, den Verantwortlichen und der Datenschutzaufsichtsbehörde im Falle von Verletzungen des Schutzes personenbezogener Daten, die durch einen Ransomware-Angriff ausgelöst worden sind, ablaufen sollte. Durch ein schnelles und abgestimmtes Handeln zwischen dem Auftragsverarbeiter und den Verantwortlichen auf der einen und der Vermeidung der dargestellten Problemfelder auf der anderen Seite können vermeidbare Verzögerungen im Ablauf verhindert oder zumindest minimiert werden. Dadurch werden mögliche nachteilige Auswirkungen der Verletzungen des Schutzes personenbezogener Daten auf die betroffenen Personen vermieden oder zumindest reduziert. Auch wird sichergestellt, dass die Benachrichtigung der betroffenen Personen nicht erst in größerem zeitlichem Abstand zum eigentlichen Vorfall erfolgt.

Im Falle eines angenommenen hohen Risikos für Rechte und Freiheiten betroffener Personen sollte das Abwenden von möglichen Schäden ein primäres Interesse aller Beteiligten sein. Dies gilt auch unabhängig von den gesetzlichen Anforderungen der DS-GVO. Daher sollte ein besonderes Augenmerk auf eine unverzügliche und angemessene Benachrichtigung der betroffenen Personen und auf ihre erforderliche Unterstützung gerichtet werden.

Ausgearbeitete und regelmäßig geübte Prozesse sowie Notfallhandbücher unterstützen die effektive und effiziente Behandlung von IT-Sicherheitsvorfällen. Bei der Konzeption ebendieser müssen die Umsetzungen der datenschutzrechtlichen Anforderungen als Teil der vorgesehenen Prozesse sichergestellt werden. Insbesondere bei Auftragsverarbeitungen werden bei Auftragsverarbeitern und Verantwortlichen ineinandergreifende Prozesse für Meldeketten bei Datenschutzverletzungen benötigt, die gemeinsam regelmäßig geprobt, evaluiert und im Bedarfsfall angepasst werden sollten.

Für eine zeitnahe Reaktion ist es essenziell, dass der Auftragsverarbeiter die Verantwortlichen schnell und angemessen informiert. Es kann dabei sinnvoll sein, dass er die Verantwortlichen an ihre datenschutzrechtlichen Pflichten erinnert, insbesondere wenn es sich bei den Verantwortlichen um kleinere Unternehmen oder Organisationen handelt.

Mit Art. 28 Abs. 3 Buchst. f DS-GVO ist bereits festgelegt, dass die Unterstützung eines Verantwortlichen bei der Einhaltung seiner Pflichten durch den Auftragsverarbeiter vertraglich zu regeln ist. Darunter fallen insbesondere auch die Pflichten, die die Behandlung von Verletzungen des Schutzes personenbezogener Daten betreffen. Je nach Verarbeitungstätigkeit kann es daher sinnvoll sein, für etwaige Datenschutzverletzungen entsprechende, vom Auftragsverarbeiter zu erbringende Leistungen vertraglich festzuhalten, insbesondere auch mit zeitlichen Garantien.

17.4
Prüfung des Kommunikationsmedieneinsatzes bei einem großen Verband

Sofern bestimmte Formen von Datenschutzverletzungen bei einzelnen Verantwortlichen gehäuft auftreten, kann dies für die Datenschutzaufsichtsbehörde einen Grund darstellen, eine anlasslose Prüfung durchzuführen. Eine solche Prüfung kann besonders bei komplexeren Organisationsstrukturen die Zusammenarbeit unterschiedlicher Fachreferate erfordern und mehrere Schwerpunkte aufweisen. Ein Beispiel für eine mögliche Herangehensweise bei einer solchen Prüfung zeigt der Bericht von einer derzeit noch in Durchführung befindlichen Prüfung bei einem Verband.

Gelegentlich stelle ich fest, dass bestimmte Verletzungen des Schutzes personenbezogener Daten bei einzelnen Verantwortlichen gehäuft auftreten. Mitunter kann dies einen Grund für mich darstellen, eine tiefergehende Prüfung zu initiieren. So meldete ein großer Verband mit Sitz in Hessen in der Vergangenheit mehrere Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO im Zusammenhang mit Phishing. Mindestens eine dieser Meldungen offenbarte Mängel auf Ebene der technischen und organisatorischen Maßnahmen. Zu diesem Vorfall habe ich bereits in meinem 48. Tätigkeitsbericht zum Datenschutz berichtet. Die Bearbeitung dieser Meldungen wurde zunächst ohne aufsichtsbehördliche Maßnahmen abgeschlossen, da davon ausgegangen wurde, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen vorsah, um vergleichbare Vorfälle künftig besser zu vermeiden. Jedoch blieb zunächst noch offen, ob die geplanten Maßnahmen tatsächlich im erwarteten Maße umgesetzt werden würden und damit nun ein angemessener Schutz bei der Verarbeitung personenbezogener Daten bei den entsprechenden Verarbeitungstätigkeiten besteht. Daher habe ich mich entschlossen, gemäß Art. 58 Abs. 1 Buchst. b DS-GVO eine anlasslose aufsichtsbehördliche Prüfung des Verantwortlichen zu initiieren.

In den Jahren 2020 und 2021 sahen sich die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vor vielfältige Herausforderungen gestellt, nicht zuletzt auch in Folge der COVID-19-Pandemie. Die Nutzung von Kommunikationsmedien bildete hierbei einen der Schwerpunkte, insbesondere der Einsatz von Videokonferenzsystemen (VKS). Von der DSK wurden u. a. Orientierungshilfen zur Übermittlung personenbezogener Daten per E-Mail (2020, https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf) und zu VKS (2021, https://www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf) bereitgestellt. Ich selbst habe auf meiner Website ergänzende Informationen zu VKS (https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/videokonferenzsysteme-allgemeines) sowie zur Nutzung von Telefax (https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/uebermittlung-personenbezogener-daten-per-fax) veröffentlicht. Ferner habe ich im 49. Tätigkeitsbericht einen Beitrag zur Nutzung von E-Mail publiziert.

Aufgrund der mittlerweile mehr als drei Jahre zurückliegenden Verletzungen des Schutzes personenbezogener Daten und einem erneuten Vorfall im Jahre 2020 ist von dem Verband eine besondere Sensibilisierung für das Thema Phishing zu erwarten. Auch der Einsatz weiterer Kommunikationsmedien muss datenschutzrechtskonform erfolgen. Die angeführten Veröffentlichungen der DSK und meiner Behörde bieten für die jeweiligen Kommunikationsmedien dabei Orientierung und Hilfestellungen.

Vor diesem Hintergrund habe ich die Prüfung ausgewählter Verarbeitungstätigkeiten hinsichtlich des datenschutzrechtskonformen Einsatzes bestimmter Kommunikationsmedien begonnen. Entsprechend der Schwerpunkte der behördlichen Veröffentlichungen habe ich im Vorfeld den Kommunikationsmedieneinsatz von VKS, E-Mail und Telefax für die Prüfung ausgewählt. Um eine effiziente und verhältnismäßige Prüfung zu ermöglichen, habe ich das Ziel der Prüfung vorab klar abgegrenzt, um etwa die Ausweitung der Prüfung auf Verarbeitungstätigkeiten, die außerhalb des Beschäftigtendatenschutzes liegen, zu vermeiden.

Den fachlich-juristischen Schwerpunkt der Prüfung bildet, ausgehend von den Kategorien betroffener Personen der früheren Vorfälle, der Beschäftigtendatenschutz. Aufgrund von ersten Erkenntnissen, die darauf hindeuten, dass bei den Verarbeitungstätigkeiten des Verantwortlichen Auftragsverarbeiter mit Sitz in Ländern außerhalb des Geltungsbereichs der DS-GVO zum Einsatz kommen, wird ein weiterer Fokus auf dem internationalen Datentransfer liegen. Ebenso werden Kolleginnen und Kollegen aus den Bereichen Vereinsdatenschutz und technisch-organisatorischer Datenschutz ihre Expertise zur Prüfung beitragen.

Die Prüfung ist so aufgebaut, dass zunächst anhand des Prüfauftrags und der darin enthaltenen Prüfgegenstände eine Übersicht infrage kommender Verfahren unter Nutzung der relevanten Kommunikationsmedien vom Verantwortlichen angefordert wurde. Diese Übersicht musste auf einem hohen Abstraktionsniveau lediglich die Bezeichnung der Verfahren, die Kategorien betroffener Personen sowie die eingesetzten Kommunikationsmedien enthalten. Aus dieser ersten Stellungnahme des Verantwortlichen wurde bereits erkennbar, dass dieser das Telefax nicht mehr einsetzt und dieses als Prüfgegenstand somit entfallen konnte. Zusammen mit dieser Verfahrensübersicht wurden auch Informationen zur Verbandsstruktur angefordert, da sich der Verband aus mehreren Körperschaften zusammensetzt, die bei der Verarbeitung personenbezogener Daten auf Grundlage von Auftragsverarbeitungsverträgen gemäß Art. 28 DS-GVO miteinander ins Verhältnis treten.

Die Verfahrensübersicht erlaubte es mir, gezielt Verarbeitungstätigkeiten auszusuchen, die einer Prüfung unterzogen werden sollen. Ich habe daher im Anschluss daran gemäß Art. 30 Abs. 4 DS-GVO die entsprechenden Auszüge des Verzeichnisses von Verarbeitungstätigkeiten des Verantwortlichen sowie die verbandsinternen Geschäftsbesorgungs- und Auftragsverarbeitungsverträge angefordert. Zu diesen Verträgen gehören auch Übersichten über die von den einzelnen Verantwortlichen und Auftragsverarbeitern ergriffenen technischen und organisatorischen Maßnahmen. Außerdem war nun zweifelsfrei zu erkennen, dass externe Auftragsverarbeiter mit Sitz in den USA zum Einsatz kommen. Da eine solche Datenübermittlung derzeit regelmäßig nur aufgrund geeigneter Garantien gemäß Art. 46 DS-GVO erfolgen kann, habe ich den Verband außerdem gebeten, ein sogenanntes Transfer Impact Assessment gemäß den Klauseln 14 und 15 der Standarddatenschutzklauseln der Europäischen Kommission vorzulegen. Ein solches Transfer Impact Assessment muss aufzeigen, welche Risiken der Verantwortliche bei der Datenübermittlung in das Drittland berücksichtigt und welche ergänzenden Maßnahmen er ergreift, um sicherzustellen, dass bei dieser Verarbeitung ein Schutzniveau für die personenbezogenen Daten erreicht wird, das mit dem innerhalb des Geltungsgebiets der DS-GVO vergleichbar ist. Bei der Bewertung der Angemessenheit solcher ergänzenden Maßnahmen orientiere ich mich unter anderem an den EDSA-Empfehlungen 01/2020 (https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf) zu diesem Thema.

Der Verband hat meiner Behörde alle bislang geforderten Unterlagen übermittelt. Zum Redaktionsschluss dieses Tätigkeitsberichts befinden sie sich in der eingehenden Prüfung durch meine Mitarbeiterinnen und Mitarbeiter.

17.5
Datenschutzrelevante Schwachstellen in selbstentwickelter Software

Fehler im Rahmen der Eigenentwicklung von Software können während des betrieblichen Einsatzes erhebliche negative Auswirkungen auf den Schutz personenbezogener Daten haben. Daraus ergeben sich Auswirkungen auf den gesamten Lebenszyklus von IT-Systemen und IT-Diensten von der Inbetriebnahme bis zur Aussonderung. Daher müssen Verantwortliche bereits bei der Entwicklung die Anforderungen des Datenschutzes umsetzen und geeignete technische und organisatorische Maßnahmen (TOM) ergreifen.

Im Berichtszeitraum gingen bei mir Beschwerden und Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO ein, die im Zusammenhang mit ausnutzbaren Schwachstellen in selbstentwickelter Software standen. Betroffen waren insbesondere mobile Applikationen (Apps) und Web-Anwendungen, bei deren Nutzung es zu Verletzungen des Schutzes personenbezogener Daten im Sinn des Art. 4 Nr. 12 DS-GVO und zur Offenlegung von ungeschützten Datenstrukturen gekommen war. Ursachen waren u. a. Schwachstellen bei der Authentisierung und Autorisierung sowie weitere, allgemein bekannte Schwachstellen, wie man sie z. B. in den Top 10 des Open Web Application Security Projects (OWASP Top 10) findet. OWASP ist eine Non-Profit-Organisation, die das Ziel verfolgt, die Sicherheit von Anwendungen und Diensten im Internet zu verbessern. Die erkannten Schwachstellen waren auf Fehler im Rahmen der Programmierung zurückzuführen.

Schwachstelle

Schwachstellen sind im Folgenden als Fehler in der Software zu verstehen, die dazu führen können, dass IT-Systeme und IT-Dienste anfällig für Bedrohungen werden. Daraus resultieren konkrete Gefährdungen für die Verarbeitung personenbezogener Daten. Werden solche Schwachstellen erfolgreich ausgenutzt, können Verletzungen der in Art. 32 Abs. 1 Buchst. b DS-GVO vorgegebenen Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste die Folge sein (s. auch 50. Tätigkeitsbericht, Kap. 18.3).

Individualsoftware

Selbstentwickelte Software (Individualsoftware) ist eine individuell für die Bedürfnisse und Anforderungen einer einzelnen Organisation oder Behörde entwickelte Software. Im Gegensatz zu Standardsoftware wird sie nicht

für einen großen Markt potenzieller, zum Teil noch unbekannter Anwender entwickelt. Individualsoftware wird in den hier berücksichtigten Fällen von den eigenen Softwareentwicklern einer Organisation oder einer Behörde zur eigenen Verwendung durch diese erstellt.

Identifizierte Schwachstellen

Im Folgenden gehe ich beispielhaft und nicht abschließend auf ausgewählte Schwachstellen aus mir im Berichtszeitraum bekanntgewordenen Vorfällen ein. Diese Vorfälle traten alle im Zusammenhang mit Individualsoftware auf.

Über eine App wurde auf ein Unternehmensportal zugegriffen, das eigentlich Kunden nur die jeweils eigenen Daten einsehen lassen sollte. Jedoch konnte auf strukturiert abgelegte Dokumente mit personenbezogenen Daten anderer Kunden ohne Schutz durch Authentifizierungs- und Autorisierungsmaßnahmen zugegriffen werden. Aufgrund eines fehlerhaften Berechtigungskonzeptes, sowohl im Bereich der eingesetzten App als auch im Unternehmensportal, waren bei der Entwicklung der Anbindung zwischen der App und dem Unternehmensportal Authentisierungs- und Autorisierungsmechanismen fehlerhaft umgesetzt worden.

Gegenstand einer weiteren Schwachstelle waren vom Verantwortlichen verwendete Hyperlinks, die es den Benutzern ermöglichten, über die Web-Anwendung auf personenbezogene Daten zuzugreifen. Als Authentisierungs- und Autorisierungsmerkmal war in den Hyperlinks eine Identifikationsnummer enthalten, die dem jeweiligen Benutzer zugeordnet war. Im vorliegenden Fall konnte durch ein Verändern dieser Identifikationsnummer auf personenbezogene Daten anderer Benutzer zugegriffen werden. Da die Identifikationsnummer fortlaufend vergeben wurde, war es leicht möglich, gültige Identifikationsnummern zu erraten. Durch diese Schwachstelle konnte ohne weitere Authentisierungsmerkmale unberechtigt Einblick in zum Teil besondere Kategorien von personenbezogenen Daten im Sinn des Art. 9 DS-GVO genommen werden. Angriffe, die solche oder vergleichbare Schwachstellen ausnutzen, sind auch als „Web Parameter Tampering“ (OWASP) oder Parameter-Manipulation bekannt.

In einem weiteren Fall wurden in einer Web-Anwendung nach der Eingabe des Benutzernamens und des Passwortes diese Authentisierungsmerkmale als Parameter des Uniform Resource Locator (URL) im Klartext übertragen. Grundsätzlich können durch das Zugänglichmachen von Authentisierungsmerkmalen, über die betroffene IT-Anwendung hinaus, weitreichende Risiken für den Betroffenen entstehen, wenn diese mehrfach verwendet werden. Gleichzeitig kann über einen solchen Zugang Schaden für den Verantwortlichen selbst entstehen.

Mögliche Maßnahmen

Die folgenden aufgeführten Anforderungen an und Maßnahmen für die Eigenentwicklung von Software konzentrieren sich auf die dargestellten Schwachstellen und sind nicht abschließend. Ziel ist im Folgenden, einen ersten Eindruck zu konkreten Handlungsoptionen zu geben, um vergleichbaren Schwachstellen während der Entwicklung vorzubeugen. Weitere Maßnahmen sollten den einschlägigen Regelwerken entnommen werden. Beispielhaft und nicht abschließend soll in diesem Zusammenhang auf die umfangreichen Informationen zu geeigneten Maßnahmen des BSI und des OWASP verwiesen sein.

Entwickler sollten bereits in der Entwicklungsphase einer Software die datenschutzrechtlichen Anforderungen und mögliche TOMs zu deren Umsetzung kennen. Hierdurch können sie von Beginn an dazu beitragen, dass die Software später datenschutzrechtskonform eingesetzt werden kann.

Eine wichtige Voraussetzung für die Eigenentwicklung von Software sind die initiale sowie die fortlaufende Qualitätssicherung. Hierbei sollten insbesondere auch die Aspekte des Datenschutzes in ausreichendem Maß berücksichtigt werden. Ist die Qualitätssicherung fester Bestandteil im Entwicklungsprozess, erhöht sich die Wahrscheinlichkeit, dass Schwachstellen bereits im Rahmen der Umsetzung erkannt und noch vor der Inbetriebnahme der Software behoben werden können. Einige der in diesem Beitrag aufgezeigten Schwachstellen hätten beispielsweise im Rahmen geeigneter Funktionstests erkannt und behoben werden können (BSI, IT-Grundschutz-Kompendium, „CON.8 Software-Entwicklung“, Stand Februar 2022, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf). Von Herstellern kommunizierten Schwachstellen und sonstigen Hinweisen, etwa in Artikeln, Beiträgen im Internet oder von Institutionen wie BSI, HBDI oder Hessen CyberCompetenceCenter (Hessen3C), sollten auch bei eigenentwickelter Software Aufmerksamkeit geschenkt werden.

Wird neue Software nicht ausreichend getestet, können Fehler in der Software übersehen werden. Solche Fehler gefährden nicht nur personenbezogene Daten im Betrieb, sondern unter Umständen auch andere Anwendungen und IT-Systeme in der Produktivumgebung. Werden Sicherheitsfunktionen, z. B. die Umsetzung grundlegender Schutzanforderungen, nicht getestet, ist nicht sichergestellt, dass der spätere Einsatz der Software den Anforderungen des Art. 32 Abs. 1 DS-GVO genügen kann. In Abhängigkeit von den jeweils ausnutzbaren Schwachstellen können infolgedessen personenbezogene Daten unbefugt offengelegt, manipuliert oder zerstört werden.

In Bezug auf Schwachstellen in eigenentwickelter Software sollte nicht nur an den selbst erstellten Quellcode gedacht werden, sondern auch an integrierte Bibliotheken und Frameworks. Beispielhaft soll an dieser Stelle die im Dezember 2021 bekannt gewordene Schwachstelle im Framework Log4J erwähnt werden. Diese ermöglichte es Angreifern unter bestimmten Bedingungen, eigenen Programmcode auf den betroffenen Servern auszuführen. Das frei verfügbare Framework war unter anderem in eine Vielzahl unterschiedlicher Individualsoftware integriert worden, wodurch die auf diesen basierenden IT-Systeme und -Dienste zumindest potenziell angreifbar waren. Sicherheitsupdates sollten deshalb möglichst zeitnah identifiziert und unter Berücksichtigung der betrieblichen Belange so schnell wie möglich eingespielt werden. Erreichen verwendete Bibliotheken und Frameworks das Ende ihres Lebenszyklus, muss dies proaktiv erkannt und derart berücksichtigt werden, dass veraltete Komponenten frühzeitig ersetzt werden. Damit Schwachstellen bei der Verwendung von Bibliotheken und Frameworks erkannt und behoben werden können, müssen ferner Verfahren zur regelmäßigen Überprüfung etabliert und angewendet werden. Gleiches gilt für zur Ausführung eigenentwickelter Software eingesetzte Laufzeitumgebungen.

Neben einer kontinuierlich begleitenden Überprüfung ist auch die regelmäßige Durchführung von Penetrationstests (Pentests) unter weiteren Maßnahmen in Erwägung zu ziehen. Bei Pentests handelt es sich um umfassende Tests der Sicherheit von IT-Systemen und IT-Diensten, in denen auch softwarebedingte Schwachstellen erkannt werden können. Im Schwerpunkt wird bei solchen Tests nach Schwachstellen gesucht, die geeignet sind, unbefugt in die IT-Systeme und -Dienste einzudringen. Pentests gehen über den automatisierten Einsatz von Schwachstellenscannern hinaus.

Abschließend ist zu bedenken, dass die oben beschriebenen Ansätze und Verfahren nicht nur für das erste Projekt zur initialen Umsetzung der eigenentwickelten Software zur Anwendung kommen sollten. Sie werden vielmehr auch in allen Folgeprojekten benötigt, etwa im Rahmen der Weiterentwicklung der Software.

Fazit

Software ohne Fehler gibt es nicht. Dies gilt nicht zuletzt auch für selbstentwickelte Individualsoftware. Die aufgezeigten Fälle stehen beispielhaft für im Berichtszeitraum aufgetretene Verletzungen des Schutzes personenbezogener Daten aufgrund von ausgenutzten Schwachstellen in Individualsoftware. Sie zeigen exemplarisch die mit der Verarbeitung von personenbezogenen Daten mittels selbstentwickelter Software einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen aufgrund von ausnutzbaren

Schwachstellen. Es sei darauf hingewiesen, dass solche Risiken nicht nur auf Eigenentwicklungen und Individualsoftware beschränkt sind, sondern auch mit Standardsoftware einhergehen. Es müssen also immer geeignete Methoden und Vorgehensweisen festgelegt und gelebt werden, damit Risiken erkannt und hierfür geeignete TOMs abgeleitet sowie bereits während der Erstellung der Software erfolgreich umgesetzt werden können. Unverzichtbar ist ein Verfahren zum Testen und zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit solcher Maßnahmen in selbstentwickelter Software, auch über den selbst programmierten Quellcode hinaus. Ergänzend können Pentests zum Einsatz kommen. Die Nutzung valider Informationsquellen sind ein wichtiges Hilfsmittel, um bereits bei der Erstellung von Software, aber auch danach Risiken erkennen und beheben zu können. Dies beinhaltet insbesondere auch die Möglichkeit zur schnellen Identifikation und Umsetzung notwendiger Aktualisierungen, etwa für integrierte Bibliotheken und Frameworks sowie für Laufzeitumgebungen. Gleiches gilt auch für etwaige Ankündigungen eines bevorstehenden Lebenszyklusendes von integrierten Komponenten und den resultierenden Bedarf nach Ersatz.

17.6
Benachrichtigung von Betroffenen bei Missbrauch von E-Mail-Konten

Stellt eine verantwortliche Stelle fest, dass ihre Kommunikationsdienste durch einen Angreifer übernommen und zum Versand von Phishing-Nachrichten missbraucht werden, ist sie verpflichtet, auf Basis einer Risikobeurteilung zu prüfen, ob die Betroffenen über den Vorfall zu benachrichtigen sind. Bei einer solchen Prüfung besteht die Gefahr, dass die verantwortliche Stelle die Menge der betroffenen personenbezogenen Daten nicht vollständig erfasst und nur eine Teilmenge betrachtet. Ein Beispiel eines solchen Falles zeigt der Bericht von einer kürzlich erfolgten Meldung durch ein Wirtschaftsunternehmen.

Im Berichtszeitraum beobachtete ich einen Anstieg von Meldungen über Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO, die aus der widerrechtlichen Übernahme von E-Mail-Konten resultierten. Angreifer kaperten erfolgreich fremde E-Mail-Konten und missbrauchten diese anschließend für den Versand von maliziösen Phishing-E-Mails. Bei dieser Angriffsform versuchten sich die Angreifer als vertrauenswürdiger Absender auszugeben und gestalteten ihre Nachrichten so, als wären es legitime Anfragen. Das Ziel der Angreifer ist es, die Empfänger zur Preisgabe persönlicher Informationen wie Bankdaten, Kreditkartennummern oder Zugangsdaten zu bewegen. Beispielsweise werden unter Bezugnahme auf

frühere Konversationen „geänderte Bankverbindungen“ durch die Angreifer übermittelt, um Überweisungsbetrug zu begehen. Teilweise werden auch Hyperlinks zu von den Angreifern erstellten, vorgeblichen Anmeldemasken von Diensten wie Server-Portalen verteilt, um weitere Zugangsdaten abzugreifen.

Im zweiten Quartal des Berichtszeitraums erhielt ich eine Meldung gemäß Art. 33 DS-GVO eines börsennotierten Unternehmens über die erfolgreiche Übernahme und den nachfolgenden Missbrauch des E-Mail-Funktionspostfaches einer Filiale des Unternehmens. Über das gekaperte E-Mail-Konto wurden Phishing-E-Mails in mittlerer vierstelliger Anzahl an Kunden und Mitarbeitende versendet. Nach Entdeckung des Vorfalls und Einleitung von technischen und organisatorischen Maßnahmen zur Beendigung desselben meldete die verantwortliche Stelle, dass die betroffenen Personen gemäß Art. 34 DS-GVO über die Datenschutzverletzung durch ein Anschreiben benachrichtigt worden seien.

Im Rahmen der Sachverhaltsaufklärung stellte ich Rückfragen zum Vorfall sowie zu den Arten und Kategorien betroffener personenbezogener Daten, die in den Inhalten und Anhängen der E-Mails des betroffenen E-Mail-Kontos enthalten waren. Die verantwortliche Stelle antwortete hierauf, dass die betroffenen E-Mails nur personenbezogene Daten in Form von Vorname und Name des jeweiligen E-Mail-Empfängers enthielten. Im Verlauf der weiteren Kommunikation stellte sich heraus, dass die verantwortliche Stelle ausschließlich die Empfänger der versendeten Phishing-Mails als Betroffene betrachtet und somit auch nur diese über den Vorfall informiert hatte.

Die Vorgehensweise der verantwortlichen Stellen, dass nur die Empfänger der versendeten Phishing-Nachrichten über den Vorfall benachrichtigt wurden, beobachtete ich bei einem großen Teil der eingehenden Meldungen in gleichgelagerten Fällen. Regelmäßig werden die Optionen, die sich den Angreifern bei der Übernahme eines E-Mail-Kontos bieten, nicht vollständig betrachtet. So ist stets davon auszugehen, dass die Angreifer ihren Zugriff nicht nur zum Versand von maliziösen Phishing-Mails nutzen. Zusätzlich erhalten sie Zugriff auf Inhalte und Anhänge der E-Mails im übernommenen E-Mail-Postfach und können somit Kenntnis von darin enthaltenen personenbezogenen Daten erlangen. Somit ist zusätzlich eine Verletzung der Vertraulichkeit dieser Daten gegeben. Dieser Umstand macht es notwendig, dass im Rahmen einer Risikobeurteilung nach Art. 34 Abs. 1 DS-GVO nicht nur die Empfänger der Phishing-Nachrichten als betroffene Personen berücksichtigt werden. Zusätzlich müssen auch diejenigen Personen, deren personenbezogene Daten in den Inhalten des übernommenen E-Mail-Kontos gespeichert oder verarbeitet werden, mit in die Betrachtungen einbezogen werden. Ebenso sind eventuell weitere Funktionalitäten von E-Mail-Diensten zu prüfen. In Diensten

wie Kalender, Kalenderanhängen und Adressbüchern können sich weitere personenbezogene Daten befinden und vom Vorfall betroffen sein. Ferner habe ich in zurückliegenden Meldungen gleichgelagerter Fälle beobachtet, dass Angreifer ihren Zugriff auf E-Mail-Konten nutzen, um beispielsweise automatische Weiterleitungs- oder Löschregeln zu erstellen. Mit solchen Regeln können etwa eingehende Hinweise misstrauischer Empfänger einer Phishing-Mail sofort gelöscht oder neue E-Mail-Nachrichten automatisiert an eine fremde E-Mail-Adresse weitergeleitet werden.

Die verantwortliche Stelle hat gemäß Art. 33 Abs. 5 DS-GVO die Pflicht, alle im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten zu dokumentieren, um mir eine Überprüfung zu ermöglichen. Zu einer solchen Dokumentation gehören selbstverständlich auch die Ermittlung der Betroffenen sowie die Risikobeurteilung. Meine Behörde fordert bei der Bearbeitung von Meldungen nach Art. 33 DS-GVO regelmäßig diese Dokumentation an und prüft sie auf Vollständigkeit und Nachvollziehbarkeit. Wenn diese Dokumentation nicht vollständig ist, kann dies einen Pflichtverstoß darstellen.

Gibt es bei der verantwortlichen Stelle Unklarheiten zu den Themenfeldern Beurteilung des Risikos, Meldung an die Aufsichtsbehörde und Meldung an die Betroffenen, so kann diese die Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten der Art. 29-Datenschutzgruppe (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/wp250rev01_de.pdf) sowie das Kurzpapier Nr. 18 der DSK (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-08/kp_18_risiko.pdf) als Orientierungshilfe heranziehen. Die Leitlinien befassen sich in Kapitel 3 und 4 mit Hinweisen zu den drei Themenfeldern und im Anhang B der Leitlinien wird eine Liste mit Fallbeispielen in unterschiedlichen Szenarien dargestellt. Die DSK wiederum beschreibt in ihrem Kurzpapier ausführlich ihre Auffassung darüber, wie die DS-GVO im praktischen Vollzug angewendet werden sollte, und geht hier insbesondere auf die Punkte Bestimmung, Beurteilung und Eindämmung des Risikos ein.

Im dem vorliegenden Fall habe ich die verantwortliche Stelle über die obigen Umstände in Kenntnis gesetzt und zu einer Erweiterung der Risikobetrachtung auf die Inhalte der E-Mails und deren Anhänge im betroffenen E-Mail-Konto aufgefordert. Die verantwortliche Stelle hat mir bestätigt, im Rahmen einer neuen Risikobetrachtung auch die Inhalte und Anhänge der E-Mail in dem betroffenen Konto zu berücksichtigen.

17.7
Kein Backup? kein Mitleid! – Gewährleistung der Verfügbarkeit

Zur Gewährleistung des Schutzes personenbezogener Daten gehört es, deren Verfügbarkeit sicherzustellen. Ein wesentlicher Baustein hierzu ist die regelmäßige Durchführung von Datensicherungen (Backups). Nicht zuletzt die steigende Anzahl an erfolgreichen Ransomware-Angriffen zeigt, dass die Anforderungen an wirksame Backup-Konzepte gestiegen sind. Im Folgenden wird ein Überblick über mögliche Auswirkungen von fehlenden oder unzureichenden Datensicherungen bei Datenschutzvorfällen gegeben. Hierauf aufbauend werden die von Verantwortlichen und Auftragsverarbeitern in jedem Fall zu berücksichtigen Anforderungen an Backup-Konzepte skizziert.

Motivation

„Kein Backup? Kein Mitleid!“, diese Aussage ist inzwischen zu einem verbreiteten Sprichwort in IT-affinen Kreisen geworden und wird meistens mit einem leicht spöttischen Unterton rezitiert. Kaffeetassen, T-Shirts und andere Merchandise-Artikel mit diesem Sprichwort werden als ideales Geschenk für IT-Administratoren und Informatiker beworben. Was sich vielleicht als ein typischer Spruch von IT’lern anhören mag, hat allerdings auch eine juristische Entsprechung in der DS-GVO. Denn zu den Grundsätzen des Datenschutzes gehört es nach Art. 5 Abs. 1 Buchst. f DS-GVO, verarbeitete personenbezogene Daten gegen Verlust, Zerstörung oder Schädigung durch geeignete technische und organisatorische Maßnahmen zu schützen. Die Durchführung von regelmäßigen und wirksamen Datensicherungen ist wahrscheinlich die häufigste zu diesen Zwecken angewandte geeignete Maßnahme.

Die Existenz eines vorhandenen Backups und die Frage, wie dieses eingesetzt werden kann, wird oftmals erst dann relevant, wenn auf Grund eines Vorfalls gesicherte Daten wiederhergestellt werden sollen oder müssen. Dies ist beispielsweise der Fall, wenn etwas aus Versehen gelöscht oder überschrieben wurde, eine Festplatte beim Zugriff nur noch Fehler produziert oder ein IT-Gerät ausfällt oder abhandenkommt. In diesen Fällen zeigt sich, dass durch ein fehlendes, ein nicht wirksames oder ein unzureichendes Backup die Verfügbarkeit von personenbezogenen Daten gefährdet sein kann. Hiermit verbunden sind entsprechende Risiken für die Rechte und Freiheiten betroffener Personen.

Die Kategorie von Datenschutzvorfällen, bei der die Relevanz von vollständigen und richtig umgesetzten Backups am anschaulichsten ist, sind die sogenannten Ransomware-Angriffe. Zusammengefasst handelt es sich bei Ransomware-Angriffen um Angriffe auf IT-Systeme oder IT-Netzwerke mit krimineller Absicht. Ziel dieser Angriffe ist es, die auf den erfolgreich

kompromittierten IT-Systemen gespeicherten Daten zu verschlüsseln und für die Bereitstellung der zur Entschlüsselung notwendigen Schlüssel die Zahlung eines Lösegeldes zu verlangen. Da Backups den Zielen der Angreifer entgegenstehen, suchen Angreifer in der Regel gezielt nach diesen, um sie ebenfalls zu verschlüsseln oder unbrauchbar zu machen. In meinem 50. Tätigkeitsbericht (Kap. 18.2) für das Jahr 2021 habe ich mich mit Ransomware-Angriffen genauer befasst.

Beispiele aus der aufsichtsbehördlichen Praxis

Die folgenden Beispiele aus mir gemeldeten Datenschutzvorfällen im Berichtszeitraum illustrieren die Relevanz von Backups.

Das erste Beispiel bezieht sich auf ein kleines Unternehmen, das seine relevante Datenverarbeitung vollständig auf einem zentralen Server durchführte. Dies schloss auch das Backup der Daten auf eben diesem System ein. Durch einen erfolgreichen Ransomware-Angriff auf diesen Server wurden sämtliche Daten des Unternehmens inklusive der Backups verschlüsselt und damit unbrauchbar gemacht. Nicht alle Daten ließen sich aus „analogen“ Quellen wie Papier, Ausdrucken oder Ähnlichem wiederherstellen. Dieses Beispiel illustriert anschaulich, dass nicht jede Form eines Backups eine hinreichende Maßnahme ist, um die Verfügbarkeit von Daten zuverlässig zu gewährleisten.

Wie wichtig daher eine Datensicherung auf externen, nicht mit der angreifbaren IT-Infrastruktur verbundenen Datenträgern ist, ein sogenanntes Offline-Backup, demonstriert das zweite Beispiel eines größeren IT-Unternehmens, das ebenfalls von einem Ransomware-Angriff betroffen war. Das Unternehmen hatte zwar ein dediziertes Backup-System als sogenanntes Online-Backup. Das Backup-System war in die normale IT-Infrastruktur eingebunden und konnte direkt von den anderen IT-Systemen Datensicherungen vornehmen. Den Angreifern gelang es allerdings, sich Zugang zu diesem Online-Backup-System zu verschaffen. Sie waren damit in der Lage, nicht nur alle Backups auf diesem System zu löschen, sie hatten gleichzeitig auch Zugriff auf die an einem Punkt konzentrierten relevanten Daten des Unternehmens. Wie die IT-forensische Analyse des Vorfalls ergab, erfolgte die umfangreiche Exfiltration von Daten des Unternehmens von diesem Backup-System. Da es aber ein weiteres Backup-System gab, das die Datensicherung auf Magnetbänder – als Offline-Backup – durchführte, war es dem Unternehmen möglich, zumindest alle relevanten Daten wiederherzustellen.

Es muss nicht immer ein Ransomware-Angriff sein, der auf Grund einer ungenügenden Beschäftigung mit der wirksamen Umsetzung eines Backups die Schwere eines Datenschutzvorfalls signifikant erhöht. Ein Beispiel hierfür ist ein Verantwortlicher, der seine E-Mail-Infrastruktur von einem Auftrags-

verarbeiter betreiben ließ. Zu Vertragsbeginn war die Erstellung von Backups der E-Mail-Konten Teil des Leistungskatalogs des Auftragsverarbeiters. Nach einiger Zeit wurde die Backup-Funktionalität durch den Auftragsverarbeiter allerdings aus dem vom Verantwortlichen gebuchten Leistungsumfang entfernt. Hierauf reagierte der Verantwortliche nicht. Dies führte dazu, dass die bei einem Hackerangriff gezielt gelöschten E-Mails eines für den Verantwortlichen relevanten E-Mail-Accounts nicht wiederhergestellt werden konnten. Dieses Beispiel zeigt, dass es nicht ausreichend ist, zu Beginn einer neuen Verarbeitungstätigkeit eine Maßnahme einmal einzurichten und dann anzunehmen, dass diese über den gesamten Lebenszyklus einer Verarbeitungstätigkeit unverändert wirksam ist. Vielmehr müssen ergriffene technische und organisatorische Maßnahmen regelmäßig überprüft, bewertet und evaluiert werden. Auch müssen im Bedarfsfall Anpassungen vorgenommen werden.

Datenschutzrechtliche Bewertung mit rechtlicher Begründung

Die grundsätzliche datenschutzrechtliche Anforderung zur Gewährleistung der Verfügbarkeit verarbeiteter personenbezogener Daten ergibt sich aus Art. 5 Abs. 1 Buchst. f DS-GVO. Danach müssen personenbezogene Daten

Art. 5 Abs. 1 Buchst. f DS-GVO

in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit"); (…).

Die effektive Umsetzung eines Backup-Konzepts wäre eine technische und organisatorische Maßnahme (TOM) zum Schutz vor „unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung".

Die weiteren zu erfüllenden Anforderungen an ein solches Konzept werden in Art. 32 Abs. 1 und 2 DS-GVO zur Sicherstellung der Verfügbarkeit personenbezogener Daten konkretisiert.

Art. 32 DS-GVO

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher: Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische

und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

In Art. 32 Abs. 1 Buchst. c DS-GVO wird als Grundfähigkeit eines Backups gefordert, dass sich Daten bei einem Zwischenfall wiederherstellen lassen. In Art. 32 Abs. 1 Buchst. d DS-GVO wird gefordert, dass die technischen und organisatorischen Maßnahmen, wie das Backup, regelmäßig daraufhin überprüft, bewertet und evaluiert werden, ob die Wirksamkeit weiterhin gewährleistet ist. Für ein Backup bedeutet dies, dass nicht nur die erfolgreiche Erstellung regelmäßig überprüft werden muss, sondern auch die Wiederherstellung von Daten aus einem Backup. Als Bestandteil der organisatorischen Maßnahmen zum Thema Backup gehört es, dass entsprechende Prozesse existieren, dokumentiert sind und die für das Backup verantwortlichen Personen die Wiederherstellung von Daten regelmäßig üben.

Zur Entwicklung eines Backup-Konzepts gehört auch die Durchführung einer Risikoanalyse, um den Anforderungen aus Art. 32 Abs. 2 DS-GVO entsprechen zu können. In Verbindung mit Art. 32 Abs. 1 Buchst. b und d DS-GVO kann dies aber keine einmalige Angelegenheit am Anfang der Entwicklung sein. Vielmehr muss das Konzept ebenfalls regelmäßig kritisch überprüft, bewertet, die Wirksamkeit hinsichtlich geänderter Rahmenbedingungen evaluiert und bei Bedarf angepasst werden.

Praktische Mindestanforderungen an ein Backup-Konzept

Für die Erstellung eines Backup-Konzepts ist eine ganze Reihe von Aspekten zu berücksichtigen. Einen Überblick kann der entsprechende BSI-IT-Grundschutzbaustein „CON.3 Datensicherungskonzept“ mit den zugehörigen Umsetzungshinweisen bieten.

Als Backup-Strategie wird häufig auf die sogenannte 3-2-1-Strategie für Backups verwiesen. Bei dieser geht es darum, wie viele Kopien von Daten wie und wo vorgehalten werden sollten. 3-2-1 steht dabei dafür, dass mindestens drei Kopien der zu schützenden Daten inklusive der Originaldaten bereitgehalten werden sollen. Diese drei Kopien sollten auf mindestens zwei unterschiedlichen Speichermedien gespeichert werden. Davon sollte mindestens eine Kopie an einem separaten Standort vorgehalten werden. Diese Strategie hilft bereits gegen viele relevante Risiken, von versehentlichem Löschen von Daten über Schäden an einem Speichermedium bis hin zu katastrophalen Schäden an einem Standort. Für einen Schutz gegen gezielte Angriffe auf die IT-Infrastruktur wie bei einem Ransomware-Angriff kann dies allerdings ggf. nicht ausreichend sein.

Wie die genannten Beispiele zeigen, versuchen Angreifer in kompromittierten IT-Umgebungen in der Regel auf relevante IT-Systeme Zugriff zu erlangen und suchen dabei aktiv nach Backup-Systemen, um diese unbrauchbar zu machen. Dementsprechend sind diese Systeme explizit auch gegen einen unberechtigten Zugriff aus der eigenen IT-Umgebung heraus zu schützen. Eine offensichtliche Maßnahme wäre die Erstellung von Offline-Backups, wie beispielsweise mittels Magnetbänder, die dem Zugriff potenzieller Angreifer wirksam entzogen sind.

Der mit Offline-Backups in der Regel verbundene manuelle Aufwand steht dem Ziel entgegen, möglichst aktuelle Datenkopien zugreifbar zu haben. Mit Online-Backup-Systemen, die vollständig in die IT-Umgebung integriert sind, können demgegenüber automatisiert regelmäßig und in kürzeren Intervallen Datensicherungen durchgeführt werden. Auch bei diesen lässt sich das Risiko eines erfolgreichen Angriffs signifikant reduzieren, wenn bei der Konzeption und Umsetzung diese Backup-Systeme ähnlich gesichert werden wie IT-Systeme oder -Dienste, die über das Internet direkt erreichbar sind und damit jederzeit Angriffen ausgesetzt sein könnten. Je nach Anwendungsfall kann es ggf. sinnvoll sein, entsprechend gesicherte Online- und Offline-Backup-Systeme zu kombinieren. Wichtig ist dabei, dass das Gesamtkonzept für die umgesetzte Backup-Strategie stimmig ist.

Wie im Abschnitt zu den rechtlichen Anforderungen ausgeführt, ist es notwendig sicherzustellen, dass Backups erfolgreich durchgeführt werden und dass ein Wiederherstellen von Daten aus Backups in der erforderlichen Zeit funktioniert. Je nach Verarbeitungstätigkeit kann der alleinige Zugriff auf die Daten ohne die sie verarbeitenden IT-Systeme und -Dienste ggf. nicht ausreichend sein, um die Verfügbarkeit der Daten sicherzustellen. Dementsprechend ist es gemäß Art. 32 Abs. 1 Buchst. b DS-GVO erforderlich, auch die Verfügbarkeit dieser IT-Systeme und -Dienste durch entsprechende

Maßnahmen auf Dauer sicherzustellen. Entsprechend gut dokumentierte Notfall- oder Wiederherstellungsprozesse müssen dies ganzheitlich berücksichtigen. Die Wirksamkeit dieser Prozesse ist ebenfalls regelmäßig zu prüfen und vom zuständigen Personal auch zu üben. Gerade letzteres ist vor dem Hintergrund, dass die Notwendigkeit, auf Backups zuzugreifen, in Not- oder Stresssituationen auftritt, sehr wichtig. Es ist daher sinnvoll, die Durchführung dieser Tests unter den zuständigen Beschäftigten zu rotieren und darauf zu achten, dass auch in Vertretungssituationen entsprechend geschultes und geübtes Personal verfügbar ist.

Datensicherung ist eine Datenverarbeitung

Aus Sicht des Datenschutzes ist das Gewährleistungsziel Verfügbarkeit mittels der Durchführung von Backups von verarbeiteten personenbezogenen Daten sicherzustellen. Die Datensicherung ist selbst eine eigene Verarbeitungstätigkeit, für die Verantwortliche und Auftragsverarbeiter die entsprechenden Anforderungen der DS-GVO erfüllen müssen. Unter anderem sollten bei der Erstellung eines Backup-Konzepts die Rechte betroffener Personen, deren Daten verarbeitet werden, frühzeitig und durchgehend berücksichtigt werden. Das fängt beim Auskunftsrecht gemäß Art 15 DS-GVO an, das sich auch auf Daten beziehen kann, die ggf. noch in Backup-Systemen gespeichert sind. Analog können auch das Recht auf Berichtigung nach Art. 16 DS-GVO, das Recht auf Löschung nach Art. 17 DS-GVO und das Recht auf Einschränkung der Verarbeitung nach Art. 18 DS-GVO Daten innerhalb der Backup-Systeme betreffen. Die möglichen Auswirkungen sind daher zu untersuchen und entsprechende technische und organisatorische Maßnahmen vorzusehen, um die Ausübung der Rechte gewährleisten zu können.

Die Datensicherung als eine Verarbeitungstätigkeit muss ebenfalls die Anforderungen des Art. 32 DS-GVO an die Sicherheit der Verarbeitung personenbezogener Daten erfüllen. Die Integrität und Vertraulichkeit der gesicherten Daten müssen dementsprechend gewährleistet werden. Eine geeignete Maßnahme hierzu ist die Verschlüsselung der Daten, wenn diese richtig konzeptioniert und umgesetzt wird. Nähere Ausführungen zu diesem Themenkomplex im Zusammenhang mit Datensicherung mittels Cloud-Diensten finden im bereits zuvor referenzierten IT-Grundschutzbaustein „CON.3 Datensicherungskonzept“ des BSI eine Entsprechung mit der Standard-Anforderung „CON.3.A9 Voraussetzungen für die Online-Datensicherung“.

Fazit

Es bleibt also festzustellen, dass regelmäßige und wirksame Datensicherungen durch Backups verarbeiteter personenbezogener Daten in der Regel zu den notwendigen technischen und organisatorischen Maßnahmen zählen, um die Sicherheit der Verarbeitung insbesondere in Bezug auf die Verfügbarkeit gewährleisten zu können. Personenbezogene Daten verarbeitende Stellen müssen sich daher aktiv und kontinuierlich mit der Thematik beschäftigen, gerade auch im Hinblick auf die Bedrohungen durch Angriffe. Denn wie sagt schon das bei IT'lern beliebte Sprichwort: „Kein Backup? Kein Mitleid!"

18. Öffentlichkeitsarbeit

Im Jahr 2022 habe ich einen stärkeren Fokus auf die Öffentlichkeitsarbeit gelegt. Zum einen habe ich meine Stabsstelle Öffentlichkeitsarbeit personell um eine Stelle aufgestockt. Zum anderen habe ich mit ihr zusammen in der Außendarstellung neue Veranstaltungsformate aufgesetzt. In der Folge fällt die Bilanz der Veranstaltungen für das Jahr 2022 sehr positiv aus.

DatenDienstag

Das Jahr begann mit meiner Beteiligung am DatenDienstag zum Safer Internet Day am 8. Februar 2022 in Zusammenarbeit mit den Kollegen vom LDA Bayern und dem Museum für Kommunikation in Frankfurt. Das Thema lautete „Gemeinsam für ein besseres Internet – Herausforderungen aus Sicht der Datenschutzaufsicht". Beim DatenDienstag stellen Expertinnen und Experten Themen rund um Datenschutz und IT-Sicherheit vor und kommen anschließend mit dem Museumspublikum ins Gespräch, um das Bewusstsein für datenschutzrechtliche Fragen zu schärfen. Ich habe in meinem Vortrag anlässlich des Safer Internet Day 2022 nicht nur aktuelle Handlungsfelder aufgegriffen, sondern auch zu strukturellen Fragestellungen bei der Nutzung des Internets durch Unternehmen und Behörden gesprochen.

CAST-Forum zu Verbesserungen des Datenschutzrechts

Am 17. März 2022 fand in Darmstadt das CAST-Forum zum Thema „Verbesserungen des Datenschutzrechts – Wie lassen sich die Vorhaben der Ampelkoalition umsetzen?" statt. Die Veranstaltung wurde vom Competence Center for Applied Security Technology (CAST), dem Forum Privatheit und mir durchgeführt. Der Koalitionsvertrag zwischen SPD, Bündnis 90/Die Grünen und FDP verspricht ein „Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit". Die Koalition sieht sich „am Beginn eines Jahrzehnts im Umbruch". Die „notwendige Modernisierung" von Staat und Gesellschaft will sie vor allem durch eine Digitalisierung von Wirtschaft und Gesellschaft „vorantreiben". Der Koalitionsvertrag nennt 155 Vorhaben, die im weitesten Sinn Privatheit, Selbstbestimmung und Datenschutz betreffen oder Auswirkungen auf diese Werte haben. Mit ihrem Programm will die Koalition die Verwirklichungsbedingungen dieser Grundrechte nachhaltig verbessern. Ziel des von mir moderierten Forums war es, die programmatischen Aussagen des Koalitionsvertrags daraufhin zu analysieren, wie die abstrakten Vorgaben mit Praxiserfahrung konkretisiert werden müssen, um tatsächlich Fortschritte in einzelnen Feldern der Digitalisierung und des Datenschutzes zu erzielen.

Die Veranstaltung griff in sechs Vorträgen die gegenwärtige Situation im Datenschutzrecht und in der Datenschutzpraxis auf, informierte über die abstrakten Vorhaben der Koalition, stellte diese in den Kontext der aktuellen Datenschutzdiskussion und präsentierte Vorschläge, wie diese Vorhaben zu einer Verbesserung des Datenschutzrechts und der Datenschutzpraxis konkretisiert werden können. Die Vorträge betrafen die Themenfelder der Übermittlung personenbezogener Daten in Drittstaaten, die Stärkung der Bürgerrechte durch ein Recht auf Verschlüsselung, ein Recht auf Anonymisierung und durch Vorgaben zum IT-Schwachstellenmanagement, den Umgang mit Forschungsdaten und die Einführung neuer Institutionen wie Datenmärkte und Datentreuhänder, die rechtliche Bewertung von KI-Anwendungen in der EU-KI-Verordnung und nationalen Ergänzungen, Verbesserungen im Beschäftigtendatenschutz und die Einführung einer Überwachungsgesamtrechnung für Überwachungsgesetze.

Behördentag Hessen und Rheinland-Pfalz

Am 28. Juni 2022 fand in Frankfurt in einer Kooperation mit dem Landesdatenschutzbeauftragten Rheinland-Pfalz und dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. zum ersten Mal der „Behördentag Hessen und Rheinland-Pfalz“ statt. Die ganztägige Veranstaltung richtete sich an behördliche, kommunale und betriebliche Datenschutzbeauftragte. Die Tagung gab insbesondere Datenschutzbeauftragten öffentlicher Stellen die Gelegenheit, sich mit Fachleuten aus den Aufsichtsbehörden über Themen auszutauschen, die sie in ihrer alltäglichen Berufspraxis beschäftigen. Dazu gehörten im Berichtsjahr aktuelle Fragen des internationalen Datentransfers und der Künstlichen Intelligenz in der öffentlichen Verwaltung ebenso wie die Struktur der Landesdatenschutzgesetze und deren Zusammenspiel mit europäischen Regelwerken, wie der Datenschutz-Grundverordnung und der Datenschutz-Richtlinie im Bereich von Justiz und Inneres. Auch aktuelle Praxisthemen wie Cookies, Social-Media-Fanpages und Videokonferenzsysteme sowie Betroffenenrechte wurden in den insgesamt 17, zum Teil parallel stattfindenden Keynotes, Fachvorträgen und Podiumsdiskussionen beleuchtet. Zusätzlich zum Austausch untereinander konnten die Teilnehmenden mit ihren Fragen auch direkt an die Fachleute aus den Aufsichtsbehörden herantreten. Das galt sowohl für die Tagungspausen als auch für das interaktive Abschlusspanel „Die Aufsichtsbehörden beantworten Ihre Fragen“. Der sehr gut besuchte Datenschutztag war für alle Beteiligten ein wichtiges Element der fachlichen Weiterbildung, des gegenseitigen Verständnisses füreinander und des Erfahrungsaustausches. Es ist mir ein ganz besonderes Anliegen, diesen fachlichen Austausch zu begleiten und zu unterstützen.

Daher haben wir den 2. Behördentag Hessen – Rheinland-Pfalz bereits für den 5. Juli 2023 vorgesehen.

Tage der offenen Tür im Hessischen Landtag

Am 24. und 25. September 2022 nahm meine Behörde an den Tagen der offenen Tür des Hessischen Landtages teil. Unter dem Motto „Demokratie zum Anfassen“ hatte der Hessische Landtag alle Bürgerinnen und Bürger am Wochenende zu den Tagen der offenen Tür nach Wiesbaden in die Landeshauptstadt eingeladen. Am Stand meiner Behörde nahmen viele die Gelegenheit wahr, sich über die datenschutzrechtliche Aufsichtstätigkeit zu informieren. Meine Stabsstelle Öffentlichkeitsarbeit hatte einen Stand mit Informationsmaterialien und diversen Plakaten vorbereitet, über die meine Mitarbeiterinnen und Mitarbeiter mit den Bürgerinnen und Bürgern in regen Austausch kamen.

Festakt 50 Jahre Datenschutz in Hessen

Im Jahr 1970 hat der Hessische Landtag mit dem Hessischen Datenschutzgesetz (HDSG) das erste Datenschutzgesetz weltweit verabschiedet. Im folgenden Jahr wurde in Hessen der erste Datenschutzbeauftragte der Welt etabliert, der 1972 seinen ersten Tätigkeitsbericht veröffentlichte. Nachdem die für diese Jubiläen geplanten Feierlichkeiten 2020 und 2021 pandemiebedingt nicht durchgeführt werden durften, wurden sie alle drei am 6. Oktober 2022 in einem Festakt nachgeholt.

Die Hessische Landtagspräsidentin Astrid Wallmann eröffnete die Veranstaltung. Gewürdigt wurde durch sie u. a., dass der Hessische Landtag im Jahr 1970 internationale Datenschutzgeschichte geschrieben habe. Das Gesetz habe das Amt des Hessischen Beauftragten für Datenschutz als unabhängige Kontrollbehörde geschaffen. Betont wurde zudem, wie wichtig und zukunftsweisend diese Entscheidung gewesen ist, was bis heute zu sehen sei. Der Datenschutz stehe im digitalen Zeitalter vor ganz besonderen Herausforderungen.

Die Ministerin für Digitale Strategie und Entwicklung in Hessen, Prof. Dr. Kristina Sinemus, gratulierte im Namen der Landesregierung. Der Datenschutz habe mit zunehmender Digitalisierung noch mehr an Relevanz gewonnen. Gerade personenbezogene Daten wie im Gesundheitssektor seien ein höchst schützenswertes Gut. Daher brauche man eine gute Balance zwischen dem Nutzen der Daten und dem Schutz von Daten. Dann gelinge eine verantwortungsvolle Digitalisierung zum Wohle aller in der Gesellschaft.

Im Festvortrag würdigte Prof. Dr. Thomas von Danwitz, Richter am EuGH und Berichterstatter in vielen Gerichtsverfahren zum Datenschutz, die noch heute aktuellen Zielsetzungen und Vorgaben des ersten Hessischen Datenschutzgesetzes, die sich auch im europäischen Datenschutzrecht wiederfanden. Er skizzierte die Grundgedanken der Rechtsprechung des EuGH und schloss mit der Erkenntnis: „Eine demokratische Gesellschaft, die den Bürger ernst nimmt und – wie die Charta der Grundrechte – den Menschen in den Mittelpunkt ihres Handelns“ stellt, verwirklicht sich im Zeitalter der Digitalisierung auch und vor allem durch einen hochwertigen Datenschutz. Dieser ermögliche dem Bürger Institutionen des Staates und Wirtschaftsunternehmen gleichermaßen in freier Selbstbestimmung auf Augenhöhe zu begegnen. (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/datenschutz_in_hessen_und_europa_6_10_22_von_danwitz_kv.pdf).

Abgerundet wurde der Festakt mit einem historischen Bogen. In meinen Ausführungen habe ich an die Bedingungen der Datenverarbeitung und des Datenschutzes vor 50 Jahren mit „Gebietsrechenzentren, Lochkarten und Magnetbändern“ erinnert und habe sie mit den heutigen Herausforderungen durch die Datenmacht globaler Internetkonzerne und weltweit vernetzter Datenverarbeitung kontrastiert. Mit der Feststellung: „Gerade angesichts dieser radikalen Veränderungen gilt noch immer die Zielsetzung des ersten Hessischen Datenschutzgesetzes, dass Freiheitsrechte und Demokratie die Einhegung der Informationstechnik voraussetzen. Nur wenn sie durch datenschutzrechtliche Leitplanken und datenschutzgerechte Technikgestaltung geschützt werden, können wir sicher sein, dass wir mit Informationstechnik besser leben als ohne sie“, habe ich den Festakt geschlossen (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/rossnagel_vortrag_festakt_50_jahre_datenschutz_in_hessen.pdf).

25. Wiesbadener Forum Datenschutz

Zum Thema „Datenschutz stärkt Forschung“ schloss sich am Nachmittag des 6. Oktober 2022 das 25. Wiesbadener Forum Datenschutz an. Nach einer pandemiebedingten Pause traf sich das Fachpublikum im Hessischen Landtag und widmete sich dem Verhältnis von Forschung und Datenschutz. Beide werden vielfach als gegensätzliche Interessen gesehen. Jedoch müssen beide – Forschungsfreiheit und informationelle Selbstbestimmung – als Grundrechte gesehen werden, die einer Zuordnung bedürfen, die das jeweils andere Grundrecht möglichst wenig einschränkt. Das sei auch Voraussetzung dafür, dass das Vertrauen der Patienten gewonnen werden kann, die in die Verwendung ihrer Daten einwilligen sollen. Zum Forum waren vier Referentinnen und Referenten eingeladen, die sich in unterschied-

licher Weise dem Thema „Datenschutz stärkt Forschung“ genähert haben. Der Bundesbeauftragte (BfDI) Prof. Ulrich Kelber ging in seinem Vortrag „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz“ der Frage nach, welcher rechtspolitische Rahmen notwendig ist, um das Ziel verantwortungsvoller Datennutzung zu erreichen. Hierfür formulierte er zehn Gebote – z. B. die Unterstützung öffentlicher Interessen an der Forschung, die aktive Mitwirkung der betroffenen Personen, der Schutz personenbezogener Daten durch Anonymisierung, Pseudonymisierung und Verschlüsselung, den Einsatz von Datentreuhändern sowie den Schutz vor Re-Identifizierung. Prof. Dr. Franziska Boehm vom Karlsruher Institut für Technologie (KIT) untersuchte in ihrem Vortrag „Der besondere Schutz der Forschung in der Datenschutz-Grundverordnung“, welche besondere Berücksichtigung von Forschungsinteressen die DS-GVO vorsieht und wie diese Sonderregeln in der Praxis zur Anwendung kommen können. Dabei wies sie auf Ausnahmen z. B. von der Zweckbindung, Datenminimierung, Speicherbegrenzung, Bestimmtheit der Einwilligung, Rechten der betroffenen Personen und von Voraussetzungen der Datenübermittlung in Drittländer hin. Außerdem biete die DS-GVO den Mitgliedstaaten Öffnungsklauseln an, um Forschungszwecke weiter zu bevorzugen. Diese sollten genutzt werden, um auch im deutschen Recht unterschiedliche Rechtsregelungen zur Forschung zu harmonisieren. Prof. Dr. Dr. Eric Hilgendorf von der Universität Würzburg berichtete in seinem Vortrag „Der Datenschutz in der künftigen Regulierung europäischer Forschungsdatenräume“ von insgesamt 49 Gesetzgebungsakten oder -initiativen der Europäischen Kommission zur digitalen Transformation Europas. Zur Erleichterung der Datennutzung – insbesondere für Forschungszwecke – dienten vor allem der Data Governance Act und die Entwürfe für einen Data Act sowie zur Regulierung von insgesamt 13 europäischen Datenräumen. Dabei stellte er fest, dass der Datenschutz in diesen Gesetzgebungsakten keine systematische Berücksichtigung finde. Daher plädierte er für ein Moratorium, um Schutzvorkehrungen vor negativen Auswirkungen auf die Grundrechte ausreichend zu justieren. Prof. Dr. Hannes Federrath von der Universität Hamburg zeigte in seinem Vortrag „Datenschutzwahrende Methoden der Forschungsdatenverarbeitung“ auf, wie modernste Methoden der Informatik dazu beitragen können, effektive Forschungsprozesse ohne Datenschutzprobleme zu ermöglichen. Als Schutzmöglichkeiten stellte er fünf Privacy-Design-Strategien vor: Minimize (Beschränkung auf notwendige Daten), Separate (dezentrale Datenauswertung am Speicherort), Aggregate (von Personenbezug abstrahieren), Pertubate (Personenbezug durch Verrauschen ausschließen) und Hide (Zugriff auf personenbezogene Daten verhindern).

Von Hessen in die Welt

Mit dem Thema „Von Hessen in die Welt: Die Entwicklung des Datenschutzes im Wechselspiel von Kommunikationstechnik und Recht“ befasste sich am 2. November 2022 eine Veranstaltung, die meine Behörde in Kooperation mit dem Forum Privatheit und dem Museum für Kommunikation in Frankfurt veranstaltete. Bei der Dialog-Veranstaltung setzten sich Dr. h. c. Marit Hansen, Landesbeauftragte für Datenschutz Schleswig-Holstein, und ich als Sprecher des „Forum Privatheit“ und Hessischer Beauftragter für Datenschutz und Informationsfreiheit unter der Moderation von Dr. Ulf Buermeyer LL. M. (Vorsitzender der Gesellschaft für Freiheitsrechte e. V. und Host des Politik-Podcasts „Lage der Nation“) mit 50 Jahren Datenschutzgeschichte auseinander. Die Geschichte des Datenschutzrechts begann mit dem Hessischen Datenschutzgesetz von 1970, dem ersten Datenschutzgesetz der Welt. Dass sich seitdem viel getan hat und der Datenschutz sich von Hessen aus auf den Weg um die Welt gemacht hat, zeigte unser gemeinsamer Vortrag – ein Weg, der geprägt war von einem Wechselspiel zwischen Neuerungen in der Informations- und Kommunikationstechnik einerseits und im Datenschutzrecht andererseits. Wir haben herausgestellt, dass neue technische Entwicklungen immer wieder neue Herausforderungen für das Datenschutzrecht bedeuten, welches darauf seinerseits mit neuen Vorschriften und Gesetzen reagiert. Diese wiederum regen neue technische Entwicklungen an, um die rechtlichen Bedingungen zu erfüllen – oder sie zu umgehen. Dieses Wechselspiel zwischen Technik und Recht haben Marit Hansen aus der Sicht der Informatikerin und ich abwechselnd veranschaulicht. Telekommunikation erfolgte 1970 zum Zeitpunkt des ersten Hessischen Datenschutzgesetzes noch anonym und ohne Datenspeicherung. Heute, zur Zeit der europäischen Datenschutz-Grundverordnung, werden in der elektronischen Kommunikation so viele Daten erhoben, dass mit ihnen von allen Nutzenden vollständige Interessen-, Beziehungs- und Bewegungsprofile möglich sind und Interessen staatlicher und privater Stellen bestehen, diese für ihre Zwecke auszuwerten. Im Mittelpunkt standen Fragen wie z. B.: Welche Risiken für die Grundrechte sind mit der Entwicklung von Informationstechnik verbunden? Welche Regelungen hat das Datenschutzrecht gegen diese Risiken entwickelt? Wie können Recht und Technik zusammenwirken, um den Datenschutz zu verbessern? Und: Wie können sie dies – angesichts global agierender Unternehmen – weltweit tun?

Darüber hinaus wurde Ende des Berichtsjahres der Internetauftritt meiner Behörde aktualisiert. Der IT-Support der HZD für die alte Seite lief aus. Die neue Seite ist moderner und thematisch attraktiver geworden. Aktuell überarbeiten die Fachbereiche ihre Beiträge und garantieren damit für das nächste Jahr viele neue interessante Inhalte.

19. Arbeitsstatistik Datenschutz

19.1 Zahlen und Fakten

Die statistische Auswertung der Arbeitsmengen in diesem Kapitel entspricht den formalen Anforderungen, die die Datenschutzkonferenz vorgibt, um eine bundeseinheitliche Aussage treffen zu können. Diese Werte werden u. a. der Europäischen Kommission und dem Europäischen Datenschutzausschuss gemäß Art. 59 DS-GVO vorgelegt.

Zahlen und Fakten	Fallzahlen 01.01.2021 bis 31.12.2021	Fallzahlen 01.01.2022 bis 31.12.2022
a. „Beschwerden“ Anzahl von Beschwerden, die im Berichtszeitraum nach DS-GVO eingegangen sind. Als Beschwerden werden bei Eingang solche Vorgänge gezählt, die schriftlich eingehen und bei der eine natürliche Person eine persönliche Betroffenheit darlegt, auf die Art. 77 DS-GVO anwendbar ist. Dies schließt Abgaben ein. Telefonische Beschwerden werden nur dann gezählt, wenn sie verschriftlicht werden (z. B. durch Vermerk).	5.179 (davon 953 Abgaben)	**4.474** (davon 736 Abgaben)
b. „Beratungen“ Anzahl von schriftlichen Beratungen. Dies umfasst summarisch Beratungen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. **Nicht:** (Fern-)mündliche Beratungen, Schulungen, Vorträge etc.	2.123	**1.334**
c. „Meldungen von Datenschutzverletzungen“ Anzahl schriftlicher Meldungen	2.016	**1.754**
d. „Abhilfemaßnahmen“ Anzahl der getroffenen Maßnahmen, die im Berichtszeitraum getroffen wurden.		
(1) nach Art. 58 Abs. 2 a (Warnungen)	(1) 1	(1) **1**
(2) nach Art. 58 Abs. 2 b (Verwarnungen)	(2) 28	(2) **37**
(3) nach Art. 58 Abs. 2 c–g und j (Anweisungen und Anordnungen)	(3) 3	(3) **16**
(4) nach Art. 58 Abs. 2 i (Geldbußen)	(4) 29	(4) **113**
(5) nach Art. 58 Abs. 2 h (Widerruf von Zertifizierungen)	(5) 0	(5) **0**

e. „Europäische Verfahren“		
(1) Anzahl der Verfahren mit Betroffenheit (Art.56)	(1) 47	(1) **11**
(2) Anzahl der Verfahren mit Federführung (Art. 56)	(2) 16	(2) **2**
(3) Anzahl der Verfahren gemäß Kap. VII DS-GVO (Art. 60 ff.)	(3) 1011	(3) **982**
f. „Förmliche Begleitung bei Rechtsetzungsvorhaben“		
Hier werden pauschaliert als Gesamtzahl die von Parlament/ Regierung angeforderten und durchgeführten Beratungen genannt. Dies umfasst auch die Teilnahme in öffentlichen Ausschüssen und Stellungnahmen ggü. Gerichten	34	**35**

19.2
Ergänzende Erläuterungen zu Zahlen und Fakten

Die nachstehenden Darstellungen erläutern und ergänzen die Auswertungen in Kap. 19.1 auch im Vergleich mit dem Vorjahr und den weiteren Arbeitsgebieten im Berichtsjahr. Insgesamt stabilisiert sich die Zahl der Fälle sieben Jahre nach dem Inkrafttreten und fünf Jahre nach dem Wirksamwerden der DS-GVO auf einem sehr hohen Niveau. Dabei lässt sich beobachten, dass sich in vielen Bereichen die Qualität der Beschwerden und des Beratungsbedarfs verändert. Während zu Beginn Fragen nach eher formalen Anforderungen der DS-GVO im Vordergrund standen (etwa nach der Pflicht zur Bestellung eines Datenschutzbeauftragten, zu Informations- und Auskunftsrechten des Betroffenen), gehen viele Fragen, mit denen ich mich im Berichtsjahr zu befassen hatte, mehr in die Tiefe und werfen grundsätzliche Fragen auf.

Beschwerden und Beratungen

Auch wenn die Beschwerden und Beratungsanfragen im Zusammenhang mit COVID zurückgegangen sind, hat die Pandemie noch nachhaltigen Einfluss auf das Arbeitsaufkommen in meiner Behörde. Nach wie vor bringt der durch die Pandemie ausgelöste Digitalisierungsschub auch über die Pandemie hinaus ganz grundsätzlichen und sehr arbeitsintensiven Beratungsbedarf mit sich. So zeichnete sich im Berichtsjahr ab, dass technische Lösungen wie etwa Videokonferenztechnik, die in der Pandemie schnell zum Einsatz gebracht wurden, um Schulen, Hochschulen, Betriebe und die Verwaltung am Laufen zu halten, auch über die Pandemie hinaus zum Einsatz kommen. Da bei der Einführung Eile geboten war, mussten nun im Nachhinein die Anforderungen des Datenschutzes zur Geltung gebracht werden. Auch andere große Digitalisierungsprojekte wie zum Beispiel die Umsetzung des Onlinezugangsgesetzes, das Bund, Länder und Kommunen verpflichtet, bis 2022 ihre Verwaltungsleistungen über Verwaltungsportale auch online

anzubieten, schlagen in der Statistik nicht in dem Ausmaß zu Buche, wie sie meine Behörde tatsächlich beschäftigen.

In fast allen Bereichen, in denen meine Behörde tätig ist, spielt auch weiterhin die Frage nach den Anforderungen an DS-GVO-konforme internationale Datentransfers eine große Rolle.

Erfreulich ist, dass in einigen Bereichen die Beschwerdezahlen zurückgehen. Auch wenn es schwierig ist, hierfür die konkreten Ursachen zu benennen, beobachte ich etwa, dass es auf immer mehr Websites die Möglichkeit gibt, mit einem Mausklick alle für die Nutzung der Webseite nicht essenziellen Cookies abzulehnen. Im Bereich Handel, Gewerbe und Handwerk gehen die Beschwerden wegen nicht oder nicht korrekt beantworteter Auskunftsersuchen zurück. Solche Entwicklungen führe ich auf den erfreulichen Umstand zurück, dass sich in diesen und ähnlichen Fragen inzwischen eine gewisse Übung eingestellt hat, die weniger Anlass zur Beschwerde gibt.

Ein deutlicher Anstieg der Zahlen im Bereich Verkehr ist darauf zurückzuführen, dass zahlreiche Supermarktparkplätze von darauf spezialisierten Unternehmen mit Videotechnik überwacht werden.

Die nachfolgende Übersicht stellt die Zahl der Eingabe (Beschwerden und Beratungen) des Berichtsjahres im Vergleich zum Vorjahr dar:

Fachgebiete	Anzahl 2021			Anzahl 2022		
	Beschwerden	Beratungen	Eingaben insgesamt	Beschwerden	Beratungen	**Eingaben insgesamt**
Auskunfteien, Inkasso	634	11	645	485	2	**487**
Schule, Hochschule, Archive	132	811	943	97	200	**297**
e-Kommunikation, Internet	772	56	828	436	63	**499**
Beschäftigtendatenschutz	255	208	463	280	151	**431**
Videobeobachtung	413	74	487	408	80	**488**
Kreditwirtschaft	314	9	323	306	5	**311**
Handel, Handwerk, Gewerbe	212	53	265	135	15	**150**
Verkehr, Geodaten, Landwirtschaft	220	49	269	288	22	**310**

Gesundheit, Pflege	286	160	446	222	107	**329**
Betriebliche/ Behördliche DSB	7	180	187	8	193	**201**
Kommunen, Wahlen	142	146	288	108	143	**251**
Polizei, Justiz, Verfassungsschutz	141	90	231	153	100	**253**
Vereine, Verbände	72	73	145	97	35	**132**
Adresshandel, Werbung	197	5	202	302	4	**306**
Wohnen, Miete	77	48	125	80	76	**156**
Soziales	85	52	137	63	31	**94**
Versorgungsunternehmen	79	10	89	71	13	**84**
IT-Sicherheit, DV-Technik**	11	32	43	18	2	**20**
Versicherungen	94	12	106	51	7	**58**
Rundfunk, Fernsehen, Presse	25	2	27	22	0	**22**
Religionsgemeinschaften	2	3	5	12	1	**13**
Datenschutz außerhalb der EU	8	19	27	0	0	**0**
Forschung, Statistik	17	5	21	13	5	**18**
Ausländerrecht	3	7	10	2	7	**9**
Steuerwesen	14	3	17	18	4	**22**
Zertifizierung		1	1	0	0	**0**
Zensus				60	53	**113**
Sonstige Themen < 10 (z. B. Kammern, Ausländerwesen, Finanzwesen)	14	4	18	3	15	**18**
Zwischensumme Beschwerden und Beratungen	4.226	2.123	6.348	3.738	1.334	**5.072**

BCR-Verfahren mit deutscher oder europaweiter Federführung des HBDI	**40**	**10**
Meldungen von Datenpannen*	**2.016**	**1.754**

Gesamtsumme dokumentierter Eingaben	**8.404**	**6.836**
Zzgl. Summe telefonischer Beratungen und Auskünfte von mehr als 10 Min.**	**6.384**	**4.644**
Gesamtsumme dokumentierter + telefonischer Eingaben	**14.788**	**11.480**

*Telefonischen Nachfragen, die keinen schriftlichen Niederschlag finden, werden pauschaliert erfasst. Sie erfolgten als Beratungen, Auskünfte, Erläuterungen und Verständnisfragen zur DS-GVO u. Ä. sowohl zu allgemeinen Themen als auch zu spezifischen Fragestellungen, wie z. B. zur konkreten datenschutzrechtlichen Umsetzung der Corona-Verordnungen. Exemplarisch werden derartige Telefonate im November, als Monat ohne besondere Vorkommnisse, gezählt und als Durchschnittswert hochgerechnet.

**Weitere IT-Themen waren begleitend zu einer rechtlichen Anfrage oder einer Datenpannenmeldung zu prüfen und wurden deshalb nicht eigenständig gezählt.

Unberücksichtigt in den obigen Tabellen, aber nicht weniger erwähnenswerte Aufgaben und Themen, die im Berichtsjahr bearbeitet wurden, sind beispielsweise:

– **Tätigkeiten der internen Datenschutzbeauftragten beim HBDI**

  Es wurden **33** Auskunftsersuchen von Bürgerinnen und Bürgern zur Verarbeitung ihrer Daten beim HBDI bearbeitet sowie **10** entsprechende Beratungen durchgeführt.

– **Regelmäßige Beratungen**

Mit den intern bestellten Datenschutzbeauftragten aus verschiedenen öffentlichen Bereichen (z. B. von Ministerien, Städten und Kommunen, Hochschulen und den europäischen Datenschutz-Aufsichtsbehörden) wurden Austausche gepflegt und z. T. regelmäßige Beratungsleistungen erbracht.

– **Presse und Öffentlichkeitsarbeit**

Ich hatte im Jahr 2022 **90** Presseanfragen. Zahlreiche Veröffentlichungen und Hilfestellungen (z. B. zum Thema Videokonferenztechnik) wurden Verantwortlichen, Bürgern und Bürgerinnen auf meiner Homepage zur Verfügung gestellt.

– **Ausbildungsleistungen**

Es wurden **sieben** Referendare und Referendarinnen in ihren Wahl- bzw. Verwaltungsstationen ausgebildet.

– **Fortbildung und Vorträge**

Mitarbeitende meiner Behörde haben **33**, zum Teil mehrtägige, datenschutzrechtliche Schulungen, Seminare und Fortbildungen im öffentlichen und nichtöffentlichen Bereich durchgeführt. Ich selbst habe 15 öffentliche Vorträge zu unterschiedlichsten Datenschutzfragen gehalten sowie 14 wissenschaftliche Beiträge veröffentlicht.

– **Teilnahme an Konferenzen, Arbeitskreisen und Arbeitsgruppen**

Beratungen und Abstimmungen der Aufsichtsbehörden untereinander und in ihren Gremien auf Landes-, Bundes- und EU-Ebene, aber auch übergreifend mit Ansprechpartnern aus außereuropäischen Drittstaaten, sind mittlerweile essenziell für einen erfolgreichen Datenschutz in Hessen. Die Gremienarbeit ist mitunter sehr zeitintensiv, aber nicht mehr verzichtbar. Aufgrund der pandemischen Entwicklungen wurden persönliche Treffen oft durch Videokonferenzen ersetzt. Die Konferenzen der Datenschutzbeauftragten (DSK) und der Informationsfreiheitsbeauftragten (IFK) tagten ca. alle zwei Monate zu aktuellen Themen. Die DSK trifft sich jede Woche zu einem einstündigen Jour Fixe per Videokonferenz. Die Ergebnisse des Jahres 2022 sind im Anhang I aufgelistet, im Einzelnen aber auch auf der Homepage der Datenschutzkonferenz www.datenschutzkonferenz.de nachzulesen.

In den Arbeitskreisen der DSK ist meine Behörde in allen Bereichen beteiligt. Auch in den Unterarbeitsgruppen und Task Forces, die zu Spezialthemen eingesetzt werden, engagieren sich Mitarbeiterinnen und Mitarbeiter des HBDI. In den Arbeitskreisen Organisation und Struktur sowie Wissenschaft und Forschung führe ich den Vorsitz, in dem Arbeitskreis Auskunfteien und in der Task Force Forschungsdaten den Ko-Vorsitz. In zahlreiche EU-Gremien (z. B. International Transfers Expert Subgroup, Border, Travel, Law Enforcement Expert Subgroup, Financial Matters Expert Subgroup, CSC, SCG SIS II, SCG Eurodac, SCG VIS) konnte der HBDI seine Mitarbeit einbringen. Daneben erfolgten auch Unterstützungsleistungen an die EU-Kommission, wie z. B. durch die Teilnahme und Beiträge im Rahmen der Schengen-Evaluierung.

Abhilfemaßnahmen und Gerichtsverfahren

Abhilfemaßnahmen	**Anzahl 2021**	**Anzahl 2022**
(1) Warnungen (Art. 58 Abs. 2 a DS-GVO)	1	1
(2) Verwarnungen (Art. 58 Abs. 2 b DS-GVO)	28	37
(3) Anweisungen und Anordnungen (Art. 58 Abs. 2 c-g, j DS-GVO)	3	16
(4) Geldbußen (Art. 58 Abs. 2 i DS-GVO)	29	113
(5) Widerruf von Zertifizierungen (Art. 58 Abs. 2 h DS-GVO)	0	0
Gesamt	61	**167**

Gerichtsverfahren	**Anzahl 2021**	**Anzahl 2022**
Klagen gemäß Art. 78 Abs. 1 DS-GVO	24	13
Klagen gemäß Art. 78 Abs. 2 DS-GVO	2	4
Sonstige	8*	18*
Gesamt	34	**35**

* Davon 3 EuGH-Vorabentscheidungsverfahren, 11 Verfahren vor dem VGH in 2. Instanz, 3 Verfahren vor dem Bundesverfassungsgericht, 1 Eilverfahren.

Meldungen von Datenschutzverletzungen nach Art. 33 DS-GVO und § 60 HDSIG

Gesamtübersicht		
Grund	**Anzahl 2021**	**Anzahl 2022**
Fehlversand/Fehlzuordnung von Daten/Dokumenten	647	661
Hackerangriffe, Phishing, Schadsoftware, Sicherheitslücke	579	475
Verlust/ Diebstahl von Unterlagen, Geräten etc.	144	135
Unrechtmäßige Offenlegung/Weitergabe von Daten	121	189
Unzulässige Einsichtnahme (fehlerhafte Einrichtung von Zugriffsrechten u. a.)	98	90
Offener E-Mail-Verteiler	73	85
Missbrauch von Zugriffsrechten	44	69
Unzulässige Veröffentlichung	38	22
Nicht datenschutzkonforme Entsorgung	12	2
Unverschlüsselter E-Mail-Versand	7	12
Sonstige	253	14
Gesamt	**2.016**	**1.754**

am stärksten von Datenschutzverletzungen betroffene Bereiche	**Fälle 2021**	**Fälle 2022**
Kreditwirtschaft, Auskunfteien, Handel und Gewerbe	640	533
Beschäftigtendatenschutz	399	367
Gesundheitsbereich	288	267

Anhang zu I

1. Ausgewählte Entschließungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

1.1
Parlamentarische Untersuchungsausschüsse und Löschmoratorien: Datenschutz durch klare Vorgaben und Verarbeitungsbeschränkungen für Behörden vom 23.03.2022

https://www.datenschutzkonferenz-online.de/media/en/DSK_Entschliessung_Loeschmoratorien.pdf

1.2
Wissenschaftliche Forschung – selbstverständlich mit Datenschutz vom 23.03.2022

https://www.datenschutzkonferenz-online.de/media/en/DSK_6_Entschliessung_zur_wissenschaftlichen_Forschung_final.pdf

1.3
Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt“! vom 04.05.2022

https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Forderungen_zum_Beschaeftigtendatenschutz.pdf

1.4
Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vom 24.11.2022

https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

2. Ausgewählte Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

2.1
Zur Task Force Facebook-Fanpages vom 23.03.2022

https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Facebook_Fanpages.pdf

2.2
Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang vom 24.03.2022

https://www.datenschutzkonferenz-online.de/media/dskb/20222604_beschluss_datenminimierung_onlinehandel.pdf

2.3
Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht vom 13.04.2022

https://www.datenschutzkonferenz-online.de/media/dskb/2022_13_04_beschluss_DSK_20a_IfSG.pdf

2.4
Zusammenfassung des Berichts zur Arbeitsgruppe DSK „Microsoft-Onlinedienste“ vom 25.11.2022

https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

2.5
Festlegung zur Arbeitsgruppe DSK „Mikrosoft-Onlinedienste“ vom 25.11.2022

https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf

2.6
Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht“ vom 29.11.2022

https://www.datenschutzkonferenz-online.de/media/dskb/20221129_dskb_08_Beschluss_Verbrauchervorschriften.pdf

2.7
Abschlussbericht der Arbeitsgruppe DSK „Microsoft-Onlinedienste“ vom 07.12.2022

https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf

3. Ausgewählte Orientierungshilfen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

3.1
Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) vom 18.02.2022

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

3.2
FAQ zu Facebook-Fanpages vom 22.06.2022

https://www.datenschutzkonferenz-online.de/media/oh/20221121_oh_Fanpages_FAQ_Stand2022_11_21.pdf

3.3
Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 Version 1.1 vom 05.12.2022

https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf

3.4
Auswertung Konsultation zur Orientierungshilfe für Anbieter von Telemedien vom 05.12.2022

https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Auswertung_Konsultation_zur_Orientierungshilfe_fuer_Anbieter_von_Telemedien_final.pdf

II
Zweiter Teil
5. Tätigkeitsbericht zur Informationsfreiheit

Einführung Informationsfreiheit

Der vorliegende fünfte Tätigkeitsbericht zur Informationsfreiheit beschreibt und analysiert die Informationsfreiheit in Hessen im Jahr 5 seit der Regelung des Rechts eines allgemeinen und voraussetzungslosen Zugangs zu Akten der öffentlichen Verwaltung im Hessischen Datenschutz und Informationsfreiheitsgesetz (HDSIG). Seit dem 25. Mai 2018 sind dieser Anspruch, seine Einschränkungen und seine Durchsetzung im Vierten Teil des Gesetzes geregelt. Danach hat jede Person freien, voraussetzungslosen und kostenfreien Zugang zu Informationen, die in öffentlichen Stellen vorhanden sind. Dabei sind die Grundrechte Dritter zu achten und zu wahren. Diese betreffen die freie Selbstbestimmung über die eigenen personenbezogenen Daten und den Schutz schützenswerter Geheimnisse. Die betroffenen Dritten sind an dem Verfahren zur Freigabe der Informationen zu beteiligen. Ebenso können überwiegende öffentliche Belange wie etwa die öffentliche Sicherheit dem Zugang zu Informationen entgegenstehen. Um die Entscheidungsfindung der öffentlichen Stellen nicht zu beeinträchtigen, besteht der Informationszugang nur zu Akten aus abgeschlossenen Verfahren. Der Informationszugang ist bei öffentlichen Stellen ausgeschlossen, soweit er die Aufgabenerfüllung dieser Stellen behindern würde. Der Hessische Beauftragte für den Datenschutz nimmt auch das Amt des Hessischen Informationsfreiheitsbeauftragten wahr. Er ist Aufsichtsbehörde für die Umsetzung der Informationsfreiheit. Bürgerinnen und Bürger, die sich in ihrer Informationsfreiheit beeinträchtigt sehen, können sich mit einer Beschwerde an ihn wenden.

Dieser Regelung zur Umsetzung der Informationsfreiheit liegt folgende Zielsetzung zugrunde. In einer Demokratie darf die öffentliche Verwaltung kein geschlossener Bereich mehr sein, sondern muss ihr Handeln offen und transparent gestalten. Bürgerinnen und Bürger sollen zum einen die Möglichkeit haben, das Handeln der von ihnen gewählten und demnächst wieder zu Wahl anstehenden Leiter der öffentlichen Verwaltung nachzuvollziehen und zu bewerten. Sie sollen zum anderen informiert über die Wissensgrundlagen und Handlungsmöglichkeiten der Verwaltung sich daran beteiligen können, wie das Gemeinwohl durch Verwaltungshandeln konkretisiert wird. Sie sollen ihre Erfahrungen und ihre Vorstellungen in die aktuelle öffentliche Diskussion einbringen können. Durch das Recht auf Informationszugang gegenüber den öffentlichen Stellen erhalten Bürgerinnen und Bürger die Möglichkeit, unmittelbar Einblick in Vorgänge der öffentlichen Verwaltung zu nehmen. Sie können dadurch Entscheidungen der Verwaltung nachvollziehen, verstehen und leichter akzeptieren. Informationsfreiheit hat somit eine wichtige demokratische und rechtsstaatliche Funktion, stärkt die bürgerschaftliche Partizipation und die Kontrolle staatlichen Handelns.

Die Bundesrepublik Deutschland und dreizehn Bundesländer haben seit vielen Jahren Informationsfreiheitsgesetze, die den Informationszugang zu allen öffentlichen Stellen eröffnen. In einigen Bundesländern wurden diese Gesetze inzwischen zu Transparenzgesetzen weiterentwickelt, die die öffentliche Verwaltung verpflichten, von sich aus möglichst viele Informationen öffentlich zu stellen. Der aktuelle Koalitionsvertrag zwischen SPD, Bündnis90/Die Grünen und FDP sieht auch für den Bund ein Bundestransparenzgesetz vor (Koalitionsvertrag, S. 11).

Hessen war in dieser Entwicklung ein Nachzügler und hat erst vor fünf Jahren Informationsfreiheitsregelungen erlassen. Hierfür hat es ein eigenes Regelungskonzept gewählt, das nur von Sachsen übernommen worden ist und sich von den Regelungskonzepten aller anderen Informationsfreiheitsgesetze in Deutschland unterscheidet. Das Recht des allgemeinen Informationszugangs gilt in Hessen nicht für alle öffentlichen Stellen, sondern nur gegenüber der Landesverwaltung. Die Gemeinden und Landkreise, die die meisten Bürgerkontakte haben, sollen jeweils für sich selbst durch Satzung entscheiden, ob sie einen Informationszugang zu ihren Akten eröffnen. Solche Informationsfreiheitssatzungen haben bisher jedoch nur wenige Landkreise, Städte und Gemeinden verabschiedet. Für die meisten Verwaltungen in Hessen gilt daher noch keine Informationsfreiheit. Dementsprechend ist die Informationsfreiheit in der Praxis der Verwaltung in Hessen auch noch in geringem Maße ausgeprägt und muss sich künftig noch entwickeln (s. Kap. 2).

Inzwischen zeigt sich jedoch, dass die Daten, über die öffentliche Stellen verfügen, nicht nur für Demokratie und Rechtsstaat von großer Bedeutung sind, sondern auch Wirtschaft und Wissenschaft aus ihnen großen Nutzen ziehen könnten. Daher sehen alle Digitalisierungsstrategien auf Unions-, Bundes- und Landesebene vor, öffentliche Stellen zu verpflichten, alle geeigneten Daten öffentlich zur Verfügung zu stellen. Dementsprechend sieht der Koalitionsvertrag für den Bund eine Open Data-Regelung vor (Koalitionsvertrag, S. 17). In Hessen haben die Landtagsfraktionen von CDU und Bündnis 90/Die Grünen, nachdem der Entwurf für ein Open Data-Gesetz der FDP-Fraktion im vorherigen Berichtsjahr gescheitert ist (s. 4. Tätigkeitsbericht, Kap. 5), am 23. Januar 2023 einen Entwurf für ein Gesetz über offene Daten der Träger öffentlicher Verwaltung in den Gesetzgebungsprozess eingebracht (LT-Drs. 20/10379).

In der Union hat der Gesetzgeber in Art. 3 ff. des Open Governance Act vom 30. Mai 2022 (EU ABl. L 152 vom 3. Juni 2022, 1) Regelungen zur Weiterverwendung von Daten, die im Besitz öffentlicher Stellen sind, getroffen. Im Entwurf für einen Data Act vom 23. Februar 2022 hat die Europäische Kommission (COM(2022) 68 final) Vorschriften für einen fairen Datenzugang

und eine faire Datennutzung dieser Daten vorgeschlagen (s. hierzu auch 51. Tätigkeitsbericht zum Datenschutz, Kap. 1). Die Kommission strebt an, insgesamt 13 öffentliche Datenräume zu erzeugen, und hat dazu für den ersten Europäischen Datenraum zu Gesundheitsdaten am 3. Mai 2022 einen Verordnungsentwurf (COM(2022) 197/2) vorgelegt.

In diesen Entwicklungen zu Open Data geht es immer auch – sogar vorrangig – um die freie Nutzung von Daten öffentlicher Stellen. Soweit es sich um personenbezogene Daten handelt, erfordert dies immer auch eine Abstimmung mit den Anforderungen des Datenschutzes. Soweit dies gelingt, ist diese Entwicklung im Interesse des Grundrechtsschutzes, der Partizipation und der Entfaltungsmöglichkeiten in Wirtschaft, Wissenschaft und zivilgesellschaftlichem Engagement zu begrüßen. In diese Entwicklung passt das zurückhaltende Regelungsmodell der Informationsfreiheit in Hessen aber schwer hinein.

Als Informationsfreiheitsbeauftragter hatte ich im Berichtsjahr viele interessante Fragen zur Informationsfreiheit zu beantworten, unterstützte Bürgerinnen und Bürger bei der Durchsetzung ihres Anspruchs, beteiligte mich an der Diskussion zur rechtspolitischen Fortentwicklung der Informationsfreiheit und arbeitete mit anderen Informationsfreiheitsbeauftragten in Deutschland in der Konferenz der Informationsfreiheitsbeauftragten (IFK) zusammen. Zu diesen Tätigkeitsfeldern bietet der fünfte Tätigkeitsbericht eine kleine Auswahl. Er stellt die Entwicklung der Informationsfreiheit in Hessen im Berichtsjahr dar (Kap. 1), untersucht die Frage, wie Informationsfreiheit by Design die Umsetzung der Informationsfreiheit durch Technikgestaltung fördern kann (Kap. 2), stellt die Frage, warum kein Informationszugang zu Daten von Wirtschaftskammern gewährt wird (Kap. 3) und erläutert, wie mit exzessiven Informationsfreiheitsanträgen umgegangen werden kann (Kap. 4).

1. Entwicklung der Informationsfreiheit

Positiv ist, dass sich die öffentlichen Stellen des Landes recht gut auf den Informationszugang zu amtlichen Informationen und Aufzeichnungen eingestellt haben. Negativ ist zu bewerten, dass insbesondere der kommunale Bereich weitgehend vom Informationszugang ausgenommen ist. Vor allem in diesem Punkt besteht legislativer, zumindest aber kommunaler Handlungsbedarf.

Informationsfreiheitsbeauftragter als „Beschwerdestelle“

Als Informationsfreiheitsbeauftragter befasse ich mich insbesondere mit Eingaben von Bürgerinnen und Bürgern, die sich in ihrem Recht auf Informationszugang verletzt sehen.

In § 89 Abs. 1 S. 1 HDSIG ist geregelt, dass jeder, der sich in seinen Informationsfreiheitsrechten nach Maßgabe der §§ 80 ff. HDSIG verletzt sieht, mich als Informationsfreiheitsbeauftragten „anrufen“ kann. Von diesem Recht machten die Bürgerinnen und Bürger jährlich etwa im mittleren zweistelligen Bereich Gebrauch. Bei Beratungsanfragen, meistens von Behörden, verhält es sich zahlenmäßig ähnlich.

Werde ich im Sinne von § 89 Abs. 1 S. 1 HDSIG angerufen, befasse ich mich mit dem Beschwerdegegenstand. Komme ich zu dem Ergebnis, dass der Informationszugang zu Unrecht verwehrt wird, dann kann ich nach § 89 Abs. 3 S. 3 HDSIG die öffentliche Stelle auffordern, diesen Verstoß binnen einer bestimmten Frist zu beheben. Diese Aufforderung ist rechtlich aber kein (verbindlicher) Verwaltungsakt im Sinne von § 35 HVwVfG, sondern ein Appell an die Stelle, der durch die nach § 89 Abs. 3 S. 4 HDSIG gesetzlich vorgesehene Benachrichtigung der Aufsichtsbehörde der öffentlichen Stelle freilich einen gewissen Nachdruck enthält.

Im Großen und Ganzen werden Informationszugangsanträge aus Sicht des Informationsfreiheitsbeauftragten von den öffentlichen Stellen korrekt beschieden; öfter kommt es zu Verstößen gegen die nach § 87 HDSIG gesetzlich vorgesehenen Bescheidungsfristen. Inhaltlich verhalten sich die öffentlichen Stellen aber meistens korrekt.

Bislang verwaltungsgerichtlich noch nicht geklärt ist die Frage, ob im Fall einer Ablehnung durch mich als Informationsfreiheitsbeauftragten gegenüber dem Beschwerdeführer, nach § 89 Abs. 3 S. 3 HDSIG gegen die Stelle vorzugehen, der Beschwerdeführer anschließend gegen mich gerichtlich vorgehen kann. Dagegen spricht, dass der Gesetzgeber in § 87 Abs. 5 HDSIG verwaltungsgerichtlichen Rechtsschutz nur gegen die Stelle selbst,

von der Informationen begehrt werden, vorgesehen hat, nicht jedoch in § 89 HDSIG gegenüber dem Informationsfreiheitsbeauftragten.

Ganz abgesehen davon dürfte aber auch ohnehin für ein gerichtliches Vorgehen gegen den Informationsfreiheitsbeauftragten das Rechtsschutzbedürfnis fehlen, weil dieser ja, wie gesagt, ohnehin nicht die Stelle, um die es geht, zur Auskunft verpflichten kann. Diese Verpflichtung kann aber gerade im Fall eines verwaltungsgerichtlichen Vorgehens gegen die öffentliche Stelle selbst im Verfahren nach § 87 Abs. 5 HDSIG im Fall der Begründetheit der Klage erwirkt werden. Das spricht dafür, dass der gerichtliche Rechtsschutz auf die öffentliche Stelle konzentriert und der Informationsfreiheitsbeauftragte insoweit ausgenommen ist. Natürlich kann das Verwaltungsgericht im Rahmen seiner Prozessgestaltung betreffend die Klage gegen eine öffentliche Stelle mich als Informationsfreiheitsbeauftragten hinzuziehen.

Unzureichende Eröffnung des Informationszugangs

Personen, die sich bei mir als Informationsfreiheitsbeauftragten über nicht gewährten Informationszugang beschwerten, musste ich oft mitteilen, dass der kommunale Bereich, anders als in den anderen Bundesländern, vom Gesetzgeber – zulasten der Informationsfreiheit – „privilegiert“ wird. Nur wenn eine Kommune gemäß § 81 Abs. 1 Nr. 7 HDSIG in einer kommunalen Satzung bestimmt, dass auf sie auch der Vierte Teil des HDSIG anzuwenden ist, gelten die §§ 80 ff. HDSIG auch für sie.

§ 81 HDSIG

(1) Nach Maßgabe des § 2 Abs. 1 bis 3 gelten die Vorschriften über den Informationszugang auch für

(…)

7. die Behörden und sonstigen öffentlichen Stellen der Gemeinden und Landkreise sowie deren Vereinigungen ungeachtet ihrer Rechtsform, soweit die Anwendung des Vierten Teils durch Satzung ausdrücklich bestimmt wird.

Diese Rechtslage stößt bei den Bürgerinnen und Bürgern, die sich an mich wenden, schon seit Beginn der Informationsfreiheit in Hessen im Jahr 2018 berechtigterweise auf großes Unverständnis.

Die gesetzliche Sonderbehandlung des kommunalen Bereichs hätte sich freilich dann für die Informationsfreiheit – jedenfalls in der Praxis – nicht sonderlich nachteilig ausgewirkt, wenn die Kommunen ganz überwiegend den Informationszugang eröffnende Satzungsregelungen im Sinn von § 81 Abs. 1 Nr. 7 HDSIG getroffen hätten.

Leider ist aber das Gegenteil der Fall: In Hessen gibt es 21 Landkreise und nur vier davon haben seit 2018 den Informationszugang eingeführt (Marburg-Biedenkopf, Groß-Gerau, Darmstadt-Dieburg und der Main-Taunus-Kreis), also fast genau nur ein Fünftel der Landkreise. Bei den größeren Städten sieht es für die Informationsfreiheit auch nicht besser aus: Nur Wiesbaden, Kassel und Darmstadt haben Informationsfreiheit. Immerhin hat die Landeshauptstadt den Informationszugang, also anders als die anderen Kommunen, nicht auf den Selbstverwaltungsbereich beschränkt, sondern auch die Weisungs- und Auftragsangelegenheiten einbezogen.

Aber nicht nur der kommunale Bereich, sondern auch die Ausgestaltung der Informationsfreiheit betreffend den Landesbereich bietet nach wie vor Anlass zur Kritik: Insbesondere die rigorosen Ausschlüsse des Informationszugangs betreffend die Polizeibehörden (§ 81 Abs. 2 Nr. 1 HDSIG) und die Wirtschaftskammern (§ 81 Abs. 2 Nr. 3 HDSIG) sind hier zu nennen.

In meiner Eigenschaft als Hessischer Informationsfreiheitsbeauftragter appelliere ich daher an den Landtag und die Landesregierung ein weiteres Mal, das hessische Informationsfreiheitsrecht wie in den meisten anderen Bundesländern insbesondere in diesen Punkten zu überprüfen. Zugleich appelliere ich an den kommunalen Bereich, Informationszugang, soweit noch nicht geschehen, per Satzung zu eröffnen, solange der Satzungsvorbehalt gesetzlich in Kraft bleibt. Vorbildfunktion hat hier die Landeshauptstadt Wiesbaden, die den Informationszugang uneingeschränkt eröffnet hat.

2. Informationsfreiheit by Design

Im Bereich der Informationsfreiheit wird derzeit diskutiert, den möglichen Zugang zu amtlichen Informationen bei der Durchführung von Digitalisierungsprojekten von Anfang an mit zu bedenken. Der Beitrag beleuchtet, worum es sich bei der sogenannten „Informationsfreiheit by Design" handelt und welche Chancen und Risiken öffentliche Stellen dabei bedenken sollten.

In meinem letzten Tätigkeitsbericht habe ich dargestellt, warum die Bereitstellung und Verwendung von Open Data zu fördern ist (4. Tätigkeitsbericht, Kap. 5). In dem Zusammenhang habe ich erwähnt, dass die Europäische Datenstrategie die EU zu einem Vorbild für eine digitale Gesellschaft machen soll. Die Bereitstellung von Open Data ist als sogenannte „Bringschuld" der öffentlichen Hand zu sehen, wenn es um die Bereitstellung von Informationen durch staatliche Stellen geht. Dem steht die Informationsfreiheit als sogenannte „Holschuld" der Bürgerinnen und Bürger gegenüber. Um diesen die Ausübung von Informationsfreiheitsrechten zu erleichtern und die Transparenz des öffentlichen Verwaltungshandelns zu fördern, wird das Konzept der sogenannten „Informationsfreiheit by Design" diskutiert. Die Konferenz der Informationsfreiheitsbeauftragten (IFK) hat in ihrer 37. Sitzung am 12. Juni 2019 dazu ein Positionspapier erstellt (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-08/positionspapier_informationsfreiheit_by_design.pdf). Ähnlich dem Grundgedanken des Art. 25 DS-GVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) sollten Anforderungen an die Informationsfreiheit bereits von Anfang an durch öffentliche Stellen in die Gestaltung ihrer IT-Systeme und organisatorischen Prozesse einfließen. Nach der von der IFK verwendeten Definition zählt zu „Informationsfreiheit by Design" die Gesamtheit technischer und organisatorischer Instrumente unter Berücksichtigung des Stands der Technik, die der Wahrnehmung und Erfüllung der Rechte nach den Informationsfreiheits- und Informationszugangsgesetzen, Umweltinformationsgesetzen und Transparenzgesetzen des Bundes und der Länder dienen. Einige Bundesländer haben das Konzept der „Informationsfreiheit by Design" bereits in ihre landesrechtlichen Regelungen aufgenommen. Dies ist in Hessen bislang nicht der Fall.

Meine Behörde arbeitet derzeit zusammen mit anderen Vertreterinnen und Vertretern der IFK an der Entwicklung von Prinzipien für die „Informationsfreiheit by Design" mit. Diese Prinzipien werden zu gegebener Zeit nach Fertigstellung veröffentlicht werden. Sie richten den Fokus einerseits auf

organisatorische Maßnahmen, andererseits auf informationsfreundliche technische Voreinstellungen.

Grundsätzlich liegen die Chancen der „Informationsfreiheit by Design“ darin, dass die Transparenz der öffentlichen Hand weiter gefördert wird. Jedoch gibt es auch oft Risiken: Zum einen ist die Überprüfung der Datenqualität für Bürgerinnen und Bürger nur schwer möglich. Zum anderen sind die Daten ohne Metainformationen nicht verständlich. Stellt man den interessierten Anfragenden nur Spalten mit Daten zur Verfügung, ohne weitere Informationen zu deren Bedeutung zu liefern, sind die Daten nicht verwertbar. Diese Metainformationen sollten für „Informationsfreiheit by Design“ auch von Anfang an mit bedacht werden. Verfügt die Behörde über einen Informationsvorsprung, der für die Interpretation oder Auswertung der Daten relevant ist, sollte sie der Antragstellerin und dem Antragsteller die notwendigen Informationen zur Verfügung stellen. Zudem muss sich die informationspflichtige Stelle darüber bewusst sein, dass mit technischen Mitteln verfügbar gemachte und bereitgestellte Daten oft verkettbar sind und damit ein Personenbezug wiederhergestellt werden könnte oder andere Rechte Dritter wie z. B. Geschäftsgeheimnisse verletzt werden könnten. Dies muss besonders bei großen Datenmengen berücksichtigt werden, die über maschinenlesbare Schnittstellen (automatisierbar) abrufbar gemacht werden. Der Datenschutz und die Rechte Dritter dürfen durch die Informationsfreiheit nicht ausgehebelt werden – auch dann nicht, wenn die „Informationsfreiheit by Design“ gewährleistet wird.

3. (Kein) Informationszugang gegenüber Wirtschaftskammern

Der absolute Ausschluss des Informationszugangs gegenüber den Industrie- und Handelskammern sowie Handwerkskammern ist rechtlich nicht stringent. Die im hessischen Informationsfreiheitsrecht ohnehin vorhandenen Regelungen zur Wahrung der Persönlichkeitsrechte, der Geschäftsgeheimnisse und anderer Rechte reichen aus. Auch die Kammern für z. B. Rechtsanwälte, Notare und Ärzte kommen mit diesen Regelungen aus.

Die aktuelle Rechtslage

Der hessische Landesgesetzgeber hat sich im Unterschied zu anderen Bundesländern entschieden, die Industrie- und Handelskammern sowie die Handwerkskammern vollständig vom Informationszugang auszunehmen. Diese Regelung findet sich in § 81 Abs. 2 Nr. 3 HDSIG.

§ 81 HDSIG
(2) Die Vorschriften des Vierten Teils gelten nicht für
(…)
3. die Industrie- und Handelskammern und die Handwerkskammern,
(…)

Bewertung

Im Gesetzgebungsverfahren wurde durchaus gesehen (LT-Drucks. 19/5728, S. 150 f.), dass die im hessischen Informationsfreiheitsrecht ohnehin vorhandenen Schutzvorschriften etwa in § 82 Nr. 3 und 4 sowie § 83 HDSIG zugunsten der Wahrung des Datenschutzes und der Wahrung von Geschäftsgeheimnissen der Kammermitglieder an sich ausreichend sind.

Das dürfte nämlich auch der Grund sein, dass andere Kammern im Bereich der berufsständischen Selbstverwaltung (Anwaltskammer, Notarkammer und auch die Ärztekammer) dem Informationszugang nach Maßgabe der §§ 80 ff. HDSIG unterliegen.

So sind seit der Geltung des Hessischen Informationsfreiheitsrechts dem Hessischen Informationsfreiheitsbeauftragen dementsprechend infolge von Informationsfreiheitsbeschwerden gemäß § 89 HDSIG Informationszugangsanträge bekannt geworden, die von berufsständischen Kammern in Hessen nach Maßgabe der §§ 80 ff. HDSIG beschieden werden mussten.

Dass die Wirtschaftskammern insofern privilegiert sind, dass ihnen gegenüber der Informationszugang absolut ausgeschlossen ist, lässt sich im Vergleich zu den anderen Kammern nicht rechtfertigen.

Von daher ist es im Sinn einer angemessenen Gleichbehandlung der Kammern und vor allem eines hinreichenden Informationszugangs geboten, die Industrie- und Handelskammern sowie die Handwerkskammern den anderen Kammern gleichzustellen, bei denen ja der Informationszugang nach Maßgabe der §§ 80 ff. HDSIG von vornherein eröffnet worden ist. Auch in den meisten anderen Bundesländern unterliegen sämtliche berufsständischen Kammern dem Informationszugang.

Diesen Informationszugang ansprechend hat die Konferenz der Informationsbeauftragten von Bund und Ländern bereits im Jahr 2015 folgende Entschließung verfasst:

„Auch Kammern sind zur Transparenz verpflichtet

Immer wieder verweigern sich berufsständische Kammern den Transparenzanforderungen der jeweiligen Informationszugangsgesetze.

Berufsständische Kammern nehmen hoheitliche Aufgaben auf Bundes- und Länderebene wahr. Für die jeweiligen Berufsgruppen besteht eine gesetzliche Pflicht zur Mitgliedschaft, die Kammern sind für Berufszulassungen zuständig und haben oft weitgehende Sanktionsmöglichkeiten.

Informationen, die im Rahmen ihrer Tätigkeit anfallen, unterfallen den Informationszugangsgesetzen von Bund und Ländern. Dies gilt auch für Jahresabschlüsse und Angaben zu Einnahmen, Ausgaben und Rückstellungen der Kammern. Für die Verpflichtung der Kammern ist es unerheblich, ob Antragstellende Kammermitglieder sind und welche Motive zur Antragstellung führten. Öffentlich-rechtliche Körperschaften befinden sich in weiten Bereichen nicht in Konkurrenz zu Marktteilnehmern – Wettbewerbsnachteile können sich zumeist nicht ergeben. Folglich stehen schutzwürdige Betriebs- und Geschäftsgeheimnisse einem Informationszugang in der Regel nicht entgegen.

Ansprüche auf Informationszugang sind unverzüglich, spätestens jedoch innerhalb der in den Informationszugangsgesetzen des Bundes bzw. der Länder genannten Fristen zu erfüllen. Eine Entscheidung darf nicht auf Gremiensitzungen verschoben, sondern sollte im Rahmen der regulären Geschäftsführung getroffen werden. Im Übrigen sind transparenzpflichtige Informationen der berufsständischen Kammern in den bereits vorhandenen Informationsregistern zu veröffentlichen.

> Die Informationsfreiheitsbeauftragten in Deutschland fordern daher die berufsständischen Kammern auf, ihren Transparenzverpflichtungen nachzukommen.“

Ich fordere daher den Landtag und die Landesregierung auf, Informationszugang gegenüber den Wirtschaftskammern in Hessen überhaupt erst einmal gesetzlich zu eröffnen.

4. Exzessive Informationsfreiheitsanträge

Exzessive Informationsfreiheitsanträge müssen von den öffentlichen Stellen nach Maßgabe des hessischen Informationsfreiheitsrechts nicht beauskunftet werden. Dies ist auch deshalb sachgerecht, weil selbst im Datenschutzrecht die (immerhin von einer Datenverarbeitung) Betroffenen keinen Anspruch auf Auskunft im Fall exzessiver Auskunftsanträge haben.

Ein Beispiel

Anfang 2022 informierte mich das Regierungspräsidium Darmstadt über folgenden Informationsfreiheitsantrag, der bei ihm eingegangen war, und bat um Beratung. Der Antrag hatte folgende Fassung:

> „Es wird beantragt, mir den Zugang zu Informationen zu folgenden Fragen zu gewähren:
> 1. Wie viele externe Dienstleister hat Ihre Behörde im Jahre 2019 und 2020 beauftragt?
> 2. Welche konkreten externen Dienstleister wurden beauftragt?
> 3. Für welche konkreten Aufgaben/Beratungen/Dienstleistungen wurden die Externen beauftragt?
> 4. Welche jeweiligen Kosten (Summe in Brutto, Netto und Umsatzsteuer) sind für die jeweiligen Externen für welche jeweilige Aufgabe/Beratung/Dienstleistung entstanden?
> 5. Welchen Inhalt hatten die jeweiligen Verträge der jeweiligen Externen zu den jeweiligen Aufgaben/Beratung/Dienstleistung?“

Das Regierungspräsidium Darmstadt war der Ansicht, dass die Beauskunftung dieses Antrages mit einem unverhältnismäßigem Aufwand verbunden sei, und es beabsichtigte deshalb, diesen Antrag auf Informationszugang negativ zu bescheiden. Dagegen habe ich keine Einwände erhoben, denn das hessische Informationsfreiheitsrecht sieht in § 85 HDSIG für solche Konstellationen ein ablehnendes Vorgehen der öffentlichen Stelle ausdrücklich vor.

§ 85 HDSIG

„(2) (…) Ein Antrag, der auf allgemeines Behördenhandeln gerichtet ist und sich auf Informationen bezieht, die aus einer Vielzahl von Aktenvorgängen oder Informationsträgern zusammengetragen werden müssen, kann abgelehnt werden, wenn der Informationszugang nur mit unverhältnismäßigem Verwaltungsaufwand möglich wäre.“

Diese Vorschrift im Hessischen Informationsfreiheitsrecht ist durchaus sinnvoll. Denn selbst im Datenschutzrecht, bei dem es ja immerhin um die Verarbeitung personenbezogener Daten der Betroffenen geht, muss gemäß Art. 12 Abs. 5 DS-GVO exzessiven Auskunftsanträgen nicht entsprochen werden.

Art. 12 DS-GVO

(5) (…) Bei … exzessiven Anträgen einer betroffenen Person kann der Verantwortliche … sich weigern, aufgrund des Antrags tätig zu werden.

Wenn also selbst im Datenschutzrecht, wenn es um die Verarbeitung personenbezogener Daten der Betroffenen geht, die verantwortlichen Stellen exzessiven Anträgen – trotz der mit der Verarbeitung der Daten einhergehenden Grundrechtsbetroffenheit – nicht nachkommen müssen, dann ist es erst recht angebracht, dies auch im Informationsfreiheitsrecht so vorzusehen, weil dort die Informationsfreiheitsanträge ja grundsätzlich „voraussetzungslos“, also ohne rechtliche Betroffenheit, zulässig sind und gem. § 87 HDSIG nach Maßgabe der §§ 80 ff. HDSIG beschieden werden müssen.

Exzessive Informationsfreiheitsanträge und kommunale Satzungsautonomie

Im Anschluss an den Vorgang beim Regierungspräsidium Darmstadt stellte sich bei mir infolge vieler kommunaler (Beratungs-)Anfragen heraus, dass der Antragsteller zumindest in Hessen seinen Antrag flächendeckend auch an andere hessische Kommunen versendet hatte. Da die meisten Kommunen in Hessen keine Informationsfreiheitssatzung im Sinn von § 81 Abs. 1 Nr. 7 HDSIG erlassen haben, sind sie insoweit nicht einmal zur Bescheidung des Antragstellers verpflichtet (gewesen), da die zur Bescheidung verpflichtende Regelung des § 87 HDSIG für diese Kommunen ohne Satzung ebenfalls nicht gilt. Gleichwohl habe ich den Kommunen vorgeschlagen, den Antragsteller auf die Nichtgeltung des Informationsfreiheitsrechts bei Kommunen ohne Satzung hinzuweisen.

Dass exzessive Anträge auf Informationszugang im kommunalen Bereich für die kommunale Motivation, Informationsfreiheitssatzungen zu erlassen, nicht förderlich sind, ist evident und für mein entgegengesetztes Anliegen kontraproduktiv, für eine Ausbreitung der Informationsfreiheit auf kommunaler Ebene zu plädieren. In diesem Zusammenhang kann ich aber immerhin positiv erwähnen, dass nunmehr auch die Landeshauptstadt Wiesbaden eine Informationsfreiheitssatzung erlassen hat.

5. Arbeitsstatistik Informationsfreiheit

Im Vergleich zum Vorjahr ergab sich ein Rückgang an Beschwerden und ein Anstieg an Beratungen.

IFG	2021	2022
Beschwerden	71	**46**
Beratungen	52	**64**

ANHANG zu II

1. Ausgewählte Entschließungen der 42. und 43. Konferenz der Informationsfreiheitsbeauftragten in Deutschland

1.1
Keine Umgehung der Informationsfreiheit durch Errichtung von Stiftungen bürgerlichen Rechts! vom 30.06.2022

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/42_Konferenz_Stiftungen-buergerliches-Recht.html?nn=253070

1.2

SMS in die Akte: Behördliche Kommunikation unterliegt umfassend den Regeln der Informationsfreiheit! vom 30.06.2022

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/42_Konferenz_SMS-in-die-Akte.html?nn=253070

1.3
Niedersachsen: Die Zeit für ein Transparenzgesetz ist gekommen vom 26.10.2022

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/42_43_Entschlie%C3%9Fung-Transparenzgesetz.html?nn=253070

Verzeichnis der Abkürzungen

Abs.	Absatz
AES	Advanced Encryption Standard
AGG	Allgemeines Gleichbehandlungsgesetz
AIA	Artificial Intelligence Act
App	Mobile Applikation
AO	Abgabenordnung
App	Mobile Applikationen
ArbR	Arbeit und Recht
Art.	Artikel
ATD	Antiterrordatei
ATDG	Antiterrordateigesetz
Aufl.	Auflage
AVV	Auftragsverarbeitungsvertrag
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
BAG	Bundesarbeitsgericht
BCR	Binding Corporate Rules (verbindliche interne Datenschutzvorschriften)
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BKA	Bundeskriminalamt
BMG	Bundesmeldegesetz
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bspw.	Beispielsweise
BTLE	Borders, Travel & Law Enforcement (Subgroup)
Buchst.	Buchstabe

BVerwG	Bundesverwaltungsgericht
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
bzw.	beziehungsweise
ca.	Circa
COVID-19	Coronavirus-Krankheit-2019
COVID-19	Coronavirus SARS-CoV-2
ComVor	Computergestützte Vorgangsbearbeitung –Vorgangsbearbeitungssystem der Polizei
CRIME	Criminal Research Investigation Management Software der Polizei
DA	Data Act
DGA	Data Government Act
d. h.	das heißt
DMA	Digital Market Act
DAS	Digital Services Act
DS-GVO, DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder; kurz: Datenschutzkonferenz
DSO	Datenschutzordnung des Hessischen Landtags
EDSA	Europäischer Datenschutzausschuss
E-Mail	electronic mail
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EWO	Einwohnermeldeamt
f.	folgende
ff.	folgende (Seiten) / fortfolgende
FITKO	Föderale IT-Kooperation

FristenVO	Verordnung zur Festlegung der Regeln für die Fristen, Daten und Termine
gem.	gemäß
GG	Grundgesetz
ggf.	gegebenenfalls
GVBl.	Gesetz- und Verordnungsblatt
GWG	Geldwäschegesetz
HAKrWG	Hessisches Ausführungsgesetz zum Kreislaufwirtschaftsgesetz
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
Hessen3C	Hessen CyberCompetenceCenter
HGB	Handelsgesetzbuch
HKHG	Hessisches Krankenhausgesetz
HKRG	Hessischen Krebsregistergesetz
HLKA	Hessisches Landeskriminalamt
HMinD	Hessische Ministerin für Digitale Strategie und Entwicklung
HMSI	Hessisches Ministerium für Soziales und Integration
HMWK	Hessisches Ministerium für Wissenschaft und Kunst
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HSOG-E	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung - Entwurf
HVSG	Hessisches Verfassungsschutzgesetz
HSL	Hessisches Statistisches Landesamt
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
HZD	Hessische Zentrale für Datenverarbeitung
IBAN	Internationale Bankkontonummer
IDM	Identitätsmanagement
i. d. R.	in der Regel

IFK	Informationsfreiheitskonferenz
IfSG	Infektionsschutzgesetz
INA	Innenausschuss
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
i. S. d.	im Sinne der/des
i. S. e.	im Sinne einer/eines
i. V. m.	in Verbindung mit
IP	Internet Protocol
IT	Informationstechnik
IT	Information Technologie
IT-Dienst	Informationstechnischer Dienst
IT-Laboratorium	Informationstechnisches Laboratorium
IT-System	Informationstechnisches System
Kap.	Kapitel
Kfz	Kraftfahrzeug
KrWG	Kreislaufwirtschaftsgesetz
lit.	Litera, Buchstabe
LfV Hessen	Landesamt für Verfassungsschutz Hessen
LT-Drs.	Landtagsdrucksache (Hessen)
NJW	Neue Juristische Wochenschrift
NZA	Neue Zeitschrift für Arbeitsrecht
NZV	Neue Zeitschrift für Verkehrsrecht
Nr.	Nummer
o. Ä.	oder Ähnliches
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWASP	Open Web Application Security Projects
OWiG	Gesetz über Ordnungswidrigkeiten
PDF	Portable Document Format
Pentest	Penetrationstest
POLAS	Polizeiauskunftssystem

PsychKHG	Hessisches Gesetz über Hilfen bei psychischen Krankheiten
QR-Code	Quick Response Code
Rdnr./Rn.	Randnummer
Rs.	Rechtssache
S.	Seite *oder* Satz
s.	siehe
s. a.	siehe auch
SCG	Supervision Coordination Group (SIS II SCG; die Gruppe besteht aus Vertretern der nationalen Aufsichtsbehörden der Mitgliedstaaten sowie dem Europäischen Datenschutzbeauftragten)
SIS II	Schengen Information System II
SIS II-Beschluss	Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation
S/MIME	Secure / Multipurpose Internet Mail Extensions
sog.	sogenannte/sogenannter/sogenanntes
SPH	Schulportal Hessen
StBerG	Steuerberatungsgesetz
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
s. u.	siehe unten
TB	Tätigkeitsbericht
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikation
TKÜ	Telekommunikationsüberwachung
TLS	Transport Layer Security
TOM	Technisch-organisatorische Maßnahmen
TTDSG	Telekommunikation-Telemedien-Datenschutzgesetz
u. a.	unter anderem
UAbs.	Unterabsatz

ULD SH	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
URL	Uniform Resource Locator
Urt.	Urteil
US(A)	Vereinigte Staaten von Amerika
UWG	Gesetz gegen den unlauteren Wettbewerb
VG	Verwaltungsgericht
vgl.	vergleiche
VKS	Videokonferenzsystem
VPN	Virtual Private Network
VwVfG	Verwaltungsverfahrensgesetz
WP	Working Paper
WP	Article 29 Data Protection Working Party
WWW	World Wide Web
z. B.	zum Beispiel
ZenDiS	Zentrum für Digitale Souveränität in der öffentlichen Verwaltung
ZensusG	Zensusgesetz
ZEVIS	Zentrales Verkehrsinformationssystem

Register der Rechtsvorschriften

Zitiert werden die jeweils zum Bearbeitungszeitpunkt geltenden Fassungen.

Gesetz/Vorschrift	Fundstelle(n)
AO	Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61), zuletzt geändert durch Artikel 1 des Gesetzes vom 12. Juli 2022 (BGBl. I S. 1142)
AGG	Allgemeines Gleichbehandlungsgesetz vom 14. August 2006 (BGBl. I S. 1897), zuletzt geändert durch Artikel 4 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2510)
ATDG	Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern (Antiterrordateigesetz ATDG)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 12 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 20.11.2019 (BGBl. I S. 1626)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 12 Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU vom 20.11.2019 (BGBl. I S. 1626)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 10 G vom 23. Juni 2021 (BGBl. I S. 1858, 1968)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 10 G vom 23. Juni 2021 (BGBl. I S. 1858, 1968, ber. 2022 I S. 1045)
BDSG a. F.	Bundesdatenschutzgesetz a.F. in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66), zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618) m.W.v. 09.11.2017. Außer Kraft getreten am 25.05.2018 aufgrund Gesetzes vom 30.06.2017 (BGBl. I S. 2097)
BGB	Bürgerliches Gesetzbuch i. d. F. vom 02.01.2002 (BGBl. I S. 42)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 02.01.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 2 des Gesetzes vom 21. Dezember 2021 (BGBl. I. S. 5252)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 02.01.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 9 des Gesetzes vom 07. November 2022 (BGBl. I. S. 1982)

BJagdG	Bundesjagdgesetz vom 29.09.1976 (BGBl. I S. 2849), zuletzt geändert durch Artikel 291 der Verordnung vom 19.06.2020 (BGBl. I S. 1328)
BKAG	Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), zuletzt geändert durch Artikel 3 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2632)
BMG	Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084), zuletzt geändert durch Artikel 4 des Gesetzes vom 21. Juli 2022 (BGBl. I S. 1182)
BMG	Bundesmeldegesetz vom 03.05.2013 (BGBl. I S. 1084), zuletzt geändert durch Art. 22 des Gesetzes vom 19.12.2022 (BGBl. I S. 2606)
BNatSchG	Gesetz über Naturschutz und Landschaftspflege (Bundesnaturschutzgesetz) vom 29.06.2009 (BGBl. I S. 2542), zuletzt geändert durch Artikel 3 des Gesetzes vom 8.12.2022
BORA	Berufsordnung für Rechtsanwälte, zuletzt geändert durch Beschluss vom 06.05.2019
BWaldG	Bundeswaldgesetz vom 02.05.1975 (BGBl. I S. 1037), zuletzt geändert durch Artikel 112 des Gesetzes vom 10.08.2021 (BGBl. I S. 3436)
DSO	Datenschutzordnung des Hessischen Landtags, Anlage 4 zur Geschäftsordnung des Hessischen Landtags vom 16.12.1993 (GVBl. I S. 628), zuletzt geändert durch Beschluss des Landtags vom 23.02.2022 (GVBl. S. 130)
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. EU L 119 S. 1)
GG	Grundgesetz Vom 23. Mai 1949, zuletzt geändert durch Art. 1 ÄndG (Art. 82) vom 19.12.2022 (BGBl. I S. 2478)
GWG	Geldwäschegesetz vom 23.06.2017 (BGBl. I S. 1822), zuletzt geändert durch Artikel 23 des Gesetzes vom 22.02.2023 (BGBl. 2023 I Nr. 51)
HAKrWG	Hessisches Ausführungsgesetz zum Kreislaufwirtschaftsgesetz vom 6. März 2013, zuletzt geändert durch Artikel 15 des Gesetzes vom 3. Mai 2018 (GVBl. S. 82)
HGB	Handelsgesetzbuch Gesetz vom 10.05.1897 (RGBl. I S. 219), zuletzt geändert durch Gesetz vom 15.07.2022 (BGBl. I S. 1146) m. W. v. 01.08.2022
HGO	Hessische Gemeindeordnung in der Fassung der Bekanntmachung vom 7. März 2005, geändert durch Art. 3 des Gesetzes vom 11. Dezember 2020 (GVBl. S. 915)

HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 03.05.2018 (GVBl. S. 82), in Kraft gesetzt am 25.05.2018, geändert durch Art. 9 des Gesetzes vom 15. November 2021 (GVBl. S. 718, 729)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 03.05.2018 (GVBl. S. 82), in Kraft gesetzt am 25.05.2018, geändert durch Art. 5 des Gesetzes vom 12.09.2018 (GVBl. S. 570)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 03.05.2018 (GVBl. S. 82), in Kraft gesetzt am 25.05.2018, geändert durch Art. 9 des Gesetzes vom 15. November 2021 (GVBl. S. 718, 729)
HKHG	Zweites Gesetz zur Weiterentwicklung des Krankenhauswesens in Hessen (Hessisches Krankenhausgesetz 2011 – HKHG 2011) vom 21.12,2010, zuletzt geändert durch Artikel 6 des Gesetzes vom 9. Dezember 2022 (GVBl. S. 752, 757)
HKRG	Hessisches Krebsregistergesetz vom 15. Oktober 2014 (GVBl. S. 241) FFN 351-91, zuletzt geändert durch Art. 8 G zur Stärkung der Gesundheitsverwaltung vom 9.12.2022 (GVBl. S. 764)
HSchG	Hessisches Schulgesetz vom 30.06.2017, zuletzt geändert durch Gesetz vom 07.12.2022 (GVBl. S. 734)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung vom 14.Januar 2005 (GVBl. I 2005 S. 14), zuletzt geändert durch Artikel 3 des Gesetzes vom 30. September 2021 (GVBl. S. 622)
HVSG	Hessisches Verfassungsschutzgesetz vom 25. Juni 2018, verkündet als Artikel 1 des Gesetzes zur Neuausrichtung des Verfassungsschutzes in Hessen vom 25. Juni 2018 (GVBl. S. 302)
HVSG	Hessisches Verfassungsschutzgesetz (HVSG) zur Fußnote [1] vom 25. Juni 2018 (GVBl. S. 302) FFN 18-7
HVwVfG	Hessisches Verwaltungsverfahrensgesetz (HVwVfG) in der Fassung vom 15. Januar 2010, zuletzt geändert durch Artikel 2 des Gesetzes vom 12. September 2018 (GVBl. S. 570)
HWaldG	Hessisches Waldgesetz Hessisches Waldgesetz (HWaldG) vom 27.06.2013, zuletzt geändert durch Gesetz vom 19.06.2019
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen vom 20. Juli 2000 (BGBl. I S. 1045), zuletzt geändert durch Art. 8b KrankenhauspflegeentlastungsG vom 20.12.2022 (BGBl. I S. 2793)
KrWG	Kreislaufwirtschaftsgesetz vom 24. Februar 2012 (BGBl. I S. 212), zuletzt geändert durch Artikel 20 des Gesetzes vom 10. August 2021 (BGBl. I S. 3436)

LuftSiG	Luftsicherheitsgesetz vom 11. Januar 2005 (BGBl. I S. 78), zuletzt geändert durch Artikel 1 des Gesetzes vom 22. April 2020 (BGBl. I S. 840)
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19.02.1987 (BGBl. I S. 602), zuletzt geändert durch Artikel 31 des Gesetzes vom 05.10.2021 (BGBl. I S. 4607, 4617)
PsychKHG	Hessisches Gesetz über Hilfen bei psychischen Krankheiten (Psychisch-Kranken-Hilfe-Gesetz - PsychKHG) vom 4.05.2017, zuletzt geändert durch Artikel 4 des Gesetzes vom 9. Dezember 2022 (GVBl. S. 764, 765)
RBStV	Rundfunkbeitragsstaatsvertrag vom 15.–21. Dezember 2010, zuletzt geändert durch den Medienstaatsvertrag vom 14. bis 28. April 2020, in Kraft getreten am 07.11.2020, Hess. GVBl. 2020 S. 607 ff.
Richtlinie (EU) 2016/680	Richtlinie (EU) 2016/680 der Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates
SGB II	Das Zweite Buch Sozialgesetzbuch – Grundsicherung für Arbeitsuchende (Artikel 1 des Gesetzes vom 24.12.2003 (BGBl. I S. 2954), in Kraft getreten am 01.01.2004 bzw. 01.01.2005, zuletzt geändert durch Gesetz vom 16.12.2022 (BGBl. I S. 2328) m. W. v. 01.01.2023
SGB V	Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung – vom 20.12.1988 (BGBl. I S. 2477), zuletzt geändert durch Art. 1, 1a, Art. 1b KrankenhauspflegeentlastungsG vom 20.12.2022 (BGBl. I S. 2793)
SGB X	Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), zuletzt geändert durch Artikel 19 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1237)
SGB XII	Das Zwölfte Buch Sozialgesetzbuch – Sozialhilfe – (Artikel 1 des Gesetzes vom 27. Dezember 2003, BGBl. I S. 3022, 3023), zuletzt geändert durch Artikel 5 des Gesetzes vom 16. Dezember 2022 (BGBl. I S. 2328) m. W. v. 01.01.2023
SIS II	Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)
StBerG	Steuerberatungsgesetz in der Fassung der Bekanntmachung vom 4. November 1975 (BGBl. I S. 2735), zuletzt geändert durch Artikel 34 des Gesetzes vom 16. Dezember 2022 (BGBl. I S. 2294)

StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 47 des Gesetzes vom 21. Dezember 2020 (BGBl. I S. 3096)
StPO	Strafprozessordnung, in der Fassung der Bekanntmachung vom 7. April 1987, zuletzt geändert durch Art. 2 G zur Durchführung der VO (EU) 2019/1148 des Europäischen Parlaments und des Rates vom 20.6.2019
StPO	Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geände4rt durch Artikel 2 des Gesetzes vom 25. März 2022 (BGBl. I S. 571)
StPO	Strafprozessordnung, in der Fassung der Bekanntmachung vom 7. April 1987, zuletzt geändert durch Art. 2 G über die Feststellung des Wirtschaftsplans des ERP-Sondervermögens für das Jahr 2022, zur elektronischen Erhebung der Bankenabgabe und zur Änd. der StPO vom 25.3.2022 (BGBl. I S. 571)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, 1319, zuletzt geändert durch Art. 2 des Gesetztes vom 25.03.2022 (BGBl. I S. 571, 587)
StVG	Straßenverkehrsgesetz vom 05.03 2003, zuletzt geändert durch Art. 2 Abs. 32 G zur Modernisierung des Verkündungs- und Bekanntmachungswesens vom 20.12.2022 (BGBl. I S. 2752)
TestV	Verordnung zum Anspruch auf Testung in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 (Coronavirus-Testverordnung – TestV) vom 21.09.2021, (BAnz AT 21.09.2021 V1) FNA 860-5-77, zuletzt geändert durch Art. 1 Sechste ÄndVO vom 11.1.2023 (BGBl. I Nr. 13)
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982), zuletzt geändert durch Artikel 4 des Gesetzes vom 12. August 2021 (BGBl. I S. 3544)
UWG	Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010 (BGBl. I S. 254), zuletzt geändert durch Artikel 20 des Gesetzes vom 24. Juni 2022 (BGBl. I S. 959)
UWG	Gesetz gegen den unlauteren Wettbewerb, Gesetz vom 03.07.2004 (BGBl. I S. 1414), zuletzt geändert durch Gesetz vom 24.06.2022 (BGBl. I S. 959) m.W.v. 01.08.2022
VwVfG	Verwaltungsverfahrensgesetz in der Fassung der Bekanntmachung vom 23.01.2003 (BGBl. I S. 102), zuletzt geändert durch Gesetz vom 25.06.2021 (BGBl. I S. 2154) m. W. v. 01.08.2021
ZensusG 2022	Gesetz zur Durchführung des Zensus 2022 im Jahr 2022 vom 26.11.2019 (BGBl. 1 S. 1851), geändert durch Art. 2 des Gesetzes vom 03.12.2020 (BGBl. I S. 2675)

Sachwortverzeichnis

E

T

U

V