21. Wahlperiode

Drucksache **21/27**

HESSISCHER LANDTAG

07. 05. 2024

Zweiundfünfzigster Tätigkeitsbericht zum Datenschutz und Sechster Bericht zur Informationsfreiheit

Hessischer Beauftragter für Datenschutz und Informationsfreiheit

vorgelegt zum 31. Dezember 2023
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 7. Mai 2024 Ausgegeben am 7. Mai 2024
Gestaltung: Satzbüro Peters, Taunusstein · Herstellung: AC medienhaus, Wiesbaden · Landtagsinformationssystem: www.Hessischer-Landtag.de

Zweiundfünfzigster Tätigkeitsbericht zum Datenschutz
und
Sechster Tätigkeitsbericht zur Informationsfreiheit

des

Hessischen Beauftragten für Datenschutz
und Informationsfreiheit

Professor Dr. Alexander Roßnagel

vorgelegt zum 31. Dezember 2023
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 21/27

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

Inhaltsverzeichnis

Kernpunkte

1. Datenschutz wird in Hessen akzeptiert und nicht grundsätzlich in Frage gestellt. Schwerwiegende Verstöße waren im Berichtszeitraum nicht festzustellen. Dennoch sind in vielen Bereichen die Anforderungen der Datenschutz-Grundverordnung (DS-GVO) noch immer nicht ausreichend umgesetzt. In vielen Beschwerden machen daher Bürgerinnen und Bürger Verletzungen ihrer Grundrechte geltend. Die Datenschutzaufsicht geht diesen Beschwerden nach und stellt in berechtigten Fällen die Verstöße ab. 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 Hardwares, Softwares, Diensten und Plattformen zu nutzen und dadurch digitale Souveränität zu erringen (Teil I Kap. 1).
3. Als Datenschutzaufsicht bin ich dafür zuständig, die Umsetzung von Datenschutz zu überwachen und durchzusetzen. Je weiter die Digitalisierung nahezu alle Bereiche der Gesellschaft durchdringt, desto mehr erfordert diese Aufgabe angesichts der beschränkten Ausstattung der Aufsichtsbehörden ein strategisches und systematisches Vorgehen. Statt Einzelfälle zu verfolgen, können viele Datenverarbeitung betreffende Maßnahmen in vielen Tausend Fällen Grundrechtsverletzungen verhindern. Hierbei waren wir unterschiedlich erfolgreich. Als sehr schwierig erweist sich die Durchsetzung von Datenschutzrecht gegenüber internationalen Digital-Konzernen. Sie versuchen, die Verhaltensstandards in ihren Vertragsbedingungen als für sie geltende weltweite Rechtsregeln durchzusetzen. Sie wehren sich daher, aus ihrer Sicht regionale Rechtsregelungen zu befolgen, weil dies ein weltweit einheitliches Dienstangebot erschwert. Im Fokus der Aufsichtsbehörden stehen derzeit Facebook und Microsoft 365. Hier sind allenfalls kleine Erfolge zu verzeichnen. Im Gegensatz dazu werden in der hessischen Verwaltung die neue Daten-

schutzleitlinie, die Professionalisierung von Datenschutzbeauftragten und eine datenschutzgerechte Technikauswahl und -gestaltung helfen, Datenschutzanforderungen breit durchzusetzen (Teil 1 Kap. 1).

4. Für die Weiterentwicklung des Datenschutzes in Hessen gewinnt die Europäisierung zunehmend an Bedeutung. Im Berichtsjahr hat der Europäische Gerichtshof die Zahl seiner Entscheidungen zum Datenschutzrecht etwa verdoppelt und mit ihnen viele umstrittene Fragen geklärt. Die Europäische Kommission hat durch ihren Angemessenheitsbeschluss vom 10. Juli 2023 zum US-EU-Data-Privacy-Framework vorerst das Problem der Datenübermittlung in die USA gelöst. Auch der Europäische Datenschutzausschuss (EDSA) trägt zunehmend zu einer Konsolidierung des Datenschutzrechts und zu einem unionsweit einheitlichen Vollzug bei. Dies erfordert stärkere Einflussnahme auf die europäischen Entwicklungen durch engagierte Mitarbeit in Arbeitskreisen des EDSA. Die Anzahl der europaweiten Verfahren, an denen ich beteiligt war, hat von 982 in Jahr 2022 auf 1062 im Jahr 2023 zugenommen. (Teil I Kap. 1 und 2).
5. Die Aufsichtstätigkeit wird weiterhin stark durch eine Juridifizierung des Datenschutzes geprägt. Die Verfahren zur Verhängung von Geldbußen stiegen von 113 im Jahr 2022 auf 124 im Jahr 2023 an. Dagegen nahmen die Gerichtsverfahren von 35 im Jahr 2022 auf 27 im Jahr 2023 leicht ab (Teil I Kap. 3). Die Bedeutung des Justiziariats bleibt weiterhin hoch.
6. 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 sechs Jahre nach dem Wirksamwerden der DS-GVO auf einem sehr hohen Niveau. Sie stieg leicht von 6.836 auf 7.162. Durch die zunehmende Digitalisierung wird die Bearbeitung der Vorgänge aber qualitativ anspruchsvoller. Große Digitalisierungsprojekte, wie z. B. die Umsetzung des Onlinezugangsgesetzes oder die Verwaltungscloud, und die Mitarbeit an der Bewertung großer IT-Plattformen, wie z. B. Facebook oder Microsoft 365, schlagen in der Statistik nicht in dem Ausmaß zu Buche, wie sie meine Behörde tatsächlich beschäftigen (Teil I Kap. 16).
7. Die Meldungen von Datenschutzverstößen gemäß Art. 33 DS-GVO nahmen im Berichtszeitraum wieder zu: von 1.754 im Jahr 2022 auf 1.934 im Jahr 2023. Sie haben damit wieder das Niveau des Jahres 2021 mit 2.016 Meldungen erreicht. Sie zu analysieren und zu bewerten und vor allem dazu beizutragen, sie in ihrem Schadenspotenzial zu beschränken und ihre Wiederholung zu verhindern, fordert einen Großteil meiner Ressourcen. Angriffe auf IT-Systeme nahmen quantitativ von 475 im Jahr 2022 auf 502 im Jahr 2023 zu und werden qualitativ immer raffinierter und

professioneller. Sie richten sich zunehmend gegen Auftragsverarbeiter, die für viele Unternehmen und Behörden arbeiten, und verstärken damit das Schadenspotenzial (Teil 1 Kap. 14).

8. In den Verwaltungsbehörden des Landes und der Kommunen werden derzeit große und anspruchsvolle Projekte der Verwaltungsmodernisierung konzipiert, geplant und umgesetzt, die eine intensive Beteiligung und kritische Mitarbeit der Datenschutzaufsicht erfordern. Aber auch viele alltägliche Probleme des Datenschutzes in Kommunen und Landesbehörden mussten geklärt werden (Teil I Kap. 5).
9. In den Schulen schreitet die Digitalisierung von Unterricht und Lernen weiter voran. Daher war das Inkrafttreten der neuen Schuldatenschutz-Verordnung eine deutliche Verbesserung des Datenschutzrechts. Mit den Schulträgern konnte ihr datenschutzrechtliches Verhältnis zu den Schulen ebenso geklärt werden wie ihre Verpflichtung zum Einsatz rechtmäßiger Regelungen zur Auftragsverarbeitung bei der Nutzung von Microsoft 365 (Teil I Kap. 6).
10. 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. Die Arbeit im Home-Office ist vielfach auch nach der Corona-Pandemie weiterhin üblich und verursacht viele Datenschutzfragen (Teil I Kap. 7).
11. Bei der Polizei, dem Landesamt für Verfassungsschutz und mehreren Staatsanwaltschaften stellten Datenschutzprüfungen keine gravierenden Verstöße gegen datenschutzrechtliche Vorgaben fest. Das Urteil des Bundesverfassungsgerichts zu hessenDATA erforderte eine Neufassung der Ermächtigungsgrundlage, die die Datenverarbeitung an die differenzierten Vorgaben des Gerichts anpasste. Im Gesetzgebungsverfahren zu den Novellen des HSOG und des HVSG habe ich kritische Anmerkungen vorgetragen, die zu einem großen Teil zu Änderungen in beiden Gesetzen führten (Teil I Kap. 4).
12. Hinsichtlich der Internetnutzung musste ich mich am Beispiel von ChatGPT mit vielen neuen Datenschutzfragen bei der Nutzung generativer Künstlicher Intelligenz befassen. Ein wichtiges Thema waren auch Abo-Modelle für Social Networks. Mit ihrer Hilfe wollen die Anbieter ihre rechtswidrige Verarbeitung von Nutzerdaten und deren Auswertung für Werbeprofile ohne Einwilligung der Nutzer ausgleichen. Da auch bei Abo-Modellen die Nutzerdaten weiterhin erhoben werden, bleibt diese Datenverarbeitung rechtswidrig (Teil I Kap. 8).

13. Im Bereich Werbung und Adresshandel musste ich vielfach intervenieren, weil Datenschutzverstöße durch die Art der Datenerhebung, durch die unzureichende Umsetzung von Werbewidersprüchen und durch die fehlende Freiwilligkeit von Werbeeinwilligungen und mangelnde technisch-organisatorische Maßnahmen festzustellen waren (Teil I Kap. 9).
14. Im Bereich der privaten Kreditwirtschaft brachten die Urteile des Europäischen Gerichtshofs zum Bonitäts-Scoring der Auskunfteien und zur Verarbeitung von Daten zur Restschuldbefreiung neue Erkenntnisse, die dazu führten, dass ich die bisherigen Verhaltensregeln des Verbands „Die Wirtschaftsauskunfteien" beanstandete. Darüber hinaus musste ich vielen Detailfragen zu Datenverarbeitungen bei unterschiedlichen Unternehmen nachgehen (Teil I Kap. 11).
15. Im Gesundheitsbereich waren vielfältige Datenschutzfragen in Kliniken, Arztpraxen und Apotheken zu bearbeiten (Teil I Kap. 12).
16. Zusammen mit dem Bundesbeauftragten für Datenschutz und Informationsfreiheit leite ich die Taskforce Forschungsdaten, die im Berichtszeitraum mehrere wichtige Stellungnahmen der Datenschutzkonferenz vorbereitete. Im Bereich der Forschung unterstützten wir mehrere Forschungsprojekte und klärten zusammen mit der Initiative Gesundheitsindustrie Hessen spezifische Datenschutzfragen im Umgang mit Gesundheitsdaten (Teil I Kap. 13).
17. 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 Kap. 1). Beschwerden und Beratungen sanken leicht von 110 auf 99. Im Berichtsjahr hat der Landtag in Hessen ein Open-Data-Gesetz beschlossen (Teil II Kap. 2), dabei aber wie bei der Regelung zur Informationsfreiheit es den Gemeinden und Landkreisen überlassen, ob sie dieses Gesetz gegen sich gelten lassen wollen (Teil II Kap. 2). Bisher ist das Recht auf Informationsfreiheit bei rein wirtschaftlichen Interessen ausgeschlossen. Ich plädiere dafür, diese Ausnahme aufzuheben (Teil II Kap. 4). Die Kosten für die Geltendmachung eines Anspruchs auf Informationsfreiheit dürfen diesen nicht praktisch verhindern. Die Regelung in Hessen entspricht den Kostenregelungen im Bund und in anderen Bundesländern und erscheint für umfangreiche Recherchen nicht unbillig (Teil II Kap. 5).

Vorwort

Dies ist der 52. Tätigkeitsbericht zum Datenschutz und der 6. Tätigkeitsbericht zur Informationsfreiheit des Hessischen Beauftragten für Datenschutz und Informationsfreiheit. Mit diesen Berichten erfülle ich meine Informationspflichten nach Art. 59 Datenschutz-Grundverordnung sowie §§ 15 Abs. 3 und 89 Abs. 4 Hessisches Datenschutz- und Informationsfreiheitsgesetz.

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.

Der 52. Tätigkeitsbericht zum Datenschutz, der die Entwicklungen im Jahr 2023 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 Tätigkeitsberichte haben die Funktion, die aktuelle Praxis des Datenschutzes und der Informationsfreiheit in Hessen zu beschreiben und zu analysieren sowie die Möglichkeiten der Aufsichtsbehörde, auf diese zugunsten der Grundrechte und der Demokratie Einfluss zu nehmen, aufzuzeigen.

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 Vervielfachung personenbezogener Daten. Dennoch ist es der Hessischen Datenschutzaufsicht gelungen, auch im Jahr 2023 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 noch weiter 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
52. Tätigkeitsbericht zum Datenschutz

1. Neue Aufgaben und Rahmenbedingungen

Der vorliegende Tätigkeitsbericht beschreibt und analysiert den Datenschutz in Hessen im Jahr 6 seit dem Geltungsbeginn der Datenschutz-Grundverordnung (DS-GVO) am 25. Mai 2018. Dieser wird immer stärker durch die Europäisierung des Datenschutzrechts geprägt. Allen voran der Europäische Gerichtshof klärt zunehmend die Unsicherheiten, die der sehr abstrakte Rechtsrahmen der DS-GVO für die Praxis des Datenschutzes gebracht hat (Kap. 1.1). In der Umsetzung des Datenschutzrechts tun sich die Aufsichtsbehörden vor allem gegenüber den internationalen Digitalkonzernen schwer, die ihre große Wirtschaftsmacht dazu benutzen, gegenüber dem europäischen Datenschutzrecht eigene Rechtsordnungen auf ihren Plattformen durchzusetzen (Kap. 1.2). Gegenüber den Verantwortlichen in Deutschland müssen die Aufsichtsbehörden versuchen, die Grundlagen für eine strategische und systematische Umsetzung des Datenschutzrechts zu verbessern (Kap. 1.3). Die notwendige Mitwirkung im Europäischen Datenschutzausschuss und die Zusammenarbeit der Aufsichtsbehörden in Deutschland bestimmen und verändern zunehmend die Aufgaben und Handlungsmöglichkeiten der Datenschutzaufsicht (1.4).

1.1 Rechtsprechung des Europäischen Gerichtshofs

Das nationale Datenschutzrecht und die Tätigkeit der Aufsichtsbehörden wird immer stärker durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH) geprägt. Er hat allein im Berichtsjahr mehr als 25 wichtige Entscheidungen zum Datenschutz und zur Auslegung der DS-GVO getroffen und dadurch viele Streitfragen geklärt. Jede Entscheidung konzentriert sich zwar auf ihren Entscheidungsgegenstand, enthält aber immer auch über ihn hinausweisende Bemerkungen. Diese wiederum werden interessengeleitet unterschiedlich interpretiert, so dass die Entscheidungen viele neue Fragen hinterlassen, über die gestritten wird und die Rechtsunsicherheit für Verantwortliche und Aufsichtsbehörden bewirken (s. 50. Tätigkeitsbericht, Kap. 1). Im Berichtsjahr waren vor allem die folgenden Entscheidungen für die Aufsichtstätigkeit in Hessen bedeutsam.

Urteil vom 7. Dezember 2023 zu SCHUFA I

An dem Verfahren war ich als Beklagter des Ausgangsverfahrens beteiligt. Das Urteil des EuGH in der Rechtssache C 26/22 und C-64/22[1] beruhte auf einer Vorlage durch das Verwaltungsgericht Wiesbaden (s. auch Kap. 3.1 und 11.3). In dem zugrundeliegenden Gerichtsverfahren und dem vorausgegangenen Beschwerdeverfahren wurde darüber gestritten, ob die SCHUFA sich für die dreijährige Speicherung einer Restschuldbefreiung auf die von der Datenschutzaufsichtsbehörde genehmigten Verhaltensregeln des Verbands „Die Wirtschaftsauskunfteien" berufen kann. Der EuGH hat Feststellungen zum Beschwerdeverfahren, zur zulässigen Speicherdauer für Restschuldbefreiungen und zu datenschutzrechtlichen Verhaltensregeln getroffen.

Wichtig für die Durchführung von Beschwerdeverfahren sind die Feststellungen, dass die Beschwerde nicht einer Petition gleichkommt und die Datenschutzaufsichtsbehörde nicht nur eine Bearbeitung der Beschwerde schuldet, sondern die Beschwerde die Durchführung eines normalen Verwaltungsverfahrens erfordert. Die Entscheidung der Datenschutzaufsichtsbehörde, eine Beschwerde zurückzuweisen, ist ein Verwaltungsakt mit Rechtswirkung. Er unterliegt einer vollständigen inhaltlichen Überprüfung durch das zuständige Gericht. Dies gilt allerdings nur für die Feststellung und Bewertung des Sachverhalts. Dagegen besteht für die Durchführung des Beschwerdeverfahrens und für die Festlegung der aufsichtsrechtlichen Maßnahmen ein Ermessensspielraum der Aufsichtsbehörde. Die Ausübung des Ermessens kann das Gericht nur auf Ermessensfehler überprüfen. Es kann nicht seine Entscheidung an die Stelle der Entscheidung der Aufsichtsbehörde setzen. Diese Feststellungen erzeugen für alle Beteiligten an der Durchführung von Beschwerdeverfahren Rechtssicherheit. Sie führen aber zu einer weiteren Juridifizierung der Aufsichtstätigkeit (s. 50. Tätigkeitsbericht, Kap. 1 und 51. Tätigkeitsbericht Kap. 1).

Die Feststellungen hinsichtlich der datenschutzrechtlichen Verhaltensregeln sind dagegen weniger aussagekräftig. Alle hatten Feststellungen zu ihrer Verbindlichkeit für die verschiedenen Beteiligten erhofft. Der EuGH hat jedoch lediglich festgestellt, dass die Verhaltensregeln nur die Vorgaben der DS-GVO auslegen können, sie jedoch nicht ausweiten oder verändern dürfen. Wenn sie z. B. die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO konkretisieren, ist an dieser Norm zu prüfen, ob sie die Grenze zwischen Auslegung und Ausweitung einhalten. Wer wie sehr an sie

1 EuGH Urteil vom 7.12.2023, C 26/22 und C-64/22 – ECLI:EU:C:2023:958, NJW 2024, 417.

gebunden ist und durch sie entlastet wird, wenn sie die Norm nur auslegen, bleibt leider weiterhin umstritten.

Hinsichtlich der Frage, wie lange private Wirtschaftsauskunfteien Informationen aus öffentlichen Registern in ihren eigenen Datenbanken speichern dürfen, kann der EuGH – über den Einzelfall der Informationen über eine Restschuldbefreiung hinaus – wohl so verstanden werden, dass die zulässige Speicherfrist sich in erster Näherung an dem Zeitraum der Veröffentlichung im öffentlichen Register orientiert. Dies bedeutet für Informationen aus dem Insolvenzregister eine Höchstfrist von sechs Monaten und aus dem Schuldnerverzeichnis von drei Jahren.

Urteil vom 7. Dezember 2023 zu SCHUFA II

In dem Verfahren C-634/21, dem ebenfalls eine Vorlage durch das Verwaltungsgericht Wiesbaden zugrunde lag und an dem ich wiederum beteiligt war, ging es um die Frage, ob die Erstellung eines Bonitäts-Scores durch die SCHUFA und dessen Verwendung durch ein Kreditinstitut eine grundsätzlich verbotene automatisierte Entscheidung nach Art. 22 Abs. 1 DS-GVO darstellt (s. auch Kap. 3.1 und 11.2). Die Feststellungen des EuGH[2] betreffen alle arbeitsteilig erstellten Entscheidungen, die von einem automatisierten Entscheidungsunterstützungssystem vorbereitet und von einem Menschen getroffen werden. Für die Einordnung der Kette von Entscheidungsschritten als „ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung“ ist nach EuGH entscheidend, ob dem vorbereitenden Ergebnis eine „maßgebliche Rolle“ im Rahmen der abschließenden menschlichen Festlegung des Ergebnisses zukommt. Ob dies der Fall ist, hängt von den Umständen des Einzelfalls ab. Diese Feststellung des EuGH wird künftig für viele Entscheidungsunterstützungssysteme und insbesondere viele Anwendungen Künstlicher Intelligenz von entscheidender Bedeutung sein.

Urteil vom 5. Dezember 2023 zu Deutsche Wohnen

In dem Verfahren C-807/21, dem eine Vorlage durch das Kammergericht Berlin zugrunde lag, ging es um die Fragen, ob eine Aufsichtsbehörde eine Geldbuße unmittelbar gegen ein Unternehmen verhängen kann und ob dem Unternehmen hierfür ein Verschulden nachgewiesen werden muss. Im Ausgangsfall hatte die Aufsichtsbehörde in Berlin gegen die Deutsche Wohnen SE eine Geldbuße in Höhe von über 14 Mio. Euro verhängt. Der

2 EuGH Urteil vom 7.12.2023, C-634/21 – ECLI:EU:C:2023:957, NJW 2024, 413.

EuGH stellte fest,[3] dass ein Unternehmen als Verantwortlicher selbst gegen datenschutzrechtliche Vorgaben verstoßen und deshalb auch unmittelbar zum Adressaten einer Geldbuße nach Art. 83 DS-GVO werden kann.[4]

Hierfür genügt es festzustellen, dass der Verstoß von Personen begangen wurde, die dem Unternehmen zuzuordnen sind, ohne dass diese identifiziert werden müssen. Allerdings muss der Verantwortliche den Verstoß schuldhaft begangen haben. Hierfür genügt aber festzustellen, dass das Unternehmen „sich über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte, gleichviel, ob ihm dabei bewusst war, dass es gegen die Vorschriften der DSGVO verstößt".[5] Dabei setzt die Verhängung einer Sanktion „keine Handlung und nicht einmal eine Kenntnis seitens des Leitungsorgans dieser juristischen Person voraus". [6]

Diese Feststellungen des EuGH werden die Aufsichtstätigkeit der Aufsichtsbehörden erheblich erleichtern. Sie können jetzt mit ausreichender Rechtssicherheit gegen Datenschutzverstöße auch juristischer Personen vorgehen. Die unmittelbare Haftung eines Unternehmens macht die Verhängung einer Geldbuße nicht davon abhängig, dass es der Aufsichtsbehörde gelingt, unternehmensinterne Verantwortlichkeiten nachzuweisen, um die Zurechnung eines Verstoßes einer Leitungsperson zur juristischen Person zu begründen. Die zur Ermittlung von Tat und Täter erforderlichen Vor-Ort-Untersuchungen, Zeugenvernehmungen und sonstigen polizeilichen Maßnahmen sind nicht mehr notwendig. Hinsichtlich des Verschuldens wird – von Ausnahmefällen abgesehen – davon auszugehen sein, dass eine juristische Person sich über die Rechtswidrigkeit ihres Verhaltens nicht im Unklaren sein konnte. Für einen Ausschluss des Verschuldens reicht es jedenfalls nicht aus, dass der Verantwortliche eine eigene Rechtsauffassung entwickelt hat oder sich einer Rechtsmeinung eines Anwalts, einzelner Gerichtsentscheidungen oder Stimmen in der Literatur anschließt, wenn die zuständige Aufsichtsbehörde, die DSK oder der EDSA ihre entgegenstehende Rechtsauffassung bekannt gegeben haben. Unternehmen werden gut beraten sein, wenn sie vor dem Einsatz neuer Techniksysteme oder der Einführung neuer Geschäftsmodelle bei der Aufsichtsbehörde nachfragen, wie sie das neue Verhalten der juristischen Person bewertet.

---

3 EuGH Urteil vom 5.12.2023, C-807/21 – ECLI:EU:C:2023:950, NJW 2024, 343

4 S. näher Roßnagel/Rost, Geldbußen gegen juristische Personen, ZD 2024, 183–188.

5 EuGH vom 5.12.2023, C-683/21, – ECLI:EU:C:2023:950, NJW 2024, 343, Rn. 76.

6 EuGH vom 5.12.2023, C-683/21, – ECLI:EU:C:2023:950, NJW 2024, 343, Rn. 76.

Urteil vom 4. Juli 2023 zu Meta

In seinem Urteil vom 4. Juli 2023 in der Rechtssache C-252/21[7] traf der EuGH wichtige Feststellungen zum Datenschutzrecht, obwohl es in dem Urteil in erster Linie um die Befugnisse des Bundeskartellamts ging. In Ausgangsverfahren hatte Meta gegen dieses Amt geklagt, weil es Facebook Handlungen untersagen wollte, die gegen Vorgaben der DS-GVO verstießen. Darin sah es eine missbräuchliche Ausnutzung einer marktbeherrschenden Stellung. Konkret ging es um die automatisierte Erstellung von detaillierten Profilen der Nutzer des Netzwerks, aber auch von Nicht-Nutzern ohne Einwilligung.

Der EuGH prüfte die Praxis der Datenerhebung und -verwendung von Facebook danach, ob sie durch Art. 6 Abs. 1 gerechtfertigt werden kann. Insbesondere für die Datenverarbeitung zur Vertragserfüllung nach Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO und zu überwiegenden berechtigten Interessen nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO konnte der EuGH nicht feststellen, dass sie die Praxis von Facebook legitimieren. Die Datenerhebung im Internet sah er auch nicht als von Art. 9 Abs. 2 Buchst. e DS-GVO gedeckt an. Außerdem kann die Zustimmung zu den AGB von Facebook nicht als eine wirksame freiwillige Einwilligung in die umstrittene Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 9 Abs. 2 Buchst. a DS-GVO angesehen werden. Diese Feststellungen des EuGH, dass Facebook rechtswidrig Daten erhebt und verwendet, ist sowohl in der Auseinandersetzung mit Meta (s. Kap. 1.3) als auch für die Bewertung anderer sozialer Netzwerke von entscheidender Bedeutung.

Urteil vom 30. März 2023 zu Hessischem Kultusministerium

In seinem Urteil in der Rechtssache C-34/21[8] hat der EuGH wichtige Feststellungen zum Beschäftigtendatenschutz getroffen. Zugrunde liegt ihm ein Streit zwischen dem Hauptpersonalrat der Lehrerinnen und Lehrer und dem Hessischen Kultusministerium bezogen auf die Verpflichtung der Lehrerinnen und Lehrer, während der COVID-Pandemie Unterricht über Videokonferenzsysteme anzubieten. Das Verwaltungsgericht Wiesbaden legte dem EuGH die Frage vor, ob die Generalklausel des § 23 Abs. 1 Satz 1 HDSIG, die wortgleich mit der Regelung des § 26 Abs. 1 Satz 1 BDSG ist, mit Art. 88 DS-GVO vereinbar ist (s. Kap. 7.2).

Nach Art. 88 Abs. 1 DS-GVO können die Mitgliedstaaten „spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im

7 EuGH vom 4.7.2023, C-252/21 – ECLI:EU:C:2023:537, NJW 2023, 2997.

8 EuGH vom 30.3.2023, C-34/21 – ECLI:EU:C:2023:270; NJW 2023, 1639.

Beschäftigungskontext“ erlassen. Hierzu stellte der EuGH fest, dass eine „spezifischere Vorschrift“ nur vorliegt, wenn sie die Vorgaben von Art. 88 Abs. 2 DS-GVO erfüllt. Dies ist nur der Fall, wenn sie „geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person“ enthält. Da dies bei § 23 Abs. 1 Satz 1 HDSIG nicht der Fall ist, muss diese als unionsrechtswidrig angesehen werden. Dies ist für die Regelungen zum Beschäftigtendatenschutz im nicht-öffentlichen Bereich von großer Bedeutung. Hierzu habe ich eine Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023, C-34/21, veröffentlicht.[9]

Für die Beschäftigten im öffentlichen Bereich, die von § 23 Abs. 1 Satz 1 HDSIG erfasst werden, insbesondere für die Lehrerinnen und Lehrer, ändert sich in der Praxis jedoch nichts, weil die Mitgliedstaaten für diesen Bereich Regelungen nach Art. 6 Abs. 3 DS-GVO erlassen können, die keine spezifischeren Vorschriften fordern.[10]

Insofern ist dieses Urteil wichtig für die gesetzgeberischen Bemühungen um eine eigenständige Regelung des Beschäftigtendatenschutzes, bringt für die Beteiligten im Ausgangsverfahren jedoch nur einen Wechsel der Öffnungsklausel.

1.2
Durchsetzung des Datenschutzrechts gegenüber Digital-Konzernen

Als sehr schwierig erweist sich die Durchsetzung von Datenschutzrecht gegenüber internationalen Digital-Konzernen. Sie versuchen, die Verhaltensstandards in ihren Vertragsbedingungen als für sie geltende weltweite Rechtsregeln durchzusetzen. Sie wehren sich daher, aus ihrer Sicht regionale Rechtsregelungen zu befolgen, weil dies ein weltweit einheitliches Dienstangebot erschwert. Im Fokus der Datenschutzaufsichtsbehörden stehen derzeit Facebook und Microsoft 365. Ein wenig entspannt hat sich die Situation dadurch, dass die Europäische Kommission die Datenschutzregelungen in den USA unter dem Data Privacy Framework als angemessen anerkannt hat. Die Übertragung personenbezogener Daten ohne ausreichende Schutzvorkehrungen ist jedoch nur ein Teil der Rechtsverstöße von Facebook und Microsoft.

9 https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-05/handreichung_beschaeftigtendatenschutz_eugh-urteil.pdf.

10 S. hierzu auch ausführlich Roßnagel/Wetzstein/Horlbeck, Unionsrechtliche Vorgaben für das Recht des Beschäftigtendatenschutzes – Auswirkungen des EuGH-Urteils vom 30.3.2023, DuD 2023, 429–434.

Angemessenheitsbeschluss für Datenverarbeitungen in die USA

Die Europäische Kommission hat am 10. Juli 2023 einen neuen Angemessenheitsbeschluss zum Datentransfer in die USA auf der Grundlage des sog. EU-US Data Privacy Framework (EU-US DPF) erlassen (s. Kap. 2.2). Dies ist der dritte Versuch, Datenübermittlungen in die USA mit den Anforderungen der Grundrechtecharta in Übereinklang zu bringen, nachdem der EuGH die Angemessenheitsbeschlüsse für „Safe Harbor“ im Jahr 2015 und „Privacy Shield“ im Jahr 2020 für unionsrechtswidrig erklärt hat. Für beide Urteile des EuGH war entscheidend, dass die US-Sicherheitsbehörden zu weitgehende Befugnisse besitzen, personenbezogene Daten zu verarbeiten, und betroffene Personen dagegen unzureichende Rechtsschutzmöglichkeiten haben. Beides wurde im EU-US DPF verbessert. Ob dies ausreichend war, muss wiederum der EuGH klären.

Der Angemessenheitsbeschluss ist für Datenschutzaufsichtsbehörden bindend. Soweit das EU-US DPF greift, müssen sie den Angemessenheitsbeschluss als rechtliche Grundlage für Datenübertragungen in die USA akzeptieren. Diese Grundlage gilt jedoch nicht für die USA insgesamt, sondern nur sektoral. Sie gilt nur für US-Organisationen, die der Aufsicht der US Federal Trade Commission oder des US Department of Transportation unterliegen und z. B. nicht für Banken, Versicherungen und Telekommunikationsanbieter. Sie gilt weiter nur für US-Organisationen, die sich selbst unter dem EU-US DPF zertifiziert haben. Und sie gilt schließlich nur für diejenigen Organisationen, die in die „Data Privacy Framework List“[11] des US Department of Commerce aufgenommen wurden. Microsoft und Facebook erfüllen alle drei Forderungen. Damit ist jedoch die Rechtmäßigkeit ihrer Datenverarbeitung noch nicht gewährleistet. Vielmehr ist festzustellen, dass diese gegen viele Vorgaben des europäischen und deutschen Datenschutzrechts verstoßen.

Facebook

Bereits in meinem letztjährigen Tätigkeitsbericht habe ich auf die Rechtslage zum Betrieb von Facebook-Seiten (= Fanpages) hingewiesen (51. Tätigkeitsbericht, Kap. 2). Die Rechtswidrigkeit der Datenverarbeitung im Facebook-Dienst hat auch der EuGH in seinem Urteil vom 4. Juli 2023 (C-252/21) untersucht und bestätigt (s. Kap. 1.1). Über diese Rechtslage habe ich auch alle öffentlichen Stellen in Hessen informiert.

Im Berichtszeitraum hat der Bundesbeauftragte für Datenschutz und Informationsfreiheit am 17. Februar 2023 dem Bundespresseamt den weiteren Betrieb seiner Facebook-Fanpage untersagt. Das Bundespresseamt will jedoch

11 https://www.dataprivacyframework.gov/s/participant-search.

die Reichweite von Facebook für seine Informationen weiter nutzen und hat gegen diesen Bescheid Klage beim Verwaltungsgericht Köln eingereicht. Ebenso hat die Sächsische Datenschutz- und Transparenzbeauftragte am 5. Juli 2023 der Sächsischen Staatskanzlei untersagt, ihre Facebook-Fanpage weiter zu betreiben. Auch die Staatskanzlei hat vor dem Verwaltungsgericht in Dresden dagegen geklagt. Beide Gerichtsverfahren waren zum Ende des Berichtszeitraums noch nicht abgeschlossen.

Sowohl die Datenschutzaufsichtsbehörden als auch die Bundes- und die Landesregierungen sehen diese beiden Gerichtsverfahren als Musterprozesse an, um zu klären, ob der Verfassungsauftrag, die Bürgerinnen und Bürger über die Tätigkeit, Vorhaben und Ziele der Regierungen zu informieren, die Nutzung einer Facebook-Seite erfordert und ob dieser Auftrag die Pflicht zur Einhaltung der Datenschutz-Grundverordnung überwiegt.

In der Zwischenzeit bis zur Klärung dieser Rechtsfrage erwarte ich, dass öffentliche Stellen in Hessen zumindest keine neuen Facebook-Fanpages eröffnen. Weiterhin müssen sie alle Informationen, die sie auf ihrer Fanpage posten, auch über andere Kanäle anbieten und über die Datenverarbeitung durch Facebook informieren. Dadurch soll ausgeschlossen sein, dass jemand gezwungen wird, Facebook zu nutzen, um bestimmte Informationen zu erhalten.

Im November 2023 hat Meta auf das Urteil des EuGH vom 4. Juli 2023 (s. Kap. 1.1) in der Weise reagiert, dass die Kunden von Facebook zwischen einem geldfreien Facebook-Account mit Werbung oder einem kostenpflichtigen Facebook-Account (im Festnetz 10 Euro im Monat, über das Smartphone 13 Euro im Monat) ohne Werbung wählen können. Facebook wertet die Wahl eines geldfreien Accounts als Einwilligung in die Datenverarbeitung durch Facebook. Aber auch mit dieser Wahlmöglichkeit bleibt die Datenverarbeitung durch Facebook rechtswidrig. Beim werbefreien Account werden nämlich die Datenerhebung und die Profilbildung nicht eingeschränkt, nur die Werbung entfällt. Die mit der Wahl für die kostenfreie Version verbundene Zustimmung zur Datenverarbeitung ist keine wirksame Einwilligung, weil sie nicht freiwillig ist und auf unzureichenden Informationen beruht. Außerdem kann sie das Tracking der Nicht-Facebook-Account-Inhaber nicht rechtfertigen.

In einigen Bereichen ist durchaus ein positiver Trend erkennbar, dass der Einsatz von Facebook-Seiten und ähnlichen Angeboten zunehmend kritisch hinterfragt und vermehrt die Nutzung von Alternativen in Betracht gezogen wird. So hat die Landesregierung als Alternative zu ihrer Facebook-Fanpage eine Instanz bei Mastodon eingerichtet, der von allen hessischen Ministerien – unterschiedlich stark – genutzt wird. Auch der Hessische Landtag und meine Behörde nutzen diese Instanz (s. Kap. 15.2).

Microsoft 365

In der Vergangenheit hat sich die DSK mehrfach mit dem datenschutzrechtskonformen Einsatz der cloudbasierten Online-Dienste der Firma Microsoft befasst und im vorangegangenen Berichtszeitraum u. a. festgestellt, dass datenschutzrechtlich Verantwortliche ihre Nachweispflicht im Zusammenhang mit der Nutzung des Angebots Microsoft 365 nicht ohne weiteres erfüllen können.[12] Indem Microsoft seine Produktfamilie MS 365 als Clouddienste anbietet, hat sich die datenschutzrechtliche Rolle vom Microsoft geändert. Microsoft ist nicht mehr ein Anbieter einer Software, die der Lizenznehmer auf seinem Gerät installiert, sondern als Anbieter von Clouddiensten ein Auftragsverarbeiter. Für den abzuschließenden Auftragsverarbeitungsvertrag bietet Microsoft seinen Kunden als Auftraggebern eine Standard-Vereinbarung an: den „Datenschutznachtrag zu den Produkten und Services von Microsoft (im Berichtszeitraum Stand 1.1.2023)“ (abgekürzt DPA). Dieser muss die Anforderungen an Auftragsverarbeiter nach Art. 28 DS-GVO erfüllen.

In der Untersuchung der Arbeitsgruppe Microsoft-Onlinedienste der DSK[13] und in ihrer Zusammenfassung [14] sind jedoch sieben wesentliche Ergebnisse aufgeführt, die einer rechtskonformen Verarbeitung personenbezogener Daten auf Basis von Microsoft 365 entgegenstehen. Von diesen bezieht sich nur einer auf die Problematik der Datenübermittlung in Drittstaaten, die durch den Angemessenheitsbeschluss vorerst geklärt ist.

Über diese Rechtslage habe ich die Landesregierung, die Schulträger, die Hochschulen, den Landkreistag, den Städtetag und den Städte- und Gemeindebund sowie die Industrie- und Handelskammern in Hessen mehrfach informiert. Ich sehe einerseits die (künftige) Abhängigkeit vieler Stellen von MS 365, sie können mittelfristig ihre Aufgaben nur erfüllen, wenn sie für ihre Datenverarbeitung diese Dienste nutzen. Andererseits tragen sie als Verantwortliche nach Art. 5 Abs. 2 DSGVO die Verantwortung für die Rechtmäßigkeit ihrer Datenverarbeitung und müssen diese jederzeit nachweisen können. Um diese Interessen auszugleichen, fordere ich aus Gründen der Verhältnismäßigkeit in einem ersten Schritt, dass sie von Microsoft eine

12 DSK, Festlegung vom 24.11.2022, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf.

13 DSK, Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf.

14 DSK, Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf.

Zusatzvereinbarung einfordern, in der mindesten die sechs folgenden Anforderungen, die so im DPA bisher fehlen, enthalten sind:

1. Microsoft muss dem Verantwortlichen ermöglichen, die Datenkategorien, die Zwecke und die Verarbeitungsschritte konkret zu bestimmen, für die MS 365 eingesetzt werden soll.
2. Microsoft darf die Daten aus der Auftragsverarbeitung nicht für eigene Zwecke verarbeiten, sondern nur für die Zwecke der Auftragserfüllung.
3. Microsoft darf nicht die Erlaubnis der Verantwortlichen unterstellen, dass MS personenbezogene Daten der (europäischen Kunden) nach gesetzlichen US-Normen (z. B. Cloud-Act, FISA 702) US-Behörden und Nachrichtendiensten offenlegen darf.
4. Microsoft muss sicherstellen, dass alle personenbezogenen Daten, die MS als Auftragsverarbeiter verarbeitet, Schutzmaßnahmen nach dem Stand der Technik (und nicht nur branchenüblichen) unterliegen.
5. Microsoft muss, vor der Einschaltung von Unterauftragsverarbeitern, diese dem Verantwortlichen im Einzelnen benennen und ihm bekanntgeben, welche Daten sie zu welchen Zwecken an welchen Orten verarbeiten, und von ihm hierzu die Zustimmung einholen.
6. Microsoft muss alle personenbezogenen Daten nach Ende der Vertragsbeziehungen mit kurzen Fristen löschen oder zurückgeben.

Die Datenschutzaufsichtsbehörden unterstützen dieses Vorgehen durch eine Handreichung.[15]

Sofern sich betroffene Personen gegen die Verarbeitung ihrer Daten mittels MS 365 beschweren und diese Verstöße geltend machen, muss ich diesen Beschwerden nachgehen, von den Verantwortlichen Nachweise einer rechtmäßigen Datenverarbeitung fordern und, soweit dies nicht nachgewiesen werden kann, diese Verstöße abstellen. Ich werde aber vorerst solchen Verstößen nicht von mir aus nachgehen, wenn die Verantwortlichen nachweisen, dass sie von Microsoft eine Zusatzvereinbarung verlangt haben, die die Rechtsverstöße des DPA beseitigt.

Dadurch ist es mir bisher gelungen, dass das Hessische Kultusministerium für alle hessischen Schulen, die hessischen Universitäten, Verwaltungsbehörden, einige Schulträger, zentrale IT-Dienstleister in Hessen und die Industrie- und Handelskammern solche Forderungen an Microsoft gerichtet haben oder sie unterstützen.

15 https://datenschutz.hessen.de/vereinbarung-zur-auftragsverarbeitung-fuer-den-einsatz-von-microsoft-365.

1.3
Grundlagen für die Umsetzung des Datenschutzrechts

Die Datenschutzaufsichtsbehörden sind dafür zuständig, die Umsetzung des Datenschutzrechts zu überwachen und durchzusetzen. Die Digitalisierung durchdringt jedoch immer stärker nahezu alle Bereiche der Gesellschaft. Dementsprechend breit sind die Aufgaben der Aufsichtsbehörde und dementsprechend tief muss sie Herausforderungen des Datenschutzes nachgehen. Dies erfordert angesichts der beschränkten Ausstattung der Aufsichtsbehörden ein strategisches und systematisches Vorgehen. Hierbei hilft die neue Datenschutzleitlinie der hessischen Landesverwaltung, die Professionalisierung von Datenschutzbeauftragten und eine datenschutzgerechte Technikauswahl und -gestaltung.

Im Gegensatz zu einem strategischen und systematischen Vorgehen nehmen in der Realität Beschwerden nach Art. 77 DS-GVO und Meldungen von Datenschutzverletzungen nach Art. 33 DS-GVO, also einzelfallorientierte Bearbeitungen, überwiegend die Kapazitäten der Aufsichtsbehörden in Anspruch. Die Aufsichtstätigkeit sollte eigentlich präventiv Datenschutzverstöße vermeiden. In der Realität ist sie stattdessen repressiv durch die Aufklärung von Datenschutzverstößen, Abhilfe und Sanktion im Einzelfall geprägt. Bezogen auf die Entwicklung von IT-Systemen, Geschäftsmodellen und Verwaltungsverfahren sollte sie konstruktiv beratend und gestaltend Datenschutz von Anfang an zur Geltung bringen. In der Realität muss sie versuchen, jeweils im Einzelfall nachträgliche Korrekturen gegen heftigen Widerstand durchzusetzen. Angesichts dieser Diskrepanz zwischen Zielsetzungen und Realität müssen Aufsichtsbehörden darauf zielen, systematisch die Bedingungen der Umsetzung von Datenschutzrecht zu verändern, um dadurch die Hebelwirkung ihrer Tätigkeit zu vervielfachen. In drei Bereichen konnte ich im Berichtsjahr hinsichtlich dieser Zielsetzung Verbesserungen erreichen.

Datenschutzleitlinie der Landesverwaltung

Datenschutz kann dann effektiv und effizient umgesetzt werden, wenn die Verantwortlichen über ein geeignetes und wirksames Datenschutzmanagement verfügen, das für den notwendigen operativen Datenschutz in der Organisation des Verantwortlichen zuständig ist. Dann können rechtzeitige und zutreffende Hinweise zum Datenschutz eine datenschutzgerechte Gestaltung und einen datenschutzkonformen Betrieb der Verarbeitungsverfahren sicherstellen. Auf diese Weise können die Pflichten des Verantwortlichen nach Art. 5 und 24 DS-GVO professionell wahrgenommen werden und die notwendigen Datenschutzdokumentationen routiniert erfolgen. Dieser opera-

tive Datenschutz ist von den Aufgaben des betrieblichen oder behördlichen Datenschutzbeauftragten zu unterscheiden, der nach Art. 39 DS-GVO, § 7 BDSG und § 7 HDSIG die Aufgabe hat, die Umsetzung des operativen Datenschutzes zu überwachen und ihm beratend zur Seite zu stehen.

Insofern ist es ein großer Fortschritt, dass die Hessische Ministerin für Digitale Strategie und Entwicklung (HMinD) mit meiner Unterstützung zusammen mit den anderen Ressorts eine Datenschutzleitlinie für IT-Verfahren und -Projekte der Hessischen Landesverwaltung erarbeitet hat (s. Kap. 5.1). Ziel dieser Datenschutzleitlinie ist es, innerhalb der Landesverwaltung einer einheitlichen Umsetzung der datenschutzrechtlichen Anforderungen zu dienen und konkrete Empfehlungen für das Datenschutzmanagement zu geben. Dadurch kann ein gemeinsames Verständnis der datenschutzrechtlichen Pflichten entstehen und eine den jeweiligen Bedingungen des Ressorts angepasste, aber an einheitlichen Grundsätzen orientierte Wahrnehmung des operativen Datenschutzes erfolgen. Die Datenschutzleitlinie stellt auch klar, wie die Arbeitsaufteilung zwischen der Leitungsebene der verantwortlichen Organisation, den Verantwortlichen für die IT-Verfahren und -Projekte, dem Datenschutzmanagement und dem oder der Datenschutzbeauftragten erfolgen sollte.

Professionalisierung der Datenschutzbeauftragten

Für die Umsetzung des Datenschutzes hat die oder der Datenschutzbeauftragte mit den Aufgaben der Beratung, Schulung, Sensibilisierung und Überwachung eine besondere Bedeutung. Daher kommt es darauf an, dass diese Aufgabe kompetent, professionell und routiniert wahrgenommen wird. Die Erfüllung dieser Aufgaben ist schwierig und unter Umständen konfliktanfällig. Mit Recht beschreiben die gesetzlichen Vorschriften daher umfassend die Benennung, die Stellung und die Aufgaben der oder des Datenschutzbeauftragten.[16] Aufgrund der hohen Anforderungen, die an Datenschutzbeauftragte gestellt werden, ist es für öffentliche Stellen mit beschränkten Ressourcen – wie kleinere Gemeinden oder Schulen – mitunter herausfordernd, diese Position zu besetzen und ausreichende Ressourcen zur Erfüllung der mit der Funktion einhergehenden Aufgaben zur Verfügung zu stellen. Es gilt somit, kreative Lösungsansätze zu entwickeln.

Hier könnte die Bündelung der Ressourcen für „Datenschutzbeauftragte“ zu einem effektiveren Datenschutz beitragen. Die Vorschriften der Art. 37

16 S. hierzu auch HBDI, Behördliche und betriebliche Datenschutzbeauftragte, https://datenschutz.hessen.de/datenschutz/datenschutzbeauftragte/behoerdliche-und-betriebliche-datenschutzbeauftragte-nach-neuem-recht.

Abs. 3 DS-GVO und § 5 Abs. 2 HDSIG sehen insoweit ausdrücklich vor, dass für mehrere öffentliche Stellen, unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe, gemeinsame Datenschutzbeauftragte benannt werden können.

Im Berichtszeitraum habe ich das Hessische Kultusministerium zu der Frage beraten, inwieweit an Schulen durch eine bessere Zuordnung der Stellenanteile „Datenschutzbeauftragter" einerseits eine Entlastung der Schulen und andererseits eine effektivere und effizientere Umsetzung des Datenschutzes erreicht werden kann. Gemeinsam wurde eine Arbeitsgruppe gebildet, die untersucht, wie auf der Grundlage der bestehenden Vorschriften eine Zentralisierung, Kompetenzbildung, Routinisierung und Professionalisierung in der Erfüllung der Aufgaben der Datenschutzbeauftragten erreicht werden kann. Die neue Landesregierung zeigt, dass sie sich der Bedeutung des Datenschutzrechts im Schulumfeld bewusst ist.[17] Ich freue mich daher auf eine Fortsetzung der lösungsorientierten und kooperativen Zusammenarbeit im kommenden Berichtszeitraum.

Technikauswahl und -gestaltung

Insbesondere in den Bereichen der Digitalisierung der Landesverwaltung und der Schulen hat sich eine gute Zusammenarbeit zwischen den Ressorts und mir hinsichtlich der Beratung bei der Entwicklung von IT-Projekten und -Verfahren ergeben. In den für den Datenschutz wichtigen Fragen der Technikauswahl und der Systemgestaltung werde ich frühzeitig und umfassend beratend eingebunden (s. Kap. 6.2 und 14.2).

Hinsichtlich der Technikauswahl geht es vor allem darum, die langfristigen Möglichkeiten datenschutzgerechter Gestaltung zu gewährleisten und datenschutzrechtliche Kriterien der Technikauswahl zu konkretisieren. Dabei ist – soweit möglich – auf digitale Souveränität in dem Sinn zu achten, dass die Fähigkeit, Datenschutz einzuhalten, gewahrt wird. Sind die Techniksysteme nicht unter Berücksichtigung des Datenschutzes entwickelt worden, fällt es den Verantwortlichen, die sie nutzen, oft schwer, ihrer Verantwortung nach der DS-GVO gerecht zu werden. Aus den gleichen Gründen sind auch Abhängigkeiten und Lock-in-Situationen zu vermeiden und Wechselmöglichkeiten zu erhalten. Die Weiterentwicklung von IT-Systemen kann – wie man am Beispiel von MS 365 sehen kann (s. Kap. 1.2) – leicht dazu führen, dass das neue System bereits gefundene datenschutzkonforme Gestaltungen oder Schutzvorkehrungen nicht mehr zulässt. Um dann zu einer datenschutzge-

17 S. Koalitionsvertrag zwischen CDU und SPD für die 21. Legislaturperiode 2024–2029, S. 11 und 17.

rechten Alternative wechseln zu können, sind z. B. Open Source- oder Multi Cloud-Strategien zu bevorzugen.

Hinsichtlich der Systemgestaltung sind die Möglichkeiten, das System auch an die datenschutzrechtlichen Bedingungen der nutzenden Organisation anzupassen und zu konfigurieren, schon bei der Systemauswahl zu berücksichtigen. Wie die Beispiele Videokonferenzsysteme an Schulen und Hochschulen in Hessen (s. 51. Tätigkeitsbericht, Kap. 3.2 und 3.3) zeigen, kann eine Beratung und Unterstützung durch Datenschutzbeauftragte und Aufsichtsbehörden zu gemeinsamen konstruktiven Lösungen führen, die Funktionalität und Datenschutz gleichermaßen ermöglichen.

Wird der Datenschutz bei Systemauswahl und -gestaltung frühzeitig und hinsichtlich aller relevanten Aspekte berücksichtigt, erspart dies dem Verantwortlichen Zeit und Kosten für nachträgliche Korrekturen und vermeidet Datenschutzverstöße und Datenschutzverletzungen. Für die Datenschutzaufsichtsbehörde erweist sich der Einsatz für präventive Beratung als viel effektiver und effizienter als nachträgliche Versuche repressiver Korrektur. Für die Durchsetzung der Grundrechte erweist sich diese Vorgehensweise als viel hilfreicher als die Bearbeitung von Beschwerden und Meldungen im jeweiligen Einzelfall, die durch eine datenschutzgerechte Auswahl und Gestaltung der Datenverarbeitungsverfahren vermieden worden wären.

1.4
Mitwirkung in deutschen und europäischen Datenschutzgremien

Obwohl die Datenschutzaufsichtsbehörden vollständig unabhängig sind, müssen sie nach Art. 51 DS-GVO zusammenarbeiten, um zu einem einheitlichen Vollzug des Datenschutzrechts zu gelangen. Daher ist die Mitarbeit im Europäischen Datenschutzausschuss (EDSA) und in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) unabdingbar. Beide Gremien haben entscheidenden Einfluss auf das Verständnis und die Auslegungen des Datenschutzrechts und auf die Arbeit der Aufsichtsbehörden. Wer darauf einwirken will, wie der Datenschutz künftig in der Union und in Deutschland verstanden und praktiziert wird, muss sich aktiv in die Arbeit des EDSA und der DSK sowie ihrer Arbeitskreise einbringen.

Mitarbeit im Europäischen Datenschutzausschuss

Der EDSA hat im Wesentlichen zwei Aufgaben (s. näher Art. 70 DS-GVO). Er legt zum einen in Form von Empfehlungen, Leitlinien und Stellungnahmen abstrakt fest, wie Regelungen in der DS-GVO im Praxisvollzug zu verstehen sind. Zum anderen entscheidet er bei Streitfragen, die zwischen den

Aufsichtsbehörden entstehen (s. Kap. 2.1). Mit diesen Entscheidungen kann er nationale Aufsichtsbehörden überregeln und zu bestimmten Handlungen anweisen.

Im EDSA hat Deutschland eine Stimme. Vertreten wird Deutschland gemäß § 17 BDSG derzeit vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem bayerischen Landesdatenschutzbeauftragten. Zu Fragen, die im EDSA zu entscheiden sind, müssen sich die Datenschutzaufsichtsbehörden des Bundes und der Länder jeweils auf eine gemeinsame Stellungnahme nach § 18 BDSG verständigen. Diese wird in der Datenschutzkonferenz erarbeitet und entschieden. Insofern bin auch ich indirekt an der Entscheidungsfindung im EDSA beteiligt.

Die Mitarbeit im EDSA findet überwiegend in den thematisch ausgerichteten Unterarbeitsgruppen („Expert Subgroups“) statt. Diese bereiten Entscheidungen, Empfehlungen, Leitlinien und Stellungnahmen des EDSA vor. Ich vertrete die Bundesländer in den Expert Subgroups „Border Travel and Law Enforcement“, „Financial Matters“ sowie dem Coordinated Supervision Committee (CSC), der EURODAC Supervision Coordination Group, der VIS Supervision Coordination Group und der SIS II Supervision Coordination Group, bin Stellvertreter in der Subgroup „International Transfer“ sowie der „Task Force Administrative Fines“ und arbeite in der „Compliance, eGovernment and Health Expert Subgroup“ an den Leitlinien zur wissenschaftlichen Forschung sowie einem von dieser Subgroup federführend bearbeiteten Zertifizierungsverfahren mit.

Mitarbeit in der Datenschutzkonferenz

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 Koordination findet überwiegend in der Datenschutzkonferenz statt (s. näher 51. Tätigkeitsbericht, Kap. 1). Sie 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 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. Die Task

Force „Forschungsdaten“ hat im Berichtszeitraum vier Stellungnahmen und Entschließungen erarbeitet, die von der DSK übernommen worden sind (s. Kap. 13.1).

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. Weiterhin hat sie nach den Änderungen im Jahr 2022 – vor allem zu verbindlichen Mehrheitsentscheidungen (s. 51. Tätigkeitsbericht, Kap. 1) – im Berichtszeitraum ihre Geschäftsordnung – wieder unter meiner Leitung – dahingehend weiterentwickelt, dass sie Regelungen zur Stellvertretung des Vorsitzes, zur Abwahl des Vorsitzes, zur Festlegung der Tagesordnungen, zur Durchführung von Umlaufverfahren und zur Änderung der Geschäftsordnung getroffen hat.

Das Bundesinnenministerium hat im Berichtszeitraum einen Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes erarbeitet, der inzwischen von der Bundesregierung beschlossen worden ist. In diesem wird in einem neuen § 16a die Datenschutzkonferenz gesetzlich eingerichtet und werden ihre Mitglieder bestimmt. Die Datenschutzkonferenz gibt sich eine Geschäftsordnung. Durch diese Regelung wird sich an der Zusammensetzung der DSK und der Praxis ihrer Zusammenarbeit nichts ändern. Sie ist mit dem Inkrafttreten des Gesetzes jedoch kein freiwilliger Zusammenschluss aller unabhängigen Datenschutzaufsichtsbehörden in Deutschland, sondern eine gesetzlich eingerichtete Institution mit Zwangsmitgliedschaft.

2. Europäische und internationale Zusammenarbeit

Die Europäisierung des Datenschutzrechts setzt eine intensive Zusammenarbeit zwischen den Aufsichtsbehörden der Mitgliedstaaten voraus, 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 die Mitarbeit der deutschen Aufsichtsbehörden im europäischen Datenschutzverbund unabdingbar (Kap. 2.1). Das EU-US Data Privacy Framework und der Angemessenheitsbeschluss der Europäischen Kommission haben eine neue Grundlage für Datentransfers in die USA geschaffen. Diese sind jedoch an bestimmte Bedingungen geknüpft, so dass ein großer Beratungsbedarf für Datenexporteure entstanden ist, dem die DSK mit Anwendungshinweisen entspricht (Kap. 2.2). Viele Datentransfers können auch auf Binding Corporate Rules gestützt werden. Hierzu hat der EDSA Empfehlungen für Verantwortliche beschlossen (Kap. 2.3).

2.1
Zusammenarbeit mit anderen europäischen Aufsichtsbehörden

Die DS-GVO verpflichtet die europäischen Datenschutzaufsichtsbehörden, in Fällen grenzüberschreitender Datenverarbeitungen, im Bemühen einen Konsens zu erzielen (Art. 60 Abs. 1 Satz 1 DS-GVO), eng zu kooperieren.

Verfahren der Kooperation und Kohärenz nach Kapitel VII DS-GVO

In allen grenzüberschreitenden Aufsichtsverfahren, denen eine grenzüberschreitende Verarbeitung personenbezogener Daten gemäß Art. 4 Nr. 23 DS-GVO zugrunde liegt, muss ich als federführende oder als betroffene Aufsichtsbehörde mit Aufsichtsbehörden anderer Mitgliedstaaten der EU zusammenarbeiten. Die Zusammenarbeit, Abstimmung und Kommunikation erfolgt elektronisch über das sog. „IMI-System“ (Internal Market Information-System, deutsch: Binnenmarkt-Informationssystem). Die Arbeitssprache im IMI-System ist Englisch (s. hierzu ausführlich 51. Tätigkeitsbericht Kap. 4.1).

Die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden arbeiten im Kooperationsverfahren eng zusammen und versuchen, einen Konsens zu erzielen. Die federführende Aufsichtsbehörde prüft den Fall und legt entsprechend Art. 60 Abs. 3 Satz 2 DS-GVO den betroffenen Aufsichtsbehörden nach Abschluss der Ermittlungen einen Beschlussentwurf vor. Gegen diesen Beschlussentwurf können nach Art. 60 Abs. 4 DS-GVO die betroffenen Aufsichtsbehörden Einspruch einlegen. Bei unlösbaren Meinungsverschiedenheiten wird die Angelegenheit dem Europäischen Da-

tenschutzausschuss (EDSA) im Kohärenzverfahren nach Art. 63 DS-GVO zur verbindlichen Entscheidung vorgelegt.

Die Zahl der über das IMI-System gemeldeten Beschwerden, Anfragen und Art. 33-Meldungen pendelte sich im Berichtszeitraum erneut etwa auf dem Vorjahresniveau ein.

Europäisches Verfahren	Anzahl 2019	Anzahl 2020	Anzahl 2021	Anzahl 2022	Anzahl 2023
Art. 56-Verfahren gesamt	633	812	1.419	645	562
Art. 56-Verfahren mit Betroffenheit	17	32	47	11	13
Art. 56-Verfahren mit Federführung	4	7	16	2	4
Art. 61-Verfahren (Amtshilfe)	65	26	92	155	144

Tabelle: Europäische Verfahren

Im Berichtszeitraum waren von der Stabsstelle Europa und Internationales insgesamt 562 im IMI-System eingetragene Art. 56-Verfahren auf eine mögliche Betroffenheit oder Federführung zu prüfen. In 13 dieser Verfahren habe ich mich als „betroffen“ gemeldet, in vier Verfahren habe ich die Bearbeitung der Beschwerde als federführende Aufsichtsbehörde übernommen.

Der im Berichtsjahr gegenüber den Vorjahren zu verzeichnende Rückgang der Art. 56-Verfahren erklärt sich unter anderem 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.

Rekordgeldbußen gegen Social Media-Plattformen

Im Berichtsjahr haben einige Kooperations- und Kohärenzverfahren nach Kapitel VII DS-GVO erneut zu vielbeachteten Maßnahmen und hohen Geldbußen geführt. Große mediale Beachtung fand unter anderem die von der irischen Data Protection Commission (DPC) gegen die Meta Platforms Ireland Limited (Irland) verhängte Geldbuße in Rekordhöhe von 1,2 Milliarden Euro

wegen unzulässiger Drittlandübermittlungen in die USA. Die Geldbuße stellt bisher die höchste unter der DS-GVO verhängte Geldbuße dar.

Die neue Rekordgeldbuße reiht sich in eine Reihe zahlreicher Geldbußen gegen den Meta-Konzern ein. Sie hat eine lange Vorgeschichte: Im Nachgang zum Schrems II-Urteil des EuGH vom 16. Juli 2020 (C-311/18) leitete die DPC Untersuchungen bei Meta Ireland ein und stellte dabei fest, dass die von der Meta-Tochter Facebook durchgeführten Übermittlungen personenbezogener Daten von Facebook-Nutzern aus der EU in die USA nicht im Einklang mit der DS-GVO stehen. Zwar hat Meta Ireland den US-Datentransfer auf das aktuelle Set der Standardvertragsklauseln (Standard Contractual Clauses, kurz: SCCs) gestützt und darüber hinaus zusätzliche Maßnahmen zum Schutz der Daten ergriffen. Diese Maßnahmen waren allerdings unzureichend. Nach Ansicht der DPC verstieß Meta gegen Art. 46 Abs. 1 DS-GVO, da die Übermittlungen unter Umständen erfolgten, die kein im Wesentlichen gleichwertiges Schutzniveau wie das der DS-GVO gewährleisten. Weder die von Meta verwendeten SCCs, noch die ergriffenen zusätzlichen Maßnahmen könnten das fehlende Schutzniveau ausgleichen und Meta könne sich nicht auf Ausnahmen vom Übermittlungsverbot berufen.

Ursprünglich beabsichtigte die DPC trotz des festgestellten Verstoßes nicht, Meta mit einer Geldbuße zu belegen, sondern wollte es bei einer Anweisung belassen. Allerdings war die DPC im Kooperationsverfahren nach Art. 63 Abs. 3 DS-GVO dazu verpflichtet, ihren Beschlussentwurf an die anderen betroffenen europäischen Datenschutzaufsichtsbehörden (darunter an mich) zur Stellungnahme zu übermitteln. Einige der betroffenen Aufsichtsbehörden waren mit dem Beschlussentwurf der DPC nicht einverstanden. Die deutschen Aufsichtsbehörden bemängelten, dass es keine Geldbuße geben sollte und der Umgang mit den rechtswidrig übermittelten Daten nicht geregelt wurde. Da auf die Einsprüche der betroffenen Aufsichtsbehörden hin keine Einigung mit der DPC erzielt werden konnte, musste der EDSA die DPC in einem Streitbeilegungsverfahren nach Art. 65 DS-GVO mit verbindlichem Beschluss anweisen, Meta mit einer Geldbuße zu belegen und Meta aufzugeben, die Datenverarbeitung mit der DS-GVO in Einklang zu bringen.

Daraufhin hat die DPC die Geldbuße in Höhe von 1,2 Milliarden Euro verhängt und Meta Ireland zudem angewiesen, die beanstandeten Datenübermittlungen unter Rückgriff auf SCCs beim Datentransfer von Facebook-Nutzerdaten aus der EU in die USA auszusetzen. Außerdem musste Facebook seine Verarbeitungsvorgänge innerhalb von sechs Monaten mit der DS-GVO in Einklang bringen. Meta hat Rechtsmittel gegen die Verhängung der Geldbuße eingelegt.

Genehmigung von verbindlichen internen Datenschutzvorschriften

Neben den über das IMI-System zu bearbeitenden grenzüberschreitenden Verwaltungsverfahren lag auch im Berichtsjahr ein weiterer Schwerpunkt in der Zusammenarbeit der EU in der Prüfung und Genehmigung von verbindlichen internen Datenschutzvorschriften (sog. Binding Corporate Rules, kurz: BCR) nach Art. 47 DS-GVO, die sich – nicht zuletzt seit dem sog. Schrems II-Urteil 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. Dieser Trend hat sich im Berichtsjahr auch nach Erlass des neuen Angemessenheitsbeschlusses der EU-Kommission für die USA auf der Grundlage des sog. EU-US Data Privacy Frameworks weiter fortgesetzt.

Bevor BCR wirksam werden können, müssen sie in einem europaweiten Kooperationsverfahren von Aufsichtsbehörden mehrerer Mitgliedstaaten gemeinsam geprüft und von der federführenden Aufsichtsbehörde genehmigt worden sein (s. zu BCR und zum Prüfverfahren 51. TB Kap. 4.1).

Da Hessen häufig Standort von großen global agierenden Unternehmensgruppen ist, bin ich häufig in BCR-Genehmigungsverfahren federführend. Im Berichtsjahr war ich in vier laufenden BCR-Genehmigungsverfahren als europaweiter BCR Lead federführend zuständig. Zusätzlich sind die jährlichen Updates der bereits bestehenden BCR-Inhaber zu prüfen. In zwei weiteren Verfahren habe ich die Co-Prüfung und in weiteren drei neuen Verfahren die innerdeutsche Federführung übernommen.

Erfreulich war, dass im Berichtszeitraum das Genehmigungsverfahren für die BCR-C und BCR-P von Cerner Health Services Deutschland GmbH zu einer positiven Stellungnahme des EDSA führte.

Mitarbeit in Gremien des EDSA

Auch im Berichtszeitraum habe ich Deutschland in der International Transfers Subgroup des EDSA vertreten und in diversen Drafting Teams und Task Forces dieser Subgroup mitgewirkt (s. hierzu ausführlich 51. TB Kap. 4.1). Durch diese Mitarbeit auf europäischer Ebene gelingt es, Einfluss auf vom EDSA zu verabschiedende Leitlinien und Empfehlungen zu nehmen, die dann für die spätere aufsichtsbehördliche Tätigkeit maßgeblich und richtungsweisend werden.

Auch die Diskussionen und Ergebnisse aus dem EDSA und seinen anderen Subgroups (z. B. Arbeitspapiere und -ergebnisse, Tagesordnungen und Protokolle) müssen zur Kenntnis genommen und berücksichtigt werden. Nur so kann die hessische Aufsichtsbehörde sich aktiv und gestaltend in

die Arbeiten auf europäischer Ebene einbringen 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 nehmen.

2.2
Neuer Angemessenheitsbeschluss zum Datentransfer in die USA

Die Europäische Kommission hat am 10. Juli 2023 einen neuen Angemessenheitsbeschluss zum Datentransfer in die USA auf der Grundlage des sog. EU-US Data Privacy Framework (EU-US DPF) erlassen. Seither können personenbezogene Daten aus der EU an unter dem EU-US DPF zertifizierte Datenempfänger in den USA übermittelt werden, ohne dass weitere Übermittlungsinstrumente oder zusätzliche Maßnahmen erforderlich sind.

Vor- und Entstehungsgeschichte des EU-US DPF

Wer personenbezogene Daten in die USA oder andere Drittländer übermitteln will, muss sich an das europäische Datenschutzrecht halten. Die DS-GVO lässt einen Datentransfer in Drittländer nur unter bestimmten Bedingungen zu, um auch bei der Übermittlung und Weiterverarbeitung ein gleichwertiges Datenschutzniveau aufrechtzuerhalten. Die EU-Kommission kann in einem Angemessenheitsbeschluss die Gleichwertigkeit des Datenschutzniveaus feststellen.

Frühere Angemessenheitsbeschlüsse für die USA hatte der EuGH insbesondere aufgrund der weitreichenden Befugnisse für US-Sicherheitsbehörden, auf die personenbezogenen Daten zuzugreifen, und unzureichender Rechtsschutzmöglichkeiten für Betroffene für ungültig erklärt: im Jahr 2015 „Safe Harbor“ und im Jahr 2020 das sog. „Privacy Shield“.

Mit der Ungültigerklärung des Angemessenheitsbeschlusses zum Privacy Shield bestand in der Praxis zuletzt eine Lücke für transatlantische Datenübermittlungen, die durch den neuen Angemessenheitsbeschluss zum EU-US DPF, dem mehrjährige Verhandlungen zwischen der EU und den USA vorangingen, geschlossen wurde.

Im März 2022 hatten die Präsidentin der Europäischen Kommission und der Präsident der Vereinigten Staaten von Amerika zunächst eine grundsätzliche Einigung über einen neuen transatlantischen Datenschutzrahmen verkündet. Im Oktober 2022 erließ der US-Präsident ein Dekret, die Executive Order 14086, die zusammen mit den regulations des US-Justizministers die grundsätzliche Einigung vom März 2022 in Rechtsvorschriften umsetzte und die Kritikpunkte des EuGH im Schrems II-Urteil adressierte. Die Europäische

Kommission veröffentlichte daraufhin im Dezember 2022 den Entwurf des Angemessenheitsbeschlusses zum EU-US DPF (s. hierzu auch 51. Tätigkeitsbericht Kap. 2). Hierzu gaben die Aufsichtsbehörden im EDSA gemeinsam eine durchaus kritische Stellungnahme ab.[18] Dennoch wurde der Beschlussentwurf von den Mitgliedstaaten im sogenannten Komitologieverfahren bestätigt und der Angemessenheitsbeschluss zum EU-US DPF daraufhin von der Europäischen Kommission am 10. Juli 2023 angenommen. Er trat am selben Tag in Kraft.

Anwendungsbereich des EU-US DPF und Prüfpflicht für Datenexporteure

Der Angemessenheitsbeschluss zum EU-US DPF ist sektoral und erfasst nur Datenübermittlungen an US-Organisationen, die sich unter dem EU-US DPF zertifiziert haben. Dies bedeutet, dass es sich nicht um einen umfassenden Angemessenheitsbeschluss für die gesamten USA handelt. Datenexporteure müssen daher prüfen, ob ihre geplanten Datenübermittlungen in den Anwendungsbereich des Beschlusses fallen und damit auf Grundlage dieses Übermittlungsinstrumentes vorgenommen werden können.

Eine Selbstzertifizierung steht bislang lediglich US-Organisationen offen, die der Aufsicht der US Federal Trade Commission (FTC, eine eigenständige US-Bundesbehörde, die für Wettbewerbskontrolle sowie Verbraucherschutz zuständig ist) oder des US Department of Transportation (DOT, US-Verkehrsministerium) unterliegen. Das EU-US DPF enthält allerdings den Hinweis, dass zukünftig gegebenenfalls Zuständigkeiten weiterer US-Behörden hinzukommen können.

Das US Department of Commerce (DOC, US-Handelsministerium) unterhält und veröffentlicht eine „Data Privacy Framework List“,[19] welche diejenigen US-Organisationen auflistet, die ihre Selbstzertifizierung unter dem EU-US DPF abgeschlossen haben. Auf dieser Liste wurden bereits kurz nach Inkrafttreten des EU-US-DPF zahlreiche US-Organisationen geführt. Nur Übermittlungen an dort aufgelistete US-Organisationen können auf den EU-US DPF gestützt werden.

---

18 EDSA, Stellungnahme 5/2023 zum Entwurf eines Durchführungsbeschlusses der Europäischen Kommission über die Angemessenheit des Schutzes personenbezogener Daten im Rahmen des Datenschutzrahmens EU-USA, https://edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_de.pdf.

19 https://www.dataprivacyframework.gov/s/participant-search.

Betroffenenrechte

Die gegenüber Verantwortlichen und Auftragsverarbeitern vorgesehenen Betroffenenrechte umfassen ein Recht auf Berichtigung oder Ergänzung unrichtiger oder unvollständiger personenbezogener Daten, ein Recht auf Löschung rechtswidrig verarbeiteter Daten sowie ein Auskunftsrecht. Betroffenen stehen darüber hinaus verschiedene Rechtsbehelfe offen. Dazu gehören unentgeltliche unabhängige Streitbeilegungsmechanismen und eine Schiedsstelle.

Zugriff auf personenbezogene Daten durch öffentliche Stellen der USA

Im Angemessenheitsbeschluss werden die gesetzlichen Grundlagen, Grenzen und Schutzmechanismen wiedergegeben, die für die Erhebung und Nutzung personenbezogener Daten durch öffentliche Stellen der USA zu Strafverfolgungszwecken oder aus Gründen der nationalen Sicherheit gelten. In aller Regel erfordern danach Zugriffe zu Strafverfolgungszwecken eine gerichtliche Anordnung, die hinreichende Verdachtsgründe im Einzelfall voraussetzt und den Umfang der zu erhebenden personenbezogenen Daten auf das für die Zwecke der Strafverfolgung erforderliche Maß begrenzt.

Beratungsbedarf und Anwendungshinweise der DSK

Seit Erlass des neuen Angemessenheitsbeschlusses haben sich zahlreiche Unternehmen und öffentliche Stellen mit Fragen dazu, wie mit dem neuen „Datenschutzrahmen“ umzugehen ist, an mich gewandt. Auch Bürgerinnen und Bürger wollen wissen, was dieser neue Beschluss bedeutet. Viele Informationen der Europäischen Kommission und des EDSA lagen zunächst nur in englischer Sprache vor und waren für Laien nur schwer verständlich.

Daher hat eine Arbeitsgruppe des Arbeitskreises Internationaler Datenverkehr, in der ich mitgearbeitet habe, Anwendungshinweise zu dem Angemessenheitsbeschluss zum EU-US Data Privacy Framework erarbeitet. Diese wurden am 4. September 2023 durch die DSK verabschiedet und sowohl auf der DSK-Website[20] als auch der HBDI-Website[21] veröffentlicht. Nach einer Einführung zum Datenschutz bei Drittlandsübermittlungen enthalten diese Anwendungshinweise einerseits Informationen für Datenexporteure, also Verantwortliche und Auftragsverarbeiter, die Daten in die USA übermitteln,

20 https://datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf.

21 https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/eu-us-data-privacy-framework-in-kraft-getreten.

andererseits erfahren betroffene Personen, welche Rechtsschutz- und Beschwerdemöglichkeiten sie haben.

Mutmaßlich nur vorübergehend Rechtssicherheit

Mit dem neuen Angemessenheitsbeschluss für den Datenaustausch mit den USA dürfte mutmaßlich nur vorübergehend wieder mehr Rechtssicherheit bestehen. Zum jetzigen Zeitpunkt handelt es sich bei dem Angemessenheitsbeschluss um geltendes EU-Recht. Aber neben den vorgesehenen Evaluationen durch die EU-Kommission, aus denen Anpassungen oder eine Aufhebung resultieren können, ist damit zu rechnen, dass auch die Nachfolgeregelung zu „Safe Harbor“ und „Privacy Shield“, wie die beiden Vorgängerabkommen, gerichtlich überprüft werden wird und letztlich der EuGH über die Rechtmäßigkeit entscheiden wird.

2.3
Empfehlungen des EDSA für Binding Corporate Rules für Verantwortliche

Im Juni 2023 hat der Europäische Datenschutzausschuss (EDSA) mit den „Recommendations on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)“ nach erfolgter öffentlicher Konsultation neue Empfehlungen zu Binding Corporate Rules für Verantwortliche (sog. Controller-BCR oder kurz: BCR-C) verabschiedet. Ich war zuvor in der International Transfers Subgroup als Co-Berichterstatter intensiv in die Erarbeitung dieser Empfehlungen involviert.

Zusätzliche Erläuterungen und Anforderungen

Die neuen Empfehlungen des EDSA[22] ersetzen und aktualisieren die vorherigen Arbeitsdokumente der Artikel-29-Datenschutzgruppe zu inhaltlichen Anforderungen an BCR-C (WP256rev.01) und das Standardantragsformular zur Genehmigung von BCR-C (WP264), indem sie beide Arbeitsdokumente zu einem Dokument zusammenführen.

Sie bieten zusätzliche Orientierungshilfen und sollen gleiche Wettbewerbsbedingungen für alle BCR-Antragsteller gewährleisten. Die neuen Empfehlungen enthalten daher sowohl ein formal überarbeitetes und aktualisiertes Antragsformular für BCR-C als auch Erläuterungen dazu, was notwendiger Inhalt von BCR-C ist. Sie treffen dabei eine genauere Unterscheidung zwi-

22 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-12022-application-approval-and_en.

schen dem, was in den BCR-C selbst enthalten sein muss, und dem, was dem sog. BCR Lead im BCR-Antrag vorgelegt werden muss, als dies noch im WP256rev.01 der Fall war.

Zudem berücksichtigen die neuen Empfehlungen die Verabredungen, die die EU- und EWR-Datenschutzbehörden im Laufe der Genehmigungsverfahren für konkrete BCR-Anträge seit Inkrafttreten der DS-GVO getroffen haben, und legen damit weitreichendere Anforderungen als zuvor fest.

Berücksichtigung der „Schrems II"-Rechtsprechung des EuGH

Insbesondere hat der EDSA mit seinen neuen Empfehlungen die inhaltlichen Anforderungen an BCR-C mit den Anforderungen aus dem sog. Schrems II-Urteil des EuGH vom 16. Juli 2020 (C-311/18) in Einklang gebracht. So wird in den Empfehlungen klargestellt, dass auch Unternehmensgruppen oder Gruppen von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, die BCR-C als Transferwerkzeug für gruppeninterne Datentransfers in Drittländer verwenden wollen, im Sinne sog. „Transfer Impact Assessments" (kurz: TIA) die Rechtslage im jeweiligen Datenempfängerland vorab umfassend dahingehend prüfen müssen, ob ein Risiko des Zugriffs von Sicherheitsbehörden im jeweiligen Datenempfängerland besteht.

Abhängig von den Ergebnissen des TIA sind ggf. ergänzend zu den BCR-C zusätzliche Maßnahmen (sog. supplementary measures) erforderlich, um den datenschutzrechtlichen Anforderungen der DS-GVO an die Übermittlung personenbezogener Daten in Drittländer gerecht zu werden. Insoweit nehmen die neuen Empfehlungen des EDSA zu BCR-C nun ausdrücklich Bezug auf die „Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten"[23], die der EDSA im November 2020 angenommen hat.

Handlungsbedarf für Antragsteller und Inhaber von Binding Corporate Rules

Zu beachten ist, dass die neuen Vorgaben aus den Empfehlungen nicht nur bei neuen Genehmigungsanträgen für BCR-C umzusetzen sind. Auch bereits genehmigte BCR-C sind von den BCR-Inhabern einer sorgfältigen Prüfung dahingehend zu unterziehen, ob sie den neuen behördlichen Vorgaben ausreichend Rechnung tragen, und ggf. zu überarbeiten. Ich erwarte von

23 https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

BCR-Inhabern, dass bereits genehmigte BCR-C im Rahmen des jährlichen Updates im Jahr 2024 mit den neuen Anforderungen in Einklang gebracht werden.

Handlungsbedarf kündigt sich zudem auch bereits für Antragsteller und Inhaber von BCR für Auftragsverarbeiter (sog. Processor-BCR oder kurz: BCR-P) an. Denn aktuell werden auch für BCR-P neue Empfehlungen in der International Transfers Subgroup des EDSA erarbeitet, die im Jahr 2024 verabschiedet werden sollen. Bis dahin sind für BCR-P weiterhin insbesondere die Arbeitspapiere WP257rev.01 und WP265 von Relevanz.

3. Verfahren vor Gerichten und zur Verhängung von Geldbußen

Die DS-GVO führt zu einer zunehmenden Juridifizierung der Aufsichtstätigkeit (s. 51. Tätigkeitsbericht Kap. 1). Auch im Berichtszeitraum hat die Zahl der Gerichtsverfahren (Kap. 3.1) und der Verfahren zur Verhängung einer Geldbuße (Kap. 3.3) jeweils wieder zugenommen. Die Leitlinien des EDSA für die Berechnung von Geldbußen (Kap. 3.2) und die Entscheidung des EuGH vom 5. Dezember 2023 zu Deutsche Wohnen (Kap. 3.4) haben die Rechtssicherheit hinsichtlich der Verhängung von Geldbußen gestärkt und dadurch die Aufsichtstätigkeit erleichtert.

3.1 Gerichtsverfahren

Auch sechs Jahre nach dem Wirksamwerden der DS-GVO bestehen noch zahlreiche ungeklärte Fragen zur Auslegung des Datenschutzrechts. In diesem Jahr fällte der Europäische Gerichtshof (EuGH) in drei Vorabentscheidungsverfahren, denen Verwaltungsstreitverfahren gegen mich vor dem Verwaltungsgericht Wiesbaden zugrunde liegen, bedeutende Entscheidungen. Dennoch konnte ich im Vergleich zum Vorjahr einen leichten Rückgang bezüglich der neuen gerichtlichen Verfahren gegen meine Behörde verzeichnen.

Überblick

Im Berichtsjahr wurden 17 neue Verwaltungsstreitverfahren gegen mich bei dem gemäß § 20 Abs. 3 BDSG zuständigen Verwaltungsgericht Wiesbaden rechtshängig. Die Klägerinnen und Kläger suchten unter anderem gerichtlichen Rechtsschutz gegen Entscheidungen in den Bereichen Videoüberwachung, Auskunfteien, Banken, Gesundheit, Werbung, Beschäftigtendatenschutz und Presse. Fünf der Verfahren hatten Klagen der Verantwortlichen gegen meine Anordnungen nach Art. 58 Abs. 1 und 2 DS-GVO zum Gegenstand. Die Mehrzahl der gerichtlichen Verfahren wurde jedoch von Beschwerdeführerinnen und Beschwerdeführern angestrengt, die mit meiner abschließenden Bewertung ihrer Beschwerden nicht einverstanden waren. In diesem Jahr kamen sechs weitere Rechtsmittelverfahren vor dem Hessischen Verwaltungsgerichtshof (VGH) hinzu. Zusätzlich gab mir das Bundesverfassungsgericht in drei Verfahren zu Verfassungsbeschwerden Gelegenheit zur Stellungnahme.

EuGH-Entscheidung C-26/22, C-64/22 und C-634/22

Ende 2023 äußerte sich der EuGH in den medial viel beachteten Urteilen in den Rechtssachen C-26/22, C-64/22 und C-634/22 zur Arbeitsweise von Wirtschaftsauskunfteien, dem Charakter von Beschwerden an die Datenschutzaufsichtsbehörden und von datenschutzrechtlichen Verhaltensregeln von Wirtschaftsverbänden (s. auch Kap. 1.1, 11.2 und 11.3).

Den verbundenen Rechtssachen C-26/22 und C-64/22 gingen zwei Beschwerden nach Art. 77 DS-GVO von betroffenen Personen bei meiner Behörde voraus. Den Klägern wurde jeweils im Rahmen von Insolvenzverfahren eine vorzeitige Restschuldbefreiung erteilt. Diese Informationen wurden im Internet gemäß § 9 Abs. 1 InsO und § 3 Abs. 1 und 2 InsBekV veröffentlicht und sechs Monate nach der Veröffentlichung wieder gelöscht. Die SCHUFA Holding AG speicherte diese veröffentlichten Informationen in ihrem Datenbestand dagegen für drei Jahre. Dies entsprach der Festlegung in den genehmigten Verhaltensregeln des Verbands der Wirtschaftsauskunfteien. Das Verwaltungsgericht Wiesbaden richtete mehrere Vorlagefragen an den EuGH, ob diese Verfahrensweise mit der DS-GVO vereinbar sei.

Auch der Rechtssache C-634/21 lag eine Beschwerde einer betroffenen Person bei mir gegen die SCHUFA Holding AG und ein Vorlagebeschluss des Verwaltungsgerichts Wiesbaden zugrunde. In diesem Verfahren ging es vor allem um die Frage, ob die Erstellung eines Bonitäts-Scores durch die Auskunftei und dessen Verwendung durch ein Kreditinstitut bei der Entscheidung über eine Kreditvergabe eine unzulässige automatisierte Entscheidung im Sinn des Art. 22 Abs. 1 DS-GVO darstellt.

Die mündlichen Verhandlungen fanden im Januar 2023 statt. Im März 2023 stellte der Generalanwalt P. Pikamäe seine Schlussanträge, denen der EuGH in seinen Entscheidungen vom 7. Dezember 2023 weitgehend folgte:

– Private Wirtschaftsauskunfteien dürfen in ihren eigenen Datenbanken aus öffentlichen Registern stammende Informationen über die Erteilung einer Restschuldbefreiung zum Zweck der Lieferung von Auskünften über die Kreditwürdigkeit nicht länger speichern als das öffentliche Insolvenzregister – folglich nicht länger als sechs Monate. Nach dem EuGH soll die erteilte Restschuldbefreiung nämlich der betroffenen Person ermöglichen, sich erneut am Wirtschaftsleben zu beteiligen, und hat daher für sie existenzielle Bedeutung. Jedenfalls nach Ablauf der sechs Monate überwiegen die Rechte und Interessen der betroffenen Person diejenigen der Öffentlichkeit und der Kreditwirtschaft, über diese Information zu verfügen. Rechtswidrig gespeicherte Daten sind zu löschen.

– Bis zur Entscheidung des EuGH war der Charakter der Beschwerde und des Beschwerdeverfahrens ebenso umstritten wie der Prüfungsumfang der Gerichte. Nach der Entscheidung des EuGH ist die Entscheidung der Datenschutzaufsichtsbehörde über eine Beschwerde eine Entscheidung mit Rechtswirkung und unterliegt daher einer vollständigen inhaltlichen Überprüfung durch das zuständige Gericht. Allerdings steht der Aufsichtsbehörde ein Ermessensspielraum zu, wie sie das Beschwerdeverfahren durchführt und welche Maßnahmen sie trifft. Diese Entscheidungen kann das Gericht nur auf Ermessensfehler überprüfen, nicht aber seine Entscheidung an die Stelle der Entscheidung der Aufsichtsbehörde setzen.
– Nach Art. 40 Abs. 1 DS-GVO müssen die Mitgliedstaaten, die Aufsichtsbehörden und die Kommission die Ausarbeitung von Verhaltensregeln fördern, mit denen Wirtschaftsverbände die abstrakten Vorgaben der Verordnung für ihre Mitglieder konkretisieren, um mehr Rechtssicherheit zu erreichen. Diese Verhaltensregeln sind nur wirksam, wenn sie von der zuständigen Datenschutzaufsichtsbehörde genehmigt worden sind. Die Verhaltensregeln des Verbands der Wirtschaftsauskunfteien legten die zulässige Speicherdauer für bestimmte Daten fest. Umstritten war bisher, welche Bedeutung solche Verhaltensregeln haben. Hierzu entschied der EuGH nun, dass Verhaltensregeln nur die Vorgaben der DS-GVO auslegen können, sie jedoch nicht ausweiten oder verändern dürfen. Dies gilt insbesondere für die Zulässigkeit der Datenverarbeitung aufgrund überwiegender berechtigter Interessen auf Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO. Insofern ist eine Speicherdauer für die Erteilung einer Restschuldbefreiung, die über die in nationalen Rechtsvorschriften normierte Speicherdauer der Daten im öffentlichen Register hinausgeht, unzulässig und unwirksam.
– Die Erstellung und Verwendung eines Scores hat der EuGH als automatisierte Entscheidung über den Kredit angesehen, sofern ihm die Kreditgeber eine „maßgebliche Rolle“ im Rahmen der Kreditgewährung beimessen. Eine automatisierte Entscheidung ist nach Art. 22 Abs. 1 DS-GVO grundsätzlich unzulässig und darf nach Art. 22 Abs. 2 DS-GVO nur aufgrund einer Einwilligung oder einer gesetzlichen Erlaubnis getroffen werden. Relevant ist folglich, ob die von Kreditgebern getroffene Ablehnung eines Kredits „maßgeblich“ vom Score der Auskunftei abhängig ist. Eine Bank verfügt aufgrund ihrer Geschäftsbeziehungen zum jeweiligen Antragsteller und aufgrund ihres angemessenen und wirksamen Risikomanagements über mehr Informationen zum Kreditnehmer, als dem Score der Wirtschaftsauskunftei tatsächlich zugrunde liegen. Es ist daher zu erwarten, dass das Kreditinstitut seine Entscheidung in der Regel nicht

maßgeblich auf den Score einer Auskunftei stützt. Anders könnte dies jedoch im Fall von Online-Krediten zu bewerten sein.

Ausblick

Die Urteile des EuGH liegen im Interesse der betroffenen Personen. Sie schaffen Klarheit und Rechtssicherheit für Auskunfteien und Datenschutzaufsichtsbehörden und alle Beteiligten. Die Entscheidungen des EuGH sind für das vorlegende Gericht bindend. Das Verwaltungsgericht Wiesbaden muss nun in seinen Entscheidungen in den Ausgangsverfahren die Rechtsauffassung des EuGH zugrunde legen und darf von dieser nicht abweichen. Die Verhaltensregeln des Verbands der Wirtschaftsauskunfteien habe ich beanstandet. Der Verband muss sie daher unter Berücksichtigung der Ausführungen des EuGH überarbeiten. Spannend bleibt, welche Auswirkungen die Interpretation des Begriffs ‚automatisierte Entscheidung' durch den EuGH zukünftig auf viele Entscheidungsunterstützungssysteme – weit über den Bereich der Auskunfteien hinaus – haben wird, die – etwa mit Künstlicher Intelligenz – Entscheidungen vorbereiten.

3.2
Leitlinien des EDSA für die Berechnung von Geldbußen

Im Frühjahr 2023 wurden die langerwarteten Leitlinien für die Berechnung von Geldbußen vom EDSA angenommen. Damit wurde ein wichtiger Schritt in Richtung Harmonisierung der datenschutzrechtlichen Geldbußenpraxis der europäischen Mitgliedstaaten gegangen.

Am 12. Mai 2023 hat der EDSA die Leitlinien für die Berechnung von Geldbußen nach Art. 83 Abs. 4 bis 6 DS-GVO angenommen.[24] An der Erarbeitung dieser Leitlinien waren aus Deutschland neben der Berliner Datenschutzbeauftragten der Bundesbeauftragte und ich beteiligt. Mit der Verabschiedung der Leitlinien für die Berechnung von Geldbußen findet ein intensiver Austausch zwischen den Mitgliedstaaten zu einem wohl abgewogenen Kompromiss. Dieser trägt zum einen den unterschiedlichen Rechtstraditionen in den EU-Mitgliedstaaten Rechnung und leistet zum anderen einen grundlegenden und lang erwarteten Beitrag zur Harmonisierung der Zumessung von Geldbußen.

Die Leitlinien berücksichtigen drei Aspekte: die Art (Kategorie) des Verstoßes, die Schwere des Verstoßes und den Umsatz des betreffenden Unternehmens.

24 https://edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf.

Die Leitlinien dienen der Harmonisierung der Bebußung nach der DS-GVO durch die Mitgliedstaaten und gestalten das Vorgehen der Behörden bei der Verhängung von Geldbußen transparenter, damit der potenziell immensen Höhe der Geldbußen durch Transparenz Rechnung getragen wird. Dabei stellen die Leitlinien sicher, dass jede Geldbuße gemäß Art. 83 Abs. 1 DS-GVO wirksam, verhältnismäßig und abschreckend ist.

Die Berechnung nach den Leitlinien, erfolgt in **fünf Schritten**:

– **1. Schritt:** Die Datenschutzaufsichtsbehörden müssen feststellen, ob der betreffende Fall eine oder mehrere sanktionierbare Handlungen umfasst und ob diese zu einem oder mehreren Verstößen geführt hat oder haben. In diesem Schritt ist zu klären, ob sämtliche Verstöße mit einer Geldbuße geahndet werden können oder nur einige von ihnen.
– **2. Schritt:** Die Datenschutzaufsichtsbehörden ermitteln für die Berechnung der Geldbuße einen Ausgangspunkt.
– **3. Schritt:** Danach prüfen die Datenschutzaufsichtsbehörden erschwerende oder mildernde Faktoren, durch die sich die festzusetzende Geldbuße erhöhen oder verringern kann.
– **4. Schritt**: Im vorletzten Schritt bestimmen die Datenschutzaufsichtsbehörden die gesetzlichen Höchstbeträge von Geldbußen gemäß Art. 83 Abs. 4 bis 6 DSGVO und sichern, dass diese Beträge nicht überschritten werden.
– **5. Schritt:** Im letzten Schritt prüfen die Datenschutzbehörden, ob der berechnete Endbetrag den Anforderungen in Bezug auf die Wirksamkeit, die abschreckende Wirkung und die Verhältnismäßigkeit genügt oder weitere Anpassungen des Betrags erforderlich sind.

Mit den Leitlinien vom 12. Mai 2023 wurde das von der DSK Ende 2019 verabschiedete Bußgeldkonzept überholt. Mit ihm hat die DSK gezeigt, dass auch in einem föderalen Aufsichtssystem eine Vereinheitlichung der Bußgeldpraxis möglich ist.

Neben den Leitlinien findet das WP 253 vom 3. Oktober 2017 weiterhin Anwendung. Während sich dieses Working Paper mit dem „Ob“ einer Sanktionierung und den Kriterien des Art. 83 Abs. 2 DS-GVO befasst, behandeln die Leitlinien vom 12. Mai 2023 die Berechnung der Geldbuße, also das „Wie“ der Sanktion.

3.3
Verhängung von Geldbußen

Im Jahr 2023 waren erneut sehr unterschiedliche Verstöße Gegenstand von Verfahren zur Verhängung von Geldbußen. Schwerpunkte der Bearbeitung stellten insbesondere Verstöße im Gesundheitsbereich, im Zusammenhang mit unrechtmäßiger Werbung sowie Verletzungen der Pflicht zur Kooperation mit der Aufsichtsbehörde dar.

Geldbußen in Zahlen

Die Verhängung von Geldbußen unterliegt unionsrechtlichen Rechtsgrundlagen. Sie ist als aufsichtsrechtliche Maßnahme nach Art. 58 Abs. 2 Buchst. i DS-GVO vorgesehen. Ihre Ausgestaltung erfolgt durch Art. 83 DS-GVO hinsichtlich der Sanktionstatbestände in Abs. 4 bis 6, hinsichtlich ihrer Zielsetzung in Abs. 1, hinsichtlich der Ermessensausübung im Einzelfall in Abs. 2 und hinsichtlich des Verfahrens in Abs. 8.[25]

Im Berichtsjahr leitete ich insgesamt 52 neue Verfahren wegen Geldbußen ein. Damit blieb die Zahl der neuen Verfahren konstant auf dem Vorjahresniveau. Mit 124 einzelnen Geldbußen hat die Zahl der verhängten Sanktionen dagegen einen neuen Rekordwert erreicht. Mit einem Betrag von 56.810 Euro verhängte ich im Jahr 2023 auch das bisher höchste jährliche Gesamtvolumen an Geldbußen.

Verstöße im Gesundheitssektor

Im Gesundheitsbereich werden regelmäßig personenbezogene Daten verarbeitet, die sich auf die körperliche oder geistige Gesundheit von natürlichen Personen beziehen. Dabei handelt es sich um Gesundheitsdaten im Sinn des Art. 4 Nr. 15 DS-GVO, die gemäß Art. 9 Abs. 1 DS-GVO unter besondere Kategorien personenbezogener Daten fallen. Diese Daten sind in der Regel besonders sensibel und erfordern ein höheres Schutzniveau. Die Ahndung von Verstößen gegen die datenschutzrechtlichen Vorgaben der Verordnung im Gesundheitsbereich hat daher einen hohen Stellenwert.

Während ich im Jahr 2022 überwiegend Geldbußen gegen Corona-Testcenter festgesetzt hatte, richtete sich der Fokus im Berichtsjahr verstärkt auf die Arztpraxen. Hierbei wurden die festgestellten Verstöße konsequent geahndet.

In einem Verfahren wurde mir durch einen Hinweisgeber bekannt, dass eine ärztliche Praxisgemeinschaft den gesamten Abfall einschließlich Patientenunter-

25 S. hierzu näher Roßnagel/Rost, Eine Geldbuße kommt selten allein. Geldbußen im Kontext aufsichtsbehördlichen Handelns, ZD 2023, 502 ff.

lagen wiederholt über einen längeren Zeitraum in einem öffentlich zugänglichen Papiermüllcontainer entsorgte. Die weggeworfenen Dokumente waren zum größten Teil geschreddert, allerdings nur so, dass sie leicht rekonstruierbar waren. Manche Patientenakten wurden durch die Praxis im Ganzen entsorgt.

Gegen die beiden Praxisinhaber habe ich wegen der festgestellten Verstöße gegen Art. 83 Abs. 5 Buchst. a DS-GVO in Verbindung mit Abs. 5 Abs. 1 Buchst. f in Verbindung mit Art. 32 Abs. 1 Buchst. b DS-GVO insgesamt Geldbußen in Höhe von 3.600 Euro verhängt.

Bußgeldmildernd wurde insbesondere berücksichtigt, dass die Ärzte den Vorfall vollständig eingeräumt, nach Einschaltung der Aufsichtsbehörde umgehend die notwendigen Maßnahmen zwecks Umsetzung einer datenschutzkonformen Datenentsorgung implementiert und mit der Behörde kooperativ zusammengearbeitet haben.

Zu Lasten der Verantwortlichen wurde dagegen gewertet, dass sie den Verstoß vorsätzlich begangen und dabei unter anderem besonders schützenswerte Gesundheitsdaten und sehr persönliche Details über ihre Patienten einem unbegrenzten Adressatenkreis offenbart haben. Darüber hinaus wurde auch schärfend berücksichtigt, dass die Verarbeitung von Gesundheitsdaten einschließlich Entsorgung von Patientendaten zur Kerntätigkeit einer Arztpraxis gehört und ein datenschutzkonformer Umfang damit unerlässlich ist. Bußgelderhöhend habe ich ferner gewertet, dass es sich um einen systematischen Verstoß handelte, der über mehrere Monate andauerte. Dies deutet auf ein fehlendes datenschutzrechtliches Bewusstsein und ein organisatorisches Problem in der Arztpraxis und ein erhöhtes Maß an Pflichtwidrigkeit der Verantwortlichen hin. Hierfür spricht, dass weder über einen längeren Zeitraum das rechtmäßige Vorgehen zur Umsetzung der mit der DS-GVO einhergehenden Pflichten sichergestellt, noch die notwendigen technischen und organisatorischen Maßnahmen umgesetzt waren.

Die Praxisinhaber haben die Bußgeldbescheide akzeptiert und unverzüglich Zahlungen geleistet.

Verstöße im Zusammenhang mit Werbung

Im Berichtsjahr habe ich mehrere Verstöße im Kontext werblicher Maßnahmen mit Sanktionen belegt. Insbesondere handelte es sich hierbei um unrechtmäßige Werbung, ohne Einwilligung der betroffenen Personen, Nichtbeachtung von Werbewidersprüchen sowie fehlende Hinweise auf das Widerspruchsrecht.

In einem Verfahren gegen ein Unternehmen, das die Merkmale einer großen Personengesellschaft gemäß §§ 267 Abs. 3 HGB in Verbindung mit § 264a

HGB erfüllt, erhielt ich eine Beschwerde eines ehemaligen Kunden des Unternehmens wegen mehrfach wiederholter unrechtmäßiger Werbemaßnahmen. Nach abschließender Bearbeitung des Beschwerdeverfahrens und der Feststellung wiederholter Missachtung von Werbewidersprüchen habe ich die verantwortliche Stelle wegen der Verstöße gegen Art. 21 Abs. 3 DS-GVO förmlich gemäß Art. 58 Abs. 2 Buchst. b DS-GVO verwarnt. Die Verwarnung wurde nicht angegriffen und ist bestandskräftig.

Mehrere Monate später teilte der Beschwerdeführer der Aufsichtsbehörde jedoch mit, dass er entgegen der Zusagen des Verantwortlichen wiederum Werbung vom Unternehmen erhalten hatte. Nach Stellungnahme des Datenschutzbeauftragten der verantwortlichen Stelle war es dem Unternehmen entgegen früherer Angaben nicht gelungen, alle dort gespeicherten Daten zur Person des Beschwerdeführers für die Verarbeitung zu Werbezwecken gemäß Art. 21 Abs. 3 DS-GVO zu sperren. Der Grund hierfür lag darin, dass dem Unternehmen drei verschiedene Datensätze zur Person des Beschwerdeführers vorlagen und nach den früheren Einwänden, aufgrund der jeweils unterschiedlichen Schreibweise der Postanschrift, lediglich zwei dieser Datensätze entdeckt und für die Werbung gesperrt wurden. Der dritte Datensatz blieb damals unentdeckt und wurde daher nicht für Zwecke der Werbung ausgenommen, was zur erneuten Verwendung der Daten des Beschwerdeführers zur werblichen Ansprache führte.

Darüber hinaus teilte das Unternehmen mit, dass es zwischenzeitlich sämtliche Datensätze zum betroffenen Kunden in den internen Systemen gelöscht hatte. Eine weitere Zusendung von Werbung sei damit nicht mehr möglich. Im Übrigen wurden die zuständigen Mitarbeitenden neben der regelmäßigen Datenschutz- und Informationssicherheitsschulung in einer umfassenden Schulung „Datenschutz im Vertrieb“ unterwiesen, damit es nicht erneut zu beschriebenen Fehlern kommt.

Durch das erneute Missachten von Werbewidersprüchen des Beschwerdeführers und den fortgesetzten Versand von Werbung hat das Unternehmen fahrlässig gegen die Rechte der betroffenen Person gemäß Art. 83 Abs. 5 Buchst. b in Verbindung mit Art. 21 Abs. 3 DS-GVO verstoßen. Diesen Verstoß habe ich mit einer Geldbuße in Höhe von 25.000 Euro sanktioniert.

Das Unternehmen als Verantwortlicher im Sinn des Art. 4 Abs. 7 DS-GVO hat die Erfüllung der gesetzlichen Pflichten im Zusammenhang mit den Rechten der betroffenen Personen sicherzustellen. Der Verantwortliche hat für die konkrete Umsetzung und Überwachung von geeigneten technischen und organisatorischen Maßnahmen zu sorgen. Bis zu meiner Einschaltung hatte das Unternehmen dagegen aus mangelnder Sorgfalt keine hinreichenden innerbetrieblichen Maßnahmen bezüglich des Umgangs mit Werbewider-

sprüchen umgesetzt, um diesen Pflichten nachzukommen. Insbesondere war nicht sichergestellt, dass bei der Sperrung von Datensätzen der betroffenen Personen auch solche mit unterschiedlichen Schreibweisen von Namen, Straßen und anderen Angaben entsprechend identifiziert und für die Werbung gesperrt werden. Hätten das vertretungsberechtigte Leitungspersonal und die ausführenden Beschäftigten pflichtbewusst gehandelt und frühzeitig entsprechende Maßnahmen ergriffen, wäre der Verstoß vermeidbar gewesen.

Bei der Bemessung der Geldbuße wog insbesondere zu Lasten des Unternehmens, dass es sich nicht um einen Erstverstoß, sondern um einen weiteren gleichgelagerten Verstoß im Zusammenhang mit Werbewidersprüchen handelte. Die im Jahr 2022 wegen der Missachtung der Werbewidersprüche des Beschwerdeführers durch mich gemäß Art. 58 Abs. 2 Buchst. b DS-GVO ausgesprochene Verwarnung, die keine nachhaltige Wirkung entfaltete, habe ich schärfend berücksichtigt. Darüber hinaus habe ich die kommerziellen Interessen des Unternehmens als Zwecke der Datenverarbeitung mittels werblicher Ansprache gesehen und bußgelderhöhend gewertet.

Zu Gunsten des Unternehmens wurde dagegen die fahrlässige Begehungsweise der Zuwiderhandlung sowie die Tatsache berücksichtigt, dass nur wenige Daten einer Person vom Vorfall betroffen waren und keine Anhaltspunkte dafür vorlagen, dass – bis auf die Unannehmlichkeiten und den Zeitaufwand – kein Schaden entstanden ist. In erheblichem Maße wirkte sich zu Gunsten des Verantwortlichen ferner aus*, dass* das Unternehmen mit der Aufsichtsbehörde konstruktiv zusammengearbeitet hat. Deutlich bußgeldsenkend habe ich darüber hinaus berücksichtigt, dass *der* Sachverhalt vollumfänglich eingeräumt und der Vorfall bedauert wurde. Darüber hinaus habe ich die im Nachgang des Vorfalls eingeleiteten Maßnahmen, wie die entsprechenden Schulungen von Mitarbeitenden, mildernd berücksichtigt.

Unter umfassender Abwägung der zumessungserheblichen Umstände und unter Berücksichtigung der wirtschaftlichen Stärke des Unternehmens ist die Geldbuße in Höhe des angesetzten Betrages wirksam, verhältnismäßig und abschreckend, um eine ernsthafte Pflichtmahnung zu erzielen.

Gegen die Entscheidung über die Geldbuße legte das Unternehmen Einspruch ein. Das Verfahren ist noch nicht rechtskräftig abgeschlossen.

Verstöße gegen die Mitwirkungspflicht

Neu hinzugekommen sind im Berichtsjahr zunehmend Verstöße der verantwortlichen Stellen gegen die Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde. So haben sich in mehreren Fällen Unternehmen und natürliche

Personen im Rahmen der gegen sie geführten Beschwerdeverfahren geweigert, mit meiner Behörde zu kooperieren.

Im Aufsichtsverfahren gegen ein Unternehmen standen Verstöße gegen die Auskunftspflicht nach Art. 15 DS-GVO sowie Art. 5 Abs. 1 Buchst. a in Verbindung mit Art. 6 DS-GVO im Raum. Um den Vorfall aufzuklären und datenschutzrechtlich zu bewerten, forderte ich die verantwortliche Stelle zur Stellungnahme auf. Darüber hinaus habe ich das Unternehmen darauf hingewiesen, dass es nach Art. 31 DS-GVO verpflichtet ist, mit mir als Aufsichtsbehörde zusammenzuarbeiten sowie nach Art. 58 Abs. 1 Buchst. a DS-GVO in Verbindung mit § 40 Abs. 4 Satz 1 BDSG mir Auskünfte zu erteilen.

Nachdem das Unternehmen nicht reagierte, habe ich es per Bescheid förmlich gemäß Art. 58 Abs. 1 Buchst. a DS-GVO zur Bereitstellung von Informationen sowie gemäß Art. 58 Abs. 2 Buchst. c DS-GVO zur Erteilung der Auskunft nach Art. 15 DS-GVO an die Beschwerdeführerin angewiesen. Für den Fall, dass das Unternehmen den erteilten Anordnungen nicht innerhalb der gesetzten Frist nachkommen sollte, habe ich gemäß § 76 Abs. 2 des Hessischen Verwaltungsvollstreckungsgesetzes (HessVwVG) jeweils ein Zwangsgeld in Höhe von 2.000 Euro angedroht. Im Laufe der weiteren Bearbeitung habe ich aufgrund der pflichtwidrigen Nichterteilung von Auskünften insgesamt sechs Zwangsgelder in Höhe eines Gesamtbetrages von 28.000 Euro festsetzen müssen.

Während der gesamten Bearbeitung des Beschwerdeverfahrens erfolgte durch das Unternehmen über einen Zeitraum von mehreren Monaten keine schriftliche oder mündliche Äußerung oder sonstige Kontaktaufnahme zur Aufsichtsbehörde, obwohl ich es mehrfach auf seine Auskunfts- und Mitwirkungspflicht hingewiesen hatte. Dadurch war mir die Sachverhaltsaufklärung deutlich erschwert.

Nach Art. 31 DS-GVO ist der Verantwortliche verpflichtet, auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten. Darüber hinaus sind nach § 40 Abs. 4 Satz 1 BDSG die der Aufsicht unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen verpflichtet, der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte zu erteilen.

Ich stellte im Rahmen meiner Befugnisse bei der Bearbeitung einer Beschwerde einer betroffenen Person dem Unternehmen konkrete Fragen. Es hat jedoch nicht mit mir zusammengearbeitet und mir keinerlei Auskünfte erteilt sowie die von mir erteilten Anweisungen nicht befolgt. Es ließ sowohl alle Schreiben als auch förmliche Bescheide unbeantwortet. Das Unternehmen nahm keinerlei Kontakt auf, sondern ignorierte gänzlich sämtliche Auskunftsanfragen und Anweisungen.

Die Weigerung, mit mir zu kooperieren, stellt einen Verstoß gegen die Mitwirkungspflicht gemäß Art. 31 DS-GVO dar. Das eingeleitete Verfahren gegen das Unternehmen wegen der Ordnungswidrigkeit nach Art. 83 Abs. 4 Buchst. a DS-GVO in Verbindung mit Art. 31 DS-GVO endete letztlich mit einer Geldbuße in Höhe von 5.000 Euro.

Eine Zahlung der festgesetzten Zwangsgelder und der Geldbuße erfolgte bislang nicht, so dass diese inzwischen im Rahmen der Zwangsvollstreckung beigetrieben werden.

Einstellungen

Neben den verhängten Geldbußen musste ich einige Verfahren im Berichtsjahr auch einstellen. Dabei handelt es sich zum Teil um Vorgänge, die durch Staatsanwaltschaften nach Einstellung des Strafverfahrens gemäß § 43 OWiG an meine Behörde zur Verfolgung etwaiger Ordnungswidrigkeiten abgegeben wurden. Darunter befanden sich unter anderem Fälle, die nicht mit einer Geldbuße bewehrt waren, für die der Tatverdacht ausgeräumt oder aber die Tat nicht nachgewiesen werden konnte und weitere Ermittlungen nicht erfolgversprechend waren. Diese Fälle wurden sodann gemäß § 170 Abs. 2 StPO in Verbindung mit § 46 Abs. 1 OWiG aus tatsächlichen Gründen eingestellt.

Die zweite Fallgruppe von Einstellungen betrifft Verfahren, die gemäß § 170 Abs. 2 StPO in Verbindung mit § 46 Abs. 1 OWiG aus rechtlichen Gründen einzustellen waren. Zum einen waren die möglichen Verstöße verjährt. Zum anderen konnten sie aufgrund eines über das Vermögen der Verantwortlichen anhängigen Insolvenzverfahrens nicht weiterverfolgt werden.

Darüber hinaus habe ich im Rahmen der Bearbeitung mehrere Bußgeldverfahren gemäß § 47 Abs. 1 OWiG aus Opportunitätsgründen eingestellt. Gemäß § 47 Abs. 1 OWiG liegt die Verfolgung und Ahndung von Ordnungswidrigkeiten im pflichtgemäßen Ermessen der Verfolgungsbehörde, solange das Verfahren bei ihr anhängig ist. Die Verwaltungsbehörde kann das Verfahren einstellen, sofern die Verhängung einer Geldbuße unter Berücksichtigung aller Umstände nicht (mehr) geboten scheint. Von der Möglichkeit der Einstellung aus Opportunitätsgründen machte ich, nach umfassender Prüfung und Abwägung aller belastenden und mildernden Umstände, bei einmaligen leichten Verstößen in Einzelfällen Gebrauch.

3.4
Geldbußen gegen Unternehmen

Die DS-GVO sieht in der Verhängung von Geldbußen gegen Verantwortliche nach Art. 58 Abs. 2 lit. i und Art. 83 ein wesentliches Instrument, um ihre Anforderungen in der Praxis umsetzen zu können. Seit dem Inkrafttreten der DS-GVO waren wichtige Fragen der Verhängung von Geldbußen gegenüber Unternehmen heftig umstritten. In zwei Vorlageentscheidungen hat der EuGH die zwei wichtigsten Fragen entschieden.

In dem Urteil vom 5. Dezember 2023[26] ging es um eine Geldbuße in Höhe von über 14 Mio. Euro, welche die Aufsichtsbehörde in Berlin gegen die Deutsche Wohnen SE verhängt hatte, weil diese es vorsätzlich unterlassen habe, die notwendigen Maßnahmen zu treffen, um die regelmäßige Löschung nicht mehr benötigter personenbezogener Daten von Mietern zu ermöglichen und durchzuführen.

In dem Vorlageverfahren ging es um die Fragen, ob die Aufsichtsbehörde eine Geldbuße unmittelbar gegen ein Unternehmen verhängen kann und ob dem Unternehmen hierfür ein Verschulden nachgewiesen werden muss.

Geldbußen gegen Unternehmen

Nach deutschem Recht kann eine Ordnungswidrigkeit grundsätzlich nur von einer natürlichen Person begangen werden. Ausnahmsweise kann ein Bußgeld nach § 30 OWiG auch gegen eine juristische Person verhängt werden, wenn eine Leitungsperson iSd § 30 Abs. 1 OWiG eine Ordnungswidrigkeit begangen hat, durch die Pflichten, welche die juristische Person treffen, verletzt worden sind oder die juristische Person bereichert worden ist oder werden sollte.

Diese Vorschrift ist jedoch bei Verstößen gegen die DS-GVO nicht anwendbar. Vielmehr sind wegen des Anwendungsvorrangs des Unionsrechts die inhaltlichen Voraussetzungen einer Geldbuße allein nach Art. 83 DS-GVO zu bestimmen. Daher kann nach dem Urteil des EuGH ein Unternehmen als Verantwortlicher selbst gegen datenschutzrechtliche Vorgaben verstoßen und unmittelbar zum Adressaten einer Geldbuße nach Art. 83 DS-GVO werden.

Außerdem hat der EuGH in Orientierung am Wettbewerbsrecht der Union klargestellt, dass es nicht erforderlich ist, den Verstoß gegen Datenschutzrecht bestimmten, zu identifizierenden natürlichen Personen zuzuordnen.

26 EuGH vom 5.12.2023, C-807/21 – ECLI:EU:C:2023:950, NJW 2024, 343.

Vielmehr genügt es festzustellen, dass der Verstoß von Personen begangen wurde, die dem Unternehmen zuzuordnen sind.[27]

Verschulden des Unternehmens

Bezogen auf die zweite umstrittene Frage hält der EuGH fest, dass die Aufsichtsbehörde Geldbußen nur wegen Verstößen gegen die Bestimmungen der DS-GVO verhängen kann, die der Verantwortliche schuldhaft, also vorsätzlich oder fahrlässig, begangen hat.

Hinsichtlich des Verschuldensmaßstabs orientiert sich der EuGH wiederum am Wettbewerbsrecht der Union.[28] Danach können Unternehmen Verstöße gegen Datenschutzrecht verschulden, ohne dass das Verschulden einer natürlichen Person nachgewiesen werden muss. Hierzu stellt der EuGH fest, „dass ein Verantwortlicher für ein Verhalten, das in den Anwendungsbereich der DS-GVO fällt, sanktioniert werden kann, wenn er sich über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte, gleichviel, ob ihm dabei bewusst war, dass es gegen die Vorschriften der DS-GVO verstößt".[29] Diese Kenntnis ist für die juristische Person festzustellen, nicht für die handelnde natürliche Person. Und bezogen auf die Leitungsorgane ist festzuhalten: Bei einer juristischen Person setzt die „Anwendung von Art. 83 DSGVO keine Handlung und nicht einmal eine Kenntnis seitens des Leitungsorgans dieser juristischen Person voraus".[30]

Das Urteil des EuGH hat umstrittene Rechtsfragen geklärt und eine tragfähige Grundlage für die Aufsichtspraxis und die Festsetzung von Geldbußen gegen Unternehmen geschaffen. Die dadurch erzeugte Rechtsklarheit wird die Einhaltung von datenschutzrechtlichen Vorgaben bei den Verantwortlichen befördern und die Aufsichtstätigkeit der Aufsichtsbehörden erleichtern (s. Kap. 1.1).

27 S. hierzu auch Roßnagel/Rost, Geldbußen gegen juristische Personen, ZD 2024, 183–188.

28 S. näher Roßnagel/Rost, Geldbußen gegen juristische Personen, ZD 2024, 183–188.

29 EuGH vom 5.12.2023, C-807/21 – ECLI:EU:C:2023:950, NJW 2024, 343, Rn. 76.

30 EuGH vom 5.12.2023, C-807/21 – ECLI:EU:C:2023:950, NJW 2024, 343, Rn. 77.

4. 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 Gegenstand eines Urteils des Bundesverfassungsgerichts zu den Rechtsgrundlagen von hessenDATA (Kap. 4.1) und der Gesetzgebungsverfahren zur Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung und des Hessischen Verfassungsschutzgesetzes (Kap. 4.2). Die Einhaltung der Voraussetzungen und Grenzen dieser Befugnisse war Gegenstand von Prüfungen bei Polizeibehörden und dem Landesamt für Verfassungsschutz (Kap. 4.3) sowie bei Staatsanwaltschaften (Kap. 4.4). Gegenüber Gerichten war die Veröffentlichung unzureichend anonymisierter Gerichtsentscheidungen zu korrigieren (Kap. 4.5).

4.1 Urteil des Bundesverfassungsgerichts zu hessenDATA und die Folgen für Hessen

Im Folgenden führe ich meinen Bericht aus dem letzten Tätigkeitsbericht (Kap. 6.1) zu hessenDATA vor dem Bundesverfassungsgericht fort und stelle das mittlerweile ergangene Urteil vom 16. Februar 2023 zur Verfassungsmäßigkeit des § 25a des Hessischen Sicherheits- und Ordnungsgesetzes (HSOG) sowie dessen Folgen für den hessischen Gesetzgeber und die Exekutive kurz dar.

Im Verfahren vor dem Bundesverfassungsgericht aufgrund mehrerer Verfassungsbeschwerden zur „Automatisierten Datenauswertung durch die Polizei in Hessen und Hamburg“ habe ich im Jahr 2022 zur damaligen Fassung des § 25a HSOG Stellung genommen. Dabei konnte ich meine datenschutzrechtliche Expertise als Sachverständiger auch in der mündlichen Verhandlung am 20. Dezember 2022 einbringen.

§ 25a HSOG (alt) ermöglichte der Hessischen Polizei, die bei ihr gespeicherten personenbezogenen Daten auch zur vorbeugenden Bekämpfung von schweren Straftaten zu analysieren. Hierfür kommt seit 2017 die an die hiesigen polizeilichen und rechtlichen Anforderungen angepasste Analyse-Software Gotham der US-Firma Palantir zum Einsatz, die in Hessen die Bezeichnung hessenDATA trägt.

§ 25a HSOG a. F.

(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 Ergebnis hatte ich in meiner Stellungnahme konstatiert, dass § 25a HSOG in dieser Fassung in mehrfacher Hinsicht erheblichen verfassungsrechtlichen Zweifeln ausgesetzt war.

Der Erste Senat des Bundesverfassungsgerichts entschied mit Urteil vom 16. Februar 2023,[31] dass § 25a Abs. 1 Alt. 1 HSOG verfassungswidrig ist und gegen die informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) verstößt, soweit sich die Regelung auf die vorbeugende Bekämpfung von Straftaten bezieht. Meine im verfassungsgerichtlichen Verfahren vorgetragenen Bedenken wurden damit auch höchstrichterlich bestätigt.

Das Bundesverfassungsgericht bemängelt im Ergebnis, dass die Rechtsgrundlage keine dem mit dieser Maßnahme der Datenanalyse verbundenen Eingriffsgewicht angemessene Eingriffsschwelle vorsieht (Urteil, Rn. 173). Die Kernaussagen der Entscheidung finden sich in den fünf vorangestellten Leitsätzen zum Urteil.

Das Bundesverfassungsgericht hat zunächst festgestellt, dass die automatisierte Datenanalyse und -auswertung einen neuen und eigenen gewichtigen Grundrechtseingriff für all diejenigen bedeutet, deren personenbezogene Daten davon betroffen sind (erster und zweiter Leitsatz). Die Anforderungen

31 BVerfG, 1 BvR 1547/19 und 1 BvR 2634/20, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html.

an eine automatisierte Datenanalyse und gesetzliche Regelung bestimmen sich nach Art und Umfang der Daten, die verarbeitet werden, sowie den zugelassenen Methoden der Datenanalyse und -auswertung; mithin kann der Gesetzgeber die Eingriffsintensität mit entsprechenden Regelungen selbst steuern (dritter Leitsatz). Sofern die Datenanalyse und -auswertung einen schwerwiegenden Grundrechtseingriff ermöglichen soll, ist dies nach Auffassung des Bundesverfassungsgerichts nur unter engen Voraussetzungen, wie bei eingriffsintensiven heimlichen Überwachungsmaßnahmen zum Schutz besonders gewichtiger Rechtsgüter, möglich, sofern für diese Rechtsgüter eine zumindest hinreichend konkretisierte Gefahr besteht (vierter Leitsatz).

Das Bundesverfassungsgericht formulierte die Anforderungen an eine verfassungskonforme gesetzliche Grundlage und Anwendung einer Analyse-Software durch staatliche Behörden im fünften Leitsatz des Urteils wie folgt:

1BvR 1547/19 und 1 BvR 2634/20

(5) Grundsätzlich kann der Gesetzgeber den Erlass der erforderlichen Regelungen zu Art und Umfang verarbeitbarer Daten und zu den zulässigen Datenverarbeitungsmethoden zwischen sich und der Verwaltung aufteilen. Er muss aber sicherstellen, dass unter Wahrung des Gesetzesvorbehalts insgesamt ausreichende Regelungen getroffen werden.

a) Der Gesetzgeber muss die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben.

b) Soweit er die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigt, hat der Gesetzgeber zu gewährleisten, dass die Verwaltung die für die Durchführung einer automatisierten Datenanalyse oder -auswertung im Einzelfall maßgeblichen Vorgaben und Kriterien in abstrakt-genereller Form festlegt, verlässlich dokumentiert und in einer vom Gesetzgeber näher zu bestimmenden Weise veröffentlicht. Das sichert auch die verfassungsrechtlich gebotene Kontrolle, die insbesondere durch Datenschutzbeauftragte erfolgen kann.

Die Entscheidung des Bundesverfassungsgerichts entfaltet nicht nur für die beiden Bundesländer Hessen und Hamburg Relevanz, deren Regelungen Gegenstand des Verfahrens waren. Die Vorgaben sind künftig von allen Bundesländern und dem Bund einzuhalten, sofern deren Behörden eine entsprechende automatisierte Datenanalyse und -auswertung personenbezogener Daten durchführen und dabei Daten aus unterschiedlichen Quellen zusammenführen wollen.

Hessen war nun aufgerufen, die bis dato geltende Regelung des § 25a HSOG bis zum 30. September 2023 zu überarbeiten und den Vorgaben des Bundesverfassungsgerichts anzupassen. Mit einem Änderungsantrag[32] zum

32 LT-Drs. 20/11235 vom 20. Juni 2023.

Gesetzentwurf zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei,[33] der auch eine Änderung des § 25a HSOG enthielt, ist der hessische Gesetzgeber diesem Auftrag nachgekommen. Die Neuregelung ist am 12. Juli 2023 in Kraft getreten.

§ 25a HSOG (neu)

(1) Die Polizeibehörden dürfen rechtmäßig gespeicherte personenbezogene Daten auf einer Analyseplattform automatisiert zusammenführen. Sie dürfen nach Maßgabe der Sätze 3 bis 6 und der Abs. 2 bis 5 diese zusammengeführten Daten, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, verknüpfen, aufbereiten und auswerten sowie für statistische Zwecke anwenden (automatisierte Anwendung zur Datenanalyse). Die automatisierte Anwendung zur Datenanalyse ist ein technisches Hilfsmittel, das es den Polizeibehörden bei der Erfüllung ihrer Aufgaben nach Maßgabe der folgenden Absätze ermöglichen soll, ihre Bewertungen, Prognosen und Entscheidungen auf der Grundlage möglichst verlässlicher Tatsachenfeststellungen zu treffen. Sie erfolgt immer anhand anlassbezogener und zielgerichteter Suchkriterien. Sie wird manuell ausgelöst und läuft regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten ab. Eine direkte Anbindung an Internetdienste ist ausgeschlossen.

(2) Die Polizeibehörden können gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenanalyse weiterverarbeiten,

1. *wenn dies 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, erforderlich ist (Abwehr konkreter Gefahren),*
2. *wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise Straftaten mit erheblicher Bedeutung begangen werden und dies zur Verhinderung dieser Straftaten erforderlich ist (Abwehr konkretisierter Gefahren),*
3. *wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass schwere oder besonders schwere Straftaten begangen werden sollen, und die Weiterverarbeitung erforderlich ist, um diese Straftaten zu verhüten (Vorbeugende Bekämpfung von Straftaten).*

Zum Zweck der automatisierten Anwendung zur Datenanalyse können Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Verkehrsdaten, Telekommunikationsdaten, Daten aus Asservaten und Daten aus dem polizeilichen Informationsaustausch zusammengeführt werden. Datensätze aus gezielten Abfragen in gesondert geführten staatlichen Registern sowie einzelne gesondert gespeicherte Datensätze aus Internetquellen können ergänzend einbezogen werden. Bei einer Maßnahme nach Satz 1 Nr. 3 dürfen Verkehrsdaten nicht in die Analyse einbezogen werden.

Bei der Anwendung zur automatisierten Datenanalyse gilt § 20 Abs. 1 und 2. Dies wird durch eine Verwaltungsvorschrift sichergestellt, die zu veröffentlichen ist. Sie beinhaltet ein Rollen- und Rechtekonzept und ein Konzept der Kategorisierung und Kennzeichnung

33 LT-Drs. 20/8129 vom 22. Juni 2022.

personenbezogener Daten. Unter Berücksichtigung der in Abs. 2 Satz 1 nach Schutzgütern und Eingriffsschwellen unterschiedenen Lagebilder orientieren sich diese Konzepte an dem übergeordneten Ziel der Reduzierung des jeweils zu analysierenden Datenvolumens, der Angemessenheit der jeweils angewandten Analysemethode und des größtmöglichen Schutzes Unbeteiligter (funktionale Reduzierung der Eingriffsintensität).

1. *Das Rollen- und Rechtekonzept regelt die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen. Maßstab für dieses Konzept sind das Gewicht der zu schützenden Rechtsgüter und der Grad der Dringlichkeit des polizeilichen Einschreitens. Es ist nach dem Prinzip auszugestalten, wonach mehr Berechtigte Zugriff auf weniger und wenige Berechtigte Zugriff auf mehr der in der Analyseplattform zusammengeführten Daten haben dürfen. Es müssen darin mindestens die einzelnen Phänomenbereiche, ihre Gewichtung und ihr Verhältnis zueinander umschrieben und die dienstrechtliche Stellung der Berechtigten, ihre Funktion und ihre spezifische Qualifizierung bezogen auf den Umfang der jeweiligen Berechtigung festgelegt werden.*
2. *Das Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten regelt anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen.*

a) *Maßstab für dieses Konzept ist zum einen der sachliche Bezug der von der Analyse betroffenen Personen zum jeweiligen Phänomenbereich (Veranlassungszusammenhang). Es folgt dem Prinzip, wonach eine automatisierte Datenanalyse umso komplexer sein darf, je gewichtiger der Veranlassungszusammenhang ist, und dass sie umso einfacher sein muss, je weniger gewichtig der Veranlassungszusammenhang ist. Ausgangspunkt ist die Differenzierung nach einerseits verurteilten, beschuldigten, verdächtigen Personen und sonstigen Anlasspersonen sowie deren Kontaktpersonen und andererseits unbeteiligten Personen. Zum Schutz Unbeteiligter werden deren personenbezogene Vorgangsdaten in eine automatisierte Datenanalyse nicht einbezogen. Das Nähere regelt eine Verwaltungsvorschrift, die insbesondere für Verkehrsdaten eine Speicherfrist von regelmäßig zwei Jahren in der Analyseplattform vorsieht.*

b) *Maßstab für dieses Konzept ist zum anderen die Kategorisierung personenbezogener Daten nach der Schwere des Eingriffs in das Recht auf informationelle Selbstbestimmung bei ihrer Erhebung (Grundrechtsrelevanz). Es müssen abstrakte Regelungen getroffen werden, die der eingeschränkten Verwendbarkeit von Daten aus schwerwiegenden Grundrechtseingriffen Rechnung tragen, und es muss durch technisch-organisatorische Vorkehrungen sichergestellt werden, dass diese Regelungen praktisch wirksam werden. In die automatisierte Anwendung zur Datenanalyse werden keine personenbezogenen Daten einbezogen, die aus Wohnraumüberwachung und Online-Durchsuchung gewonnen wurden.*

(4) Der Zugang zur automatisierten Anwendung zur Datenanalyse ist reglementiert (Zugriffskontrolle). Die Zugriffe unterliegen hierbei der ständigen Protokollierung. Jeder Fall der automatisierten Anwendung zur Datenanalyse ist von der Anwenderin oder dem Anwender zu begründen. Die Begründung dient der Selbstvergewisserung und der nachträglichen Kontrolle. Die Einzelheiten der Zugriffskontrolle und des notwendigen Inhalts der Begründung werden in einer Verwaltungsvorschrift geregelt. Die oder der behördliche Datenschutzbeauftragte ist zur Durchführung stichprobenartiger Kontrollen berechtigt.

(5) 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 Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder einer wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen. Im Übrigen bleiben die Aufgaben und Befugnisse der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit unberührt.

Aufgrund der Kurzfristigkeit des eingebrachten Änderungsantrags und des Verzichts auf die Durchführung einer öffentlichen Anhörung zu diesem konnte ich zur vorgeschlagenen und nun geltenden Regelung § 25a HSOG im Rahmen des Gesetzgebungsverfahrens im Hessischen Landtag nicht Stellung nehmen.

Ich werde die Umsetzung der neuen Regelung und den Einsatz von hessenDATA auf Grundlage des neu gefassten § 25a HSOG durch die hessischen Polizeibehörden jedoch aufmerksam und kritisch begleiten.

4.2
Novellierung des HSOG und des HVSG

Im Berichtsjahr wurde die Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) und des Hessischen Verfassungsschutzgesetzes (HVSG) abgeschlossen; die Änderungen in beiden Gesetzen sind mittlerweile in Kraft getreten. Bereits im letzten Tätigkeitsbericht habe ich das Verfahren zum Gesetzentwurf zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei beschrieben und möchte im Folgenden über den weiteren Ablauf des Gesetzgebungsverfahrens, einschließlich meiner erneuten schriftlichen und mündlichen Stellungnahme, berichten.

Im Rahmen der öffentlichen Anhörungen im Innenausschuss des Hessischen Landtags hatte ich Gelegenheit, zum Gesetzentwurf zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei vom 22. März 2022[34] und zum Änderungsantrag vom 21. März 2023[35] schriftlich und mündlich Stellung zu nehmen.[36] Die von mir in meinen Stellungnahmen gemachten kritischen Anmerkungen wurden nur

34 LT-Drs. 20/8129.

35 LT-Drs. 20/10821.

36 Ausschussvorlagen INA 20/53 vom 1. Juli 2022, Teil 1, S. 79 ff., und INA 20/73 vom 28. April 2023, Teil 1, S. 8 ff.

teilweise vom Gesetzgeber aufgegriffen. Zudem hatte ich keine Möglichkeit, meine datenschutzrechtlichen Bedenken bereits frühzeitig im Rahmen der Erstellung des Gesetzentwurfs und Änderungsantrags einzubringen.

Ein weiterer Änderungsantrag,[37] der insbesondere Änderungen im HSOG zum Gegenstand hatte, wurde am 20. Juni 2023 eingebracht. Aufgrund der Kurzfristigkeit und des Verzichts auf die Durchführung einer öffentlichen Anhörung zu diesem konnte ich mich hierzu im Rahmen des Gesetzgebungsverfahrens im Hessischen Landtag nicht äußern. Zentraler Gegenstand dieses Antrags war die Neuregelung von § 25a HSOG infolge des Urteils des Bundesverfassungsgerichts vom 16. Februar 2023 (s. hierzu Kap. 4.1).

Die gesetzlichen Änderungen zum HVSG und HSOG sind am 12. Juli 2023 in Kraft getreten.

Änderungen im HVSG

Die Neuregelungen betreffen zum einen das HVSG. Ziel des Gesetzgebers war es dabei auch, die Vorgaben der jüngeren Rechtsprechung des Bundesverfassungsgerichts[38] umzusetzen. Gegen verschiedene Normen des HVSG, auch gegen einige Neuregelungen, ist aktuell ein Verfassungsbeschwerdeverfahren vor dem Bundesverfassungsgericht anhängig,[39] in dem ich als Sachverständiger im Berichtszeitraum schriftlich Stellung genommen habe.

Im Rahmen der Novellierung wurde u. a. das Auskunftsrecht gegenüber dem Landesamt für Verfassungsschutz Hessen (LfV Hessen) in § 26 HVSG gestärkt, indem die Voraussetzung für betroffene Personen, zur Auskunftserteilung auf einen konkreten Sachverhalt hinzuweisen, gestrichen wurde. Weitere Änderungen betreffen die Möglichkeit zur Überwachung von Einzelpersonen und den Schutz unbeteiligter Dritter bei der Informationserhebung mit nachrichtendienstlichen Mitteln nach § 5 Abs. 1 und 3 HVSG sowie die Löschung der Dokumentation unzulässig erfasster Daten im Rahmen der akustischen und optische Wohnraumüberwachung nach § 7 Abs. 5 HVSG und die zulässige Verwendung mittels Wohnraumüberwachung erhobener Daten gemäß § 8 HVSG. Zudem wurden die Befugnisse des LfV Hessen in § 10 HVSG zum Abruf und zur Übermittlung von Bestandsdaten, die Eingriffsschwellen beim Einsatz verdeckter Mitarbeiter gemäß § 12 HVSG sowie der Kernbereichsschutz überarbeitet und in § 14 HVSG ergänzende

37 LT-Drs. 20/11235.

38 Urteil vom 26. April 2022, 1 BvR 1619/17, „Bayerisches Verfassungsschutzgesetz“ und Beschluss vom 9. Dezember 2022, 1 BvR 1345/21, „Polizeiliche Befugnisse nach SOG MV“.

39 BVerfG, 1 BvR 2133/22.

Regelungen zu den Schranken nachrichtendienstlicher Mittel aufgenommen. Darüber hinaus verlängerte die Novelle die Prüffrist in § 16 Abs. 7 HVSG, in Bezug auf die Erforderlichkeit der Speicherung von personenbezogenen Daten, bei schweren Straftaten mit Staatsschutzbezug von fünf Jahren auf zehn Jahre und führte in § 16 Abs. 10 HVSG eine Protokollierungspflicht bei Abfragen in Bezug auf elektronische Akten ein.

In besonderem Maße wurden auch die Rechtsgrundlagen für die Datenübermittlungen durch das LfV Hessen an andere inländische und ausländische Behörden überarbeitet und in den §§ 19a –21 HVSG neu geregelt. In § 19a Abs. 1 HVSG ist nunmehr vorgesehen, dass eine Datenübermittlung durch das LfV Hessen an andere Stellen nur zulässig ist, soweit sie zur Aufgabenerfüllung der Empfängerbehörde im Einzelfall geboten ist und kein Übermittlungsverbot nach § 23 HVSG entgegensteht. Darüber hinaus gelten gemäß § 19a Abs. 2 Satz 1 HVSG für die Übermittlung ausschließlich mit nachrichtendienstlichen Mitteln ersterhobener Daten an inländische öffentliche Stellen die zusätzlichen Anforderungen der §§ 20 – 20c HVSG sowie an ausländische öffentliche Stellen des § 21 HVSG. Je nachdem um welche Behörde es sich bei der Empfangsbehörde handelt, hat der Gesetzgeber unterschiedliche Anforderungen an die Übermittlung geknüpft. § 20 HVSG regelt die Übermittlung durch das LfV Hessen an Polizeibehörden, soweit dies zur Abwehr einer wenigstens konkretisierten Gefahr für gewisse Rechtsgüter erforderlich ist. § 20a HVSG enthält die Befugnis zur Informationsübermittlung an Strafverfolgungsbehörden, wenn bestimmte Tatsachen den Verdacht der Begehung einer besonders schweren Straftat begründen. Gemäß § 20b HVSG darf das LfV Hessen Daten an sonstige inländische öffentliche Stellen übermitteln, wenn eine gesetzliche Regelung, die den Schutz eines der in § 20 genannten Rechtsgüter bezweckt, eine Mitwirkung des Landesamts vorsieht und die Datenübermittlung im Einzelfall erforderlich ist, u. a. zur Überprüfung der Zuverlässigkeit der betroffenen Person. Nach § 20c HVSG kann eine Übermittlung zu arbeits- und dienstrechtlichen Zwecken erfolgen, u. a. im Falle von Zuverlässigkeitsüberprüfungen bei Bewerbungen für den Polizeivollzugsdienst.

Änderungen im HSOG

Zum anderen betreffen die Neuregelungen das HSOG. Zu diesen gesetzlichen Neuerungen gehören u. a. eine eigene Vorschrift in § 12a HSOG zum Schutz zeugnisverweigerungsberechtigter Berufsgeheimnisträger, die Änderung von § 14a HSOG im Hinblick auf automatische Kennzeichenlesesysteme vor dem Hintergrund der aktuellen bundesverfassungsgerichtlichen Rechtsprechung und die Streichung der zeitlichen Obergrenze von einem Jahr für die Ver-

längerung der richterlichen Anordnung von verdeckten Maßnahmen in § 15 Abs. 5 HSOG. § 16 HSOG enthält neue Regelungen für die Datenerhebung durch den Einsatz von V- Leuten, insbesondere mit Blick auf Erkenntnisse aus dem Kernbereich privater Lebensgestaltung. Zudem sieht § 31a Abs. 1 HSOG bei der elektronischen Aufenthaltsüberwachung nun die Verpflichtung vor, ein zur Verfügung gestelltes Mobiltelefon ständig in betriebsbereitem Zustand bei sich zu führen, und § 98a HSOG führt eine Legitimations- und Kennzeichnungspflicht für die Vollzugspolizei ein.

Einige weitere Neuregelungen möchte ich im Folgenden unter Bezugnahme auf meine Stellungnahmen im Gesetzgebungsverfahren kurz erläutern.

Regelüberprüfung und keine zwingende Schriftform bei Zuverlässigkeitsüberprüfungen

Der neu gefasste § 13a Abs. 2 HSOG sieht nunmehr eine Überprüfung von Bediensteten, die eine Tätigkeit in einer Behörde mit Vollzugsaufgaben anstreben, regelmäßig auch anhand von Datenbeständen des LfV Hessen vor. Damit wird die Zuverlässigkeitsüberprüfung im Hinblick auf Bewerberinnen und Bewerber in diesem Bereich von einer Einbeziehung von Datenbeständen des Verfassungsschutzes im Einzelfall hin zu einer Regelüberprüfung erweitert. Zu dieser Neuregelung hatte ich in meiner Stellungnahme zum Gesetzentwurf verschiedene datenschutzrechtliche Bedenken geäußert, die jedoch vom Gesetzgeber nicht aufgegriffen wurden.

Eine weitere Änderung betrifft die Streichung des zwingenden Schriftformerfordernisses in § 13a Abs. 2 HSOG für die Einwilligung in eine Zuverlässigkeitsüberprüfung. Für die Form der Einwilligung gelten nun keine spezifischen Vorgaben mehr, sondern die allgemeinen Voraussetzungen des § 46 HDSIG. Aber auch nach dieser Regelung muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können. Der Gesetzgeber hat diese Änderung mit einer erhöhten Praxistauglichkeit begründet.

§ 13a HSOG:

(2) Die Polizeibehörde kann die Identität der Person feststellen, deren Zuverlässigkeit überprüft werden soll, und zu diesem Zweck von ihr vorgelegte Ausweisdokumente kopieren oder Kopien von Ausweisdokumenten anfordern. Die Überprüfung erfolgt mit Einwilligung der betroffenen Person anhand von Datenbeständen der Polizeien des Bundes und der Länder, im Fall von Erkenntnissen über Strafverfahren auch der Justizbehörden und Gerichte sowie, soweit im Einzelfall erforderlich, des Landesamts für Verfassungsschutz. Im Fall des Abs. 1 Satz 1 Nr. 1 Buchst. a ist eine Überprüfung der betroffenen Personen anhand von Datenbeständen des Landesamts für Verfassungsschutz regelmäßig erforderlich. Für die Einwilligung gilt § 46 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes.

Der betroffenen Person ist zudem mitzuteilen, wo sie weitere Auskünfte zu dem Verfahren erhalten kann und dass sie sich gleichfalls an den Hessischen Datenschutzbeauftragten wenden kann. Ihr ist Gelegenheit zur Stellungnahme zu geben.

Videoüberwachung ohne Kriminalitätsanalyse mit Vermutungsregelung

In meiner Stellungnahme zum Gesetzentwurf hatte ich mich kritisch zu der neuen Regelung in § 14 Abs. 3a HSOG geäußert, die die Voraussetzungen für eine Videoüberwachung nach § 14 Abs. 3 Satz 1 HSOG in den öffentlich zugänglichen Bereichen von Flughäfen, Personenbahnhöfen, Sportstätten, Einkaufszentren und Packstationen grundsätzlich als erfüllt angesehen hätte. Mithin wäre an diesen Örtlichkeiten jegliche Kriminalitätsanalyse entfallen und eine Videoüberwachung regelmäßig zulässig gewesen. Der Gesetzgeber hat auf diese Kritik reagiert und § 14 Abs. 3a HSOG zumindest um eine sog. Beweislastumkehr in Form einer Vermutungsregelung ergänzt. So soll die Polizei nun mittels einer kursorischen Prüfung ausschließen können, dass die Voraussetzungen gemäß § 14 Abs. 3 Satz 1 HSOG in den öffentlich zugänglichen Bereichen der genannten Örtlichkeiten fehlen. Sie darf die Videoüberwachung dann auf die Vermutung stützen, dass sie zur Abwehr einer Gefahr oder aufgrund einer auf tatsächlichen Anhaltspunkten beruhenden Annahme, dass Straftaten drohen, gerechtfertigt ist. Eine solche, im Idealfall nachvollziehbar dokumentierte Prüfung ist Voraussetzung dafür, dass auch im Rahmen von datenschutzrechtlichen Kontrollen oder der Bearbeitung von datenschutzrechtlichen Beschwerden Entscheidungen nachvollzogen und bewertet werden können.

§ 14 HSOG:

(3) Die Gefahrenabwehr- und die Polizeibehörden können zur Abwehr einer Gefahr oder wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen, öffentlich zugängliche Orte mittels Bildübertragung offen beobachten und aufzeichnen. Der Umstand der Überwachung sowie der Name und die Kontaktdaten der oder des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Fest installierte Anlagen sind alle zwei Jahre daraufhin zu überprüfen, ob die Voraussetzungen für ihren Betrieb weiterhin vorliegen. Abs. 1 Satz 2 und 3 gilt entsprechend.

(3a) Es wird vermutet, dass die Voraussetzungen nach Abs. 3 Satz 1 in den öffentlich zugänglichen Bereichen von Flughäfen, Personenbahnhöfen, Sportstätten, Einkaufszentren und Packstationen vorliegen. Abs. 1 Satz 2 und 3 und Abs. 3 Satz 2 und 3 gilt entsprechend.

Nicht aufgegriffen wurde jedoch meine Kritik zur Einbeziehung von Packstationen, allen Sportstätten und Einkaufszentren in die Vermutungsregelung

des § 14 Abs. 3a HSOG sowie zu den räumlichen Grenzen der aufgezählten Örtlichkeiten. Der neuen Regelung mangelt es nach wie vor an einer hinreichenden Bestimmtheit der „öffentlich zugänglichen Bereiche“ dieser Örtlichkeiten. Dies ist insbesondere in Bezug auf den Großflughafen Frankfurt am Main problematisch.

Verwaltungsvorschrift und Negativprognose bei der Datenweiterverarbeitung

§ 20 Abs. 6 HSOG enthält nunmehr eine Vorgabe für eine Verwaltungsvorschrift zur Regelung der Übermittlung von Verfahrensausgängen und Einstellungsbegründungen seitens der Staatsanwaltschaften an die Hessische Polizei sowie das Erfordernis einer individuellen Negativprognose. Mit der Negativprognose als Voraussetzung für die Weiterverarbeitung von personenbezogenen Daten Tatverdächtigter, die bei der Strafverfolgung gewonnen wurden, hat der Gesetzgeber zumindest teilweise auf meine kritischen Anmerkungen zum Gesetzentwurf reagiert. Allerdings orientiert sich die gewählte Formulierung nicht an der von mir beschriebenen Formulierung für eine Negativprognose in § 18 Abs. 1 Nr. 3 BKAG.

§ 20 HSOG

Die Polizeibehörden können, soweit Bestimmungen der Strafprozessordnung oder andere Rechtsvorschriften nicht entgegenstehen, personenbezogene Daten, die sie im Rahmen der Verfolgung von Straftaten gewonnen haben, weiterverarbeiten, soweit dies zur Abwehr einer Gefahr oder zur vorbeugenden Bekämpfung von Straftaten erforderlich ist. Bei den Daten von Personen, die verdächtig sind, eine Straftat begangen zu haben, ist die Weiterverarbeitung nur zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass zukünftig Strafverfahren gegen die betroffenen Personen zu führen sein werden; entfällt der Verdacht, sind die Daten zu löschen. Näheres zur Übermittlung von Verfahrensausgängen und Einstellungsbegründungen seitens der Staatsanwaltschaft an die Polizei wird in einer gemeinsamen Verwaltungsvorschrift des Ministeriums des Innern und für Sport und des Ministeriums der Justiz geregelt.

Verlängerung der Aussonderungsprüffristen bei Datenspeicherung

In meiner Stellungnahme zum Gesetzentwurf hatte ich auch kritische Anmerkungen zur Gesetzesänderung in § 27 Abs. 4 HSOG gemacht, die eine erhebliche Verlängerung der Aussonderungsprüffristen bei personenbezogenen Daten, die nach § 20 Abs. 6 HSOG gespeichert sind, 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. Zwar entschärft sich durch die Aufnahme der Negativprognose in § 20

Abs. 6 HSOG die Problematik der Verlängerung der Aussonderungsprüfdaten hier ein wenig, allerdings erscheint eine einmalige Negativprognose zur auslösenden Speicherung für eine Dauer von nunmehr bis zu 20 Jahren aus datenschutzrechtlicher Sicht weiterhin bedenklich. Es erfolgte zudem keine Anpassung der Formulierung „bei fortbestehendem Verdacht“, die als Zulässigkeitsvoraussetzung für eine weitere Speicherung keine tatsächliche Schranke einzieht, da nicht erkennbar ist, wie etwa nach Ablauf der ersten zehn Jahre Regelspeicherung plötzlich ein Verdacht nicht mehr fortbestehen könnte. Der Gesetzgeber hat mithin meine Kritik nur teilweise aufgenommen.

§ 27 HSOG

(4) Die Ministerin oder der Minister des Innern wird ermächtigt, durch Rechtsverordnung die Fristen, nach deren Ablauf zu prüfen ist, ob die weitere Speicherung der Daten zur Aufgabenerfüllung erforderlich ist und gegebenenfalls nach deren Ablauf eine Löschung vorzusehen ist, zu bestimmen. Bei Daten, die nach § 20 Abs. 6 gespeichert sind, dürfen die Fristen für die Prüfung

1. *bei Erwachsenen zehn Jahre,*
2. *bei Jugendlichen fünf Jahre und*
3. *bei Kindern zwei Jahre*

nicht überschreiten, wobei unter Berücksichtigung des Verfahrensausgangs nach Art und Zweck der Speicherung sowie Art und Bedeutung des Anlasses zu unterscheiden ist. In Fällen von geringerer Bedeutung sind kürzere Fristen vorzusehen, die in den Fällen des Satz 2 Nr. 1 fünf Jahre nicht überschreiten dürfen. Die Frist für eine Verlängerung der Datenspeicherung nach Ablauf der Frist nach Satz 2 Nr. 1 darf bei fortbestehendem Verdacht einer terroristischen Straftat oder einer Sexualstraftat nach dem 13. Abschnitt des Strafgesetzbuchs (ausgenommen die §§ 183a, 184, 184d und 184e des Strafgesetzbuchs) oder einer sexuell bestimmten Straftat nach den §§ 211 bis 213 und 223 bis 228 des Strafgesetzbuchs zehn Jahre und bei fortbestehendem Verdacht einer sonstigen Straftat von erheblicher Bedeutung fünf Jahre nicht überschreiten. Weitere Verlängerungen der Frist sind bei fortbestehendem Verdacht einer terroristischen Straftat oder einer Sexualstraftat nach Satz 4 um bis zu fünf Jahre und bei fortbestehendem Verdacht einer sonstigen Straftat von erheblicher Bedeutung um bis zu zwei Jahre nur zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass die Person solche Straftaten begehen wird. Die Frist beginnt regelmäßig mit dem letzten Anlass der Speicherung, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentzug verbundenen Maßregel der Besserung und Sicherung. Werden innerhalb der Frist nach Satz 2 bis 6 weitere personenbezogene Daten über dieselbe Person gespeichert, gilt für alle Speicherungen gemeinsam die Frist, die als letzte abläuft. Bei Daten, die nach § 20 Abs. 7 über die in § 13 Abs. 2 Nr. 2 bis 5 genannten Personen gespeichert sind, dürfen die Fristen für die Prüfung drei Jahre nicht überschreiten; die Entscheidung, dass eine weitere Speicherung erforderlich ist, trifft die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter. Die Gründe für die Verlängerung der Frist nach Satz 4 und 5 sind aktenkundig zu machen. Die Beachtung der Prüfungstermine und Aufbewahrungsfristen ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten.

Elektronische Aufenthaltsüberwachung bei Platzverweis, Aufenthalts- und Kontaktverbot

In meiner Stellungnahme zum Gesetzentwurf hatte ich die vorgeschlagene Änderung des § 31 Abs. 2 Satz 3 HSOG kritisch kommentiert. Diese ermöglichte es den Gefahrenabwehr- und Polizeibehörden, die Verbindung eines Platzverweises, eines Aufenthalts- oder Kontaktverbotes nach § 31 Abs. 2 Satz 1 und 2 HSOG mit einer elektronischen Aufenthaltsüberwachung im Sinne von § 31a HSOG anzuordnen, ohne dass hierfür weitere Voraussetzungen festgelegt wurden. Hierauf habe ich mit Blick auf eine verhältnismäßige und verfassungskonforme Anwendung der Norm hingewiesen, wenn z. B. keinerlei Anhaltspunkte dafür vorliegen, dass die betreffende Person sich nicht an den Platzverweis, das Aufenthalts- oder Kontaktverbot hält. Auf diese Kritik hat der Gesetzgeber mit der Regelung in § 31 Abs. 2 Satz 3 HSOG reagiert und die Vorgabe aufgenommen, dass tatsächliche Anhaltspunkte die Annahme rechtfertigen müssen, dass sich die betreffende Person der Maßnahme widersetzen wird.

§ 31 HSOG

(2) Die Gefahrenabwehr- und die Polizeibehörden können eine Person bis zu einer richterlichen Entscheidung über zivilrechtliche Schutzmöglichkeiten ihrer Wohnung und des unmittelbar angrenzenden Bereichs verweisen, wenn dies erforderlich ist, um eine von ihr ausgehende gegenwärtige Gefahr für Leib, Leben oder Freiheit von Bewohnern derselben Wohnung abzuwehren. Unter den gleichen Voraussetzungen kann ein Betretungsverbot angeordnet und der Kontakt mit bestimmten Personen oder Personen einer bestimmten Gruppe untersagt werden. Eine Maßnahme nach Satz 1 oder 2 kann mit einer elektronischen Aufenthaltsüberwachung im Sinne des § 31a Abs. 1 verbunden werden, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass sich die betroffene Person der Maßnahme nach Satz 1 oder 2 widersetzen wird, und darf die Dauer von vierzehn Tagen nicht überschreiten. Die Maßnahme kann um weitere vierzehn Tage verlängert werden, wenn bis zu diesem Zeitpunkt eine wirksame richterliche Entscheidung über den zivilrechtlichen Schutz nicht getroffen worden ist. Das Gericht hat der zuständigen Gefahrenabwehrbehörde oder der Polizeibehörde die Beantragung des zivilrechtlichen Schutzes sowie den Tag und den Inhalt der gerichtlichen Entscheidung unverzüglich mitzuteilen. Für die elektronische Aufenthaltsüberwachung gelten im Übrigen die Bestimmungen des § 31a entsprechend.

4.3
Datenschutzkontrollen bei Polizeibehörden und Verfassungsschutz

Gesetzliche Regelungen schreiben in verschiedenen Bereichen vor, dass ich bestimmte Datenschutzkontrollen durchführe. Für das Jahr 2023 war turnusmäßig die Rechtsextremismus-Datei (RED) zu prüfen. Des Weiteren erfolgte eine Beanstandung als aufsichtsbehördliche Maßnahme im Zuge der

im Jahr 2021 erstmalig durchgeführten Datenschutzkontrolle von Ausschreibungen im Schengener Informationssystems der zweiten Generation (SIS II). Darüber hinaus konnte ich die 2022 begonnene Datenschutzkontrolle zu Telekommunikationsüberwachungen abschließen und Übermittlungen von personenbezogenen Daten Minderjähriger durch hessische Polizeidienststellen an Europol prüfen. Im Weiteren begann ich mit Datenschutzkontrollen, zu vergebenen personenbezogenen Hinweisen (PHW) bei der Hessischen Polizei und zum Zeugenschutz im Bundeszentralregister (BZR).

Beim Hessischen Landesamt für Verfassungsschutz (LfV Hessen) und dem Hessischen Landeskriminalamt (HLKA) führte ich jeweils eine Datenschutzkontrolle zu Neuspeicherungen von Personen in der RED innerhalb der Jahre 2021 und 2022 durch. Der Schwerpunkt dieser Prüfungen lag auf Speicherungen gemäß § 2 RED-G. Im Ergebnis erfolgten die Speicherungen durch das LfV Hessen und HLKA ordnungsgemäß ohne datenschutzrechtliche Bedenken.

§ 2 RED-G

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

1. *Personen,*

a) *bei denen Tatsachen die Annahme rechtfertigen, dass sie einer terroristischen Vereinigung nach § 129a des Strafgesetzbuchs mit rechtsextremistischem Hintergrund angehören oder diese unterstützen,*

b) *die als Täter oder Teilnehmer einer rechtsextremistischen Gewalttat Beschuldigte oder rechtskräftig Verurteilte sind;*

2. *Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie rechtsextremistische Bestrebungen verfolgen und in Verbindung damit zur Gewalt aufrufen, die Anwendung von rechtsextremistisch begründeter Gewalt als Mittel zur Durchsetzung*

   politischer Belange unterstützen, vorbereiten oder durch ihre Tätigkeiten vorsätzlich hervorrufen oder bei denen Schusswaffen ohne die erforderlichen waffenrechtlichen Berechtigungen, Kriegswaffen oder Explosivstoffe aufgefunden wurden, (…)

§ 11 RED-G

(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 Rechtsextremismus-Datei 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 § 9 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.

Nach Abschluss der Datenschutzkontrolle zu Ausschreibungen gemäß Art. 36 Abs. 2 SIS II-Beschluss wurde gegenüber dem Landespolizeipräsidenten im Hessischen Ministerium des Inneren und für Sport (HMdIS) eine Beanstandung gemäß § 14 Abs. 2 HDSIG wegen vier Ausschreibungen von Kontaktpersonen ausgesprochen. In seiner Stellungnahme zu dieser Beanstandung wurde die Rechtsauffassung meiner Behörde zur Unzulässigkeit der Ausschreibung von Kontaktpersonen im SIS nicht geteilt. Weitere aufsichtsbehördliche Maßnahmen werden aktuell geprüft; die vier Ausschreibungen der Kontaktpersonen, die Gegenstand der Beanstandung waren, wurden zwischenzeitlich gelöscht.

Artikel 36 SIS II-Beschluss

(1) Daten in Bezug auf Personen oder Fahrzeuge, Wasserfahrzeuge, Luftfahrzeuge und Container werden nach Maßgabe des nationalen Rechts des ausschreibenden Mitgliedstaats zur verdeckten Kontrolle oder zur gezielten Kontrolle gemäß Artikel 37 Absatz 4 eingegeben.

(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.

Gemäß § 29a Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) wurden turnusmäßig verdeckte Maßnahmen kontrolliert. Gegenstand der aktuellen Prüfung waren Telekommunikationsüberwachungsmaßnahmen der Hessischen Polizei gemäß § 15a Abs. 1 und 3 HSOG, wobei die Prüfung

beim HLKA stattfand. Hierbei wurden die formellen Voraussetzungen der jeweiligen Anordnungen, das Vorliegen entsprechender richterlicher Beschlüsse sowie die Benachrichtigung und Protokollierung geprüft. Im Ergebnis kann berichtet werden, dass keine datenschutzrechtlichen Defizite bei den Anordnungen der verdeckten Überwachungsmaßnahmen bestehen. Bezüglich der Benachrichtigungen und Protokollierungen wurden Handlungsbedarfe festgestellt und ausgesprochen. In der Folge erarbeitet das HLKA nun u. a. eine neue Dienstanweisung zu gesetzlichen Vorgaben im Zusammenhang mit verdeckten präventivpolizeilichen Maßnahmen.

§ 29a HSOG

Die oder der Hessische Datenschutzbeauftragte führt unbeschadet ihrer oder seiner sonstigen Aufgaben und Kontrollen mindestens alle zwei Jahre zumindest stichprobenartig Kontrollen bezüglich der Datenverarbeitung bei nach § 28 Abs. 2 zu protokollierenden Maßnahmen und von Übermittlungen nach § 23 durch.

Auf Anregung des Europäischen Datenschutzbeauftragten erfolgte eine gemeinsame und koordinierte Datenschutzkontrolle der Übermittlung von personenbezogenen Daten Minderjähriger durch Polizeibehörden des Bundes und der Länder an Europol. Seitens hessischer Polizeidienststellen erfolgten in drei Ermittlungskomplexen Übermittlungen an Europol. Grund dafür war jeweils ein Altersfeststellungsverfahren. Die betroffenen Personen waren zur Tatzeit nach eigenen Angaben minderjährig oder teilweise auch strafunmündig. Der Polizei lagen jedoch tatsächliche Anhaltspunkte für Strafmündigkeit und in einigen Fällen auch Volljährigkeit vor. Im Ergebnis bestanden bezüglich dieser Übermittlungen keine datenschutzrechtlichen Bedenken.

Des Weiteren führte ich eine Datenschutzkontrolle zu polizeilich vergebenen personenbezogenen Hinweisen (PHW) – konkret zum PHW „Betäubungsmittelkonsument“ (BTMK) – durch. Polizeibehörden dürfen in polizeilichen Auskunftssystemen eine solche Speicherung vornehmen. Die Speichervoraussetzungen und deren Dokumentation waren Gegenstand der Datenschutzkontrolle. Es wurden insgesamt 35 Vergaben des PHW BTMK zweier Polizeipräsidien anhand von Kriminalakten geprüft. Bis zur Fertigstellung dieses Tätigkeitsberichts war die Kontrolle noch nicht beendet.

Zum Ende des Jahres 2023 erfolgte eine Datenschutzkontrolle zum Zeugenschutz im BZR gemäß § 44a Bundeszentralregistergesetz, die noch nicht abgeschlossen ist.

Über das Ergebnis dieser beiden Kontrollen wird im nächsten Tätigkeitsbericht informiert.

§ 44a BZRG

(1) Die Registerbehörde sperrt den Datensatz einer im Register eingetragenen Person für die Auskunftserteilung, wenn eine Zeugenschutzstelle mitteilt, dass dies zum Schutz der Person als Zeuge oder Zeugin erforderlich ist.

(2) Die Registerbehörde soll die Erteilung einer Auskunft aus dem Register über die gesperrten Personendaten versagen, soweit entgegenstehende öffentliche Interessen oder schutzwürdige Interessen Dritter nicht überwiegen. Sie gibt der Zeugenschutzstelle zuvor Gelegenheit zur Stellungnahme; die Beurteilung der Zeugenschutzstelle, dass die Versagung der Auskunft für Zwecke des Zeugenschutzes erforderlich ist, ist für die Registerbehörde bindend. Die Versagung der Auskunft bedarf keiner Begründung.

(3) Die Registerbehörde legt über eine Person, über die keine Eintragung vorhanden ist, einen besonders gekennzeichneten Personendatensatz an, wenn die Zeugenschutzstelle darlegt, dass dies zum Schutze dieser Person als Zeuge oder Zeugin vor Ausforschung durch missbräuchliche Auskunftsersuchen erforderlich ist. Über diesen Datensatz werden Auskünfte nicht erteilt. Die Registerbehörde unterrichtet die Zeugenschutzstelle über jeden Antrag auf Erteilung einer Auskunft, der zu dieser Person oder zu sonst von der Zeugenschutzstelle bestimmten Daten eingeht.

4.4
Prüfung einer Staatsanwaltschaft bei verdeckten Maßnahmen nach § 100a StPO

Im Herbst 2023 habe ich eine weitere Datenschutzkontrolle bei einer hessischen Staatsanwaltschaft durchgeführt. Der Schwerpunkt lag hierbei wieder auf der Telekommunikationsüberwachung nach § 100a StPO. Die Prüfung konzentrierte sich insbesondere auf Rechtmäßigkeit, Dokumentation sowie Benachrichtigung betroffener Personen und das Unterbleiben oder endgültige Absehen von Benachrichtigungen. Zudem wurde die Zurückstellung der Benachrichtigung nach § 101 Abs. 5 Satz 2 und Abs. 6 StPO 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 meinen Mitarbeiterinnen, meinen Mitarbeitern und mir dabei Untersuchungs- und Kontrollbefugnisse zu.

Eine Telekommunikationsüberwachung nach § 100a StPO stellt eine besonders eingriffsintensive Maßnahme der Strafverfolgung dar. Im Zuge von Überwachungsmaßnahmen gemäß § 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 gemäß § 101 Abs. 4 Satz 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 Voraussetzung. Grundsätzlich hat die Benachrichtigung der betroffenen Person gemäß § 101 Abs. 5 Satz 1 StPO zu erfolgen, sobald dies ohne Gefährdung des Untersuchungszwecks, des Lebens, der körperlichen Unversehrtheit und der persönlichen Freiheit einer Person und von bedeutenden Vermögenswerten möglich ist. Die Benachrichtigung kann gemäß § 101 Abs. 5 Satz 2 StPO zurückgestellt werden, die Gründe hierfür sind aktenkundig zu machen. Erfolgt binnen zwölf Monaten nach der Zurückstellung keine Benachrichtigung, bedarf es gemäß § 101 Abs. 6 StPO für jede weitere Zurückstellung der gerichtlichen Zustimmung. Unter den Voraussetzungen des § 101 Abs. 4 Satz 3 und 4 StPO kann eine Benachrichtigung betroffener Personen zudem unterbleiben.

Für eine Stichprobe wurden Akten angefordert, die Ermittlungen betrafen, während derer Maßnahmen zur Telekommunikationsüberwachung gemäß § 100a StPO angeordnet waren. Bei der Auswahl wurde darauf geachtet, möglichst viele Dezernate und örtliche Zuständigkeitsbereiche abzudecken. Ein Großteil der Akten konnte bereitgestellt werden und innerhalb des zur Verfügung stehenden Zeitrahmens einer Überprüfung unterzogen werden. Einige wenige Akten befanden sich zum Zeitpunkt der Prüfung bei anderen Behörden und wurden dort für laufende Verfahren benötigt.

Besonderes Augenmerk sollte auf dem Vorliegen der richterlichen Anordnung für die jeweilige Maßnahme und der Durchführung der Benachrichtigung betroffener Personen sowie der Dokumentation liegen. Sofern die Benachrichtigung zurückgestellt wurde, sollte die Zurückstellung anhand der gesetzlichen Vorgaben überprüft werden.

Im Ergebnis waren die richterlichen Beschlüsse als Rechtsgrundlage der verdeckten Maßnahmen in den Akten vollumfänglich vorhanden und ordnungsgemäß dokumentiert. Ich konnte jedoch ergänzende Hinweise zu einer umfangreicheren Dokumentation der Benachrichtigungen von betroffenen Personen und der Abwägungsentscheidungen beim Unterbleiben von Benachrichtigungen geben. Mit einer solchen schriftlichen Dokumentation wird die Rechtssicherheit für die anordnende Behörde erhöht und die

Nachvollziehbarkeit der Rechtmäßigkeit im Falle von späteren Beschwerden Betroffener sichergestellt.

Die Zurückstellungen nach § 101 Abs. 5 StPO und deren Begründung durch die Staatsanwaltschaft waren anhand der Aktenlage nicht immer und nicht in Bezug auf alle Beteiligten/Betroffenen eindeutig nachzuvollziehen. Teilweise wurde die erstmalige Zurückstellung der Benachrichtigung durch das Gericht im Anordnungsbeschluss zur Maßnahme angeordnet. Für diese Akten fehlte es im Umkehrschluss jeweils an einer Zurückstellung durch die Staatsanwaltschaft, die trotz des gerichtlichen Beschlusses für die erstmalige Zurückstellung zuständig bleibt.

Die Ergebnisse und Handlungsbedarfe wurden unter Einbeziehung des Datenschutzbeauftragten der geprüften Staatsanwaltschaft sowie mit der Generalstaatsanwaltschaft erörtert. Die Dezernate der Staatsanwaltschaft sind bereits für das Thema Benachrichtigungen in der Folge von Maßnahmen zur Telekommunikationsüberwachung durch den Verantwortlichen sensibilisiert 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.

4.5
Veröffentlichung unzureichend anonymisierter Gerichtsentscheidungen

Im Wege einer Beschwerde wurde mir mitgeteilt, dass zwei unzureichend anonymisierte Gerichtsentscheidungen veröffentlicht wurden. Zusammen mit den beteiligten Gerichten konnte die Entfernung aus den Landesrechtsprechungsdatenbanken erreicht – und so eine weitere, digitale Verbreitung der personenbezogenen Daten des Beschwerdeführers eingedämmt werden.

Anfang des Jahres erreichte mich eine Beschwerde, wonach bei der Volltextveröffentlichung zweier Gerichtsentscheidungen eine mögliche Persönlichkeitsrechtsverletzung gegeben sei. Der Beschwerdeführer machte geltend, die fraglichen Texte seien zwar vor der Veröffentlichung bearbeitet worden, jedoch lasse sich aus der Kombination enthaltener Angaben (u. a.

Geburtsdatum, Wohnort, Dienstbezeichnung) auch für unbeteiligte Dritte immer noch eindeutig auf seine Person rückschließen. Im Rahmen des zugrundeliegenden Rechtsstreits waren außerdem besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DS-GVO als Sachvortrag in die Entscheidungen eingeflossen und aus diesen ersichtlich. Entscheidungsdatenbanken im Internet hatten die Texte bereits übernommen, so dass negative Auswirkungen für die Persönlichkeitsrechte des Betroffenen aufgrund des Wiedererkennungswerts wahrscheinlich waren.

Ich habe mich umgehend mit den Gerichten in Verbindung gesetzt, um zunächst die Veröffentlichung in der hessischen Landesrechtsprechungsdatenbank überprüfen zu lassen.

Beide Gerichte konnten nachvollziehen, dass angesichts der im Volltext vorhandenen Angaben zum Beschwerdeführer nicht von einer Anonymisierung im Sinne der Entfernung jeglichen Personenbezugs gesprochen werden konnte. Eine Veröffentlichung war daher unter Einbeziehung der schutzwürdigen Belange des Beschwerdeführers nicht zu rechtfertigen. Die Verantwortlichen veranlassten die Löschung der fraglichen Entscheidungen aus den Landesrechtsprechungsdatenbanken und bestätigten dies mir gegenüber. In der Folge konnte auch die Veröffentlichung in weiteren Rechtsprechungsdatenbanken rückgängig gemacht werden.

Auch wenn in diesem Fall von allen Beteiligten schnell reagiert worden ist, so lassen sich entsprechende Beeinträchtigungen der Persönlichkeitsrechte nur mit Wirkung für die Zukunft abstellen. Es liegt insofern in der Natur des Internets, dass mit einer schnellen Verbreitung und großen Streubreite personenbezogener Daten zu rechnen ist. Hier konnte durch ein zeitnahes Handeln der beteiligten Akteure zumindest eine weitere, digitale Verbreitung der personenbezogenen Daten des Beschwerdeführers verhindert werden.

Festzuhalten ist, dass für eine wirksame Anonymisierung jeder Personenbezug der veröffentlichten Daten auszuschließen ist. Dabei ist zu berücksichtigen, ob andere Personen, die die Veröffentlichung zur Kenntnis nehmen, aufgrund ihres Zusatzwissens aus den noch vorhandenen Daten auf die betroffene Person schließen können.

5. Allgemeine Verwaltung, Kommunen, Sozialverwaltung

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. Bei der Verwaltungsmodernisierung entstehen jedoch immer wieder neue Fragestellungen, wie neue technische Möglichkeiten datenschutzgerecht gestaltet werden können (Kap. 5.1). Dabei kann eine neue Datenschutzleitlinie für die Hessische Landesverwaltung unterstützend wirken (Kap. 5.2). Aber auch in alltäglichen Situationen in den Kommunen besteht ein Bedarf an Beratung und Einschreiten durch die Datenschutzaufsicht (Kap. 5.3). In öffentlichen Stellen stellt sich immer wieder die Frage, welche Interessenkonflikte bei der Ernennung eines Datenschutzbeauftragten auftreten und diese verhindern können (Kap. 5.4). In Einzelfällen gibt es immer wieder Fragestellungen, die beantwortet werden müssen und ein aufsichtsrechtliches Einschreiten erfordern – wie hinsichtlich Melderegisterauskünften bei Wahlen und Abstimmungen (Kap. 5.5), bei Vorschlagslisten für Schöffen (Kap. 5.6) und bei Datenübermittlung von einer Sozialbehörde und einem Veterinäramt (5.7).

5.1
Verwaltungsmodernisierung und Datenschutz

Big Data, KI, Cloud-Transformation, digitale Souveränität oder Datenschutz – unter dem Begriff der Verwaltungsmodernisierung lassen sich eine Vielzahl unterschiedlicher rechtlicher und praktischer Fragestellungen diskutieren. Als Hessischer Beauftragter für Datenschutz und Informationsfreiheit sehe ich meine Aufgabe darin, Verantwortliche bei der Verwaltungsdigitalisierung zu datenschutzrechtlichen Fragestellungen konstruktiv und lösungsorientiert zu beraten, um hierdurch einem effektiven und nachhaltigen Persönlichkeitsrechtsschutz zu gewährleisten.

Um das Ziel einer datenschutzkonformen Verwaltungsmodernisierung zu erreichen, ist dabei ein mehrdimensionales Vorgehen erforderlich: Neben der Beratung einzelner Digitalisierungsprojekte bedarf es ganzheitlicher Ansätze und kreativer Ideen, damit Multiplikatoreneffekte erzielt werden können. Ich habe innerhalb der Hessischen Landesverwaltung im Berichtszeitraum daher an unterschiedlichen Projekten und Themen gearbeitet, um einer datenschutzkonformen Verwaltungsdigitalisierung Vorschub zu leisten.

Die nachfolgende Auswahl soll einen Überblick über die Bandbreite meiner Tätigkeitsfelder im Berichtszeitraum geben.

Berücksichtigung von Barrierefreiheit, Informationssicherheit und Datenschutz bei IT-Vorhaben

Die Umsetzung von IT-Vorhaben im öffentlichen Bereich stellt Verantwortliche häufig vor praktische (z. B. ausreichende personelle und finanzielle Ressourcen) und rechtliche (z. B. Anforderungen des Vergabe- oder Datenschutzrechts) Herausforderungen. Während einige Fragestellungen projektspezifischer Natur sind, müssen die Querschnittsthemen Barrierefreiheit, Informationssicherheit und Datenschutz bei jedem IT-Projekt der Hessischen Landesverwaltung berücksichtigt werden. Das Landeskompetenzzentrum Barrierefreie IT (LBIT), die Abteilung Cyber- und IT-Sicherheit des Hessischen Ministeriums des Innern und für Sport (HMdIS) und ich haben in Abstimmung mit der HMinD einen übergeordneten Landesstandard zur Integration der drei Querschnittsthemen in Projekten und Verfahren erarbeitet. Verantwortlichen soll hierdurch die Umsetzung der Anforderungen der barrierefreien Informationstechnik, der Informationssicherheit und des Datenschutzes erleichtert werden.

Regelmäßiger Austausch zu Digitalthemen

Für eine stetige Fortentwicklung des Datenschutzes in der Hessischen Landesverwaltung ist ein kontinuierlicher Austausch mit zentralen Stakeholdern der Verwaltungsdigitalisierung erforderlich. Im Berichtszeitraum habe ich mich daher regelmäßig etwa mit der HMinD, der Staatskanzlei, der HZD und der ekom21 zu Fragen der Verwaltungsdigitalisierung und des Datenschutzes abgestimmt. Gesprächsschwerpunkte haben hier etwa die Themen Einsatz von Cloud-Technologien, EU-U.S. Data Privacy Framework, datenschutzkonformer Einsatz von Videokonferenzsystemen oder auch die Umsetzung des Onlinezugangsgesetzes gebildet.

Gemeinsame Entwicklung eines zukunftsfähigen Datenschutzmanagements

Als IT-Dienstleister der Hessischen Landesverwaltung hat die HZD im Kontext der Verwaltungsdigitalisierung eine besondere Rolle inne. Denn auch wenn die HZD im Verhältnis zu den Stellen der Hessischen Landesverwaltung in der Regel als Auftragsverarbeiter tätig wird und die datenschutzrechtliche Verantwortlichkeit bei den Auftraggebern verbleibt: Sie wirkt an der digitalen Strategie des Landes mit, berät die Ressorts, entwickelt IT-Lösungen und

stellt die IT-Infrastruktur für alle Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes bereit.

Die HZD hat daher nicht nur erheblichen Einfluss darauf, dass in der Hessischen Landesverwaltung datenschutzkonforme IT-Verfahren eingesetzt werden. Sie verfügt zudem über das notwendige Fachwissen, um bestimmte Fragen des Datenschutzes behördenübergreifend zu beantworten. So kann sie den Dienststellen beispielsweise eine generische Verfahrensdokumentation der eingesetzten IT zur Verfügung zu stellen (z. B. zur Vorbereitung eines Verzeichnisses der Verarbeitungstätigkeit im Sinne von Art. 30 Abs. 1 DS-GVO) und hierdurch einen wichtigen Beitrag zu einer datenschutzkonformen Verwaltungsmodernisierung leisten.

Aufgrund ihrer herausgehobenen Stellung benötigt die HZD ein zukunftsfähiges, effektives und nachhaltiges Datenschutzmanagement. Im Berichtszeitraum haben die HZD und meine Behörde daher, im Rahmen mehrerer Workshops gemeinsam Leitgedanken entwickelt, die seitens der HZD nunmehr als Grundlage für die Einführung eines neuen Datenschutzmanagements dienen. Zentraler Baustein eines gelungenen Datenschutzmanagements ist u. a. ein gemeinsames Aufgaben- und Rollenverständnis. Insbesondere bedarf es einer Differenzierung zwischen den Personen, welche die Funktion des Datenschutzbeauftragten übernehmen, und den Personen, die den Verantwortlichen bei der Umsetzung seiner datenschutzrechtlichen Aufgaben operativ unterstützen. Denn während den Datenschutzbeauftragten die Erfüllung der in Art. 39 DS-GVO und § 7 HDSIG genannten Aufgaben (z. B. Beratung, Sensibilisierung, Überwachung und Information) obliegen, unterstützen Beschäftigte des operativen Datenschutzes bei der Erfüllung der dem Verantwortlichen oder dem Auftragsverarbeiter zugewiesenen Aufgaben (z. B. datenschutzrechtliches Vertragsmanagement, Erstellung von Verfahrensdokumentation oder von Datenschutzerklärungen, Durchführung einer Datenschutz-Folgenabschätzung, Verfahren zur regelmäßigen Überprüfung der technischen und organisatorischen Maßnahmen). Sowohl für die Erfüllung der Aufgaben des Datenschutzbeauftragten als auch für den operativen Datenschutz müssen ausreichend personelle Ressourcen zur Verfügung stehen. Andernfalls können auch die besten Konzepte eines gelungenen Datenschutzmanagements in der Praxis keine ausreichende Wirkung entfalten.

Neben der Ausarbeitung gemeinsamer Leitgedanken einer gelungenen Datenschutzorganisation habe ich die HZD in einem IT-Projekt umfassend zu den datenschutzrechtlichen Anforderungen des Verarbeitungsverfahrens selbst und den ihr obliegenden Pflichten als Auftragsverarbeiter nach dem

DV-VerbundG (z. B. Unterhaltung und Pflege eines auf das jeweilige Verfahren abgestimmten Betriebshandbuches) beraten.

Verwaltungsdigitalisierung und Datenschutz sind keine Gegensätze

Die ausgewählten Beispiele meiner Tätigkeit zeigen, dass „datenschutzkonforme Verwaltungsdigitalisierung“ kein Widerspruch in sich ist. Datenschutzgerechte Verwaltungsmodernisierungsprozesse sind möglich, wenn alle Beteiligten dies als gemeinsames Ziel verfolgen und hieran vorurteilsfrei, kooperativ und lösungsorientiert arbeiten.

5.2
Eine Datenschutzleitlinie für die Hessische Landesverwaltung

Leitlinien für die Landesverwaltung sind geeignet, bestimmte gesetzliche Vorgaben, die häufig bewusst abstrakt gehalten sind, um eine möglichst große Zahl von denkbaren Fällen abzudecken, zu konkretisieren. Die einzelnen Ressorts der Hessischen Landesverwaltung sehen sich bei der Umsetzung gesetzlicher Vorgaben oft vergleichbaren Herausforderungen gegenüber. Die angemessene Berücksichtigung des Datenschutzes in IT-Verfahren und Projekten der Landesverwaltung ist eine solche Herausforderung. Daher hat die Landesregierung im Berichtszeitraum Hilfestellungen in Form von Konkretisierungen der gesetzlichen Anforderungen in Gestalt einer Datenschutzleitlinie erarbeitet. Hierbei habe ich sie unterstützt.

Leitlinien zur Konkretisierung gesetzlicher Anforderungen

Gesetzliche Anforderungen müssen in der Regel allgemein genug formuliert sein, um eine Vielzahl möglicher Ausprägungen von Szenarien der Lebenswelt abdecken zu können. Stellenweise führt dies dazu, dass beträchtliche Aufwände erforderlich sind, um für bestimmte, besondere Anwendungsfälle eine Umsetzung der gesetzlichen Anforderungen zu erreichen, oder es bleiben Regelungslücken offen, die in der Praxis zu Unklarheiten oder möglicherweise sogar Gefährdungen für Rechte und Freiheiten betroffener Personen führen können. Dabei muss es sich nicht einmal um unwahrscheinliche oder seltene Anwendungsfälle handeln. Im Gegenteil sind es häufig sogar solche Anwendungsfälle, die viele, große oder bedeutsame Stellen betreffen – so etwa die Ressorts der Hessischen Landesverwaltung –, die diese Herausforderungen mit sich bringen.

Ein Beispiel hierfür ist die Gewährleistung einer angemessenen Informationssicherheit. Sie ist eine Grundvoraussetzung dafür, dass die Hessische Landesverwaltung in einer Zeit der rasch voranschreitenden Digitalisierung die

Erfüllung ihrer Aufgaben gegenüber den Bürgerinnen und Bürgern Hessens sicherstellen kann. Aus diesem Grund hat sich die Landesregierung schon im Jahr 2005 dazu entschlossen, eine erste Informationssicherheitsleitlinie für die Hessische Landesverwaltung zu verabschieden, deren aktuelle Fassung Anregung für eine Datenschutzleitlinie gab.

Datenschutzrechtliche Anforderungen für die Landesverwaltung

Die wirksame und kontinuierliche Umsetzung der Anforderungen der DS-GVO erfordert Maßnahmen der Aufbau- und Ablauforganisation. In allen IT-Verfahren und -Projekten der Ressorts der hessischen Landesverwaltung sind die Datenschutzgrundsätze aus Art. 5 DS-GVO zu beachten. Hierfür trägt die jeweilige Behörde und damit die Behördenleitung die Verantwortung. Sie muss nach Art. 5 Abs. 2 DS-GVO die Grundsätze umsetzen, muss die Umsetzung nachweisen und trägt für die korrekte Umsetzung die Beweislast. Diese Anforderungen kann sie nur erfüllen, wenn sie ein Datenschutzmanagement betreibt, das die frühzeitige und umfängliche Beachtung der Grundsätze in all ihren IT-Projekten und -Verfahren sicherstellt und dokumentiert. Dieser operative Datenschutz ist von den Aufgaben des behördlichen Datenschutzbeauftragten zu unterscheiden, der nach Art. 39 DS-GVO und § 7 HDSIG die Aufgabe hat, die Umsetzung des operativen Datenschutzes zu überwachen und ihm beratend zur Seite zu stehen.

Zu den Aufgaben des Datenschutzmanagements bei den verantwortlichen Behörden gehören insbesondere die Erarbeitung eines Datenschutzkonzepts, die Erstellung eines Verfahrensverzeichnisses, die tatsächliche Durchführung von Datenschutz-Folgenabschätzungen, die Mitwirkung an Verträgen zur Auftragsverarbeitung, die Planung und Umsetzung von geeigneten Prozessen für Einholung, Dokumentation und ggf. Widerruf von Einwilligungen betroffener Personen oder auch Prozesse zur Gewährleistung der Rechte betroffener Personen gemäß Art. 12 ff. DS-GVO.

Diese Aufgaben ergeben sich zwar dem Grunde nach bereits verbindlich aus den Datenschutzgesetzen. Diese enthalten aber keine Vorgaben, welche organisatorischen Vorkehrungen in Behördenalltag dafür zu treffen sind, sie in einheitlicher Weise in der hessischen Landesverwaltung effektiv und effizient umzusetzen.

Erarbeitung einer Datenschutzleitlinie

Die organisatorischen Strukturen eines Datenschutzmanagements und weitere Vorkehrungen bewirken eine tatsächliche Verbesserung des Datenschutzes und tragen somit zu einer Digitalisierung der Verwaltung bei, die

den Bürgerinnen und Bürgern sowie den gesellschaftlichen Anforderungen gerecht wird. Dies wird auch von den Behörden, die mein dahingehendes Beratungsangebot wahrnehmen, so gesehen und bestätigt. Im Berichtsjahr hat sich dies so geäußert, dass die Hessische Ministerin für Digitale Strategie und Entwicklung (HMinD) mit dem Wunsch an mich herangetreten ist, meine Beratung bei der Erarbeitung einer Datenschutzleitlinie für IT-Verfahren und Projekte der Hessischen Landesverwaltung in Anspruch zu nehmen. Ziel dieser Datenschutzleitlinie ist es, der Umsetzung der datenschutzrechtlichen Anforderungen zu dienen und die Empfehlungen für konkrete Hilfestellungen für das Datenschutzmanagement und somit die oben angerissenen „Best Practices“ so festzuhalten, dass diese im Sinne einer gemeinsam nutzbaren Grundlage stets berücksichtigt werden können.

Der ressortübergreifenden Arbeitsgruppe ist es gelungen, im Berichtszeitraum mit meiner Unterstützung einen Entwurf zu erarbeiten, der im weiteren Verlauf auch mit den von der Leitlinie betroffenen Ressorts abgestimmt werden konnte. Im Ergebnis konnte die Leitlinie noch im Berichtszeitraum den zuständigen Gremien ZAL-SMOD und KASMOD in Vorbereitung einer Verabschiedung durch das Kabinett vorgelegt werden.

In der engen und äußerst konstruktiven Zusammenarbeit zwischen der HMinD und den beteiligten Ressorts und unter meiner frühzeitigen Einbindung meiner Behörde ist es gelungen, mit der Datenschutzleitlinie für die Hessische Landesverwaltung nun erstmalig landesweit anwendbare Vorkehrungen für eine wirksame Umsetzung des Datenschutzes in IT-Verfahren und Projekten festzuschreiben. Sie unterstützt die verantwortlichen Behörden als Hilfestellung bei der Bewältigung der ihnen zufallenden datenschutzrechtlichen Aufgaben, durch Empfehlungen bezüglich geeigneter Organisationsstrukturen, Verfahrensabläufe, Aufgabenkataloge, Zuständigkeitsabgrenzungen, Zusammenarbeitsregeln und auch Vereinfachungen.

Um sie durch Erfahrungen aus der Praxis anreichern zu können und ggf. notwendige Anpassungen zu ermöglichen, ist für die Leitlinie nach fünf Jahren eine Evaluierung vorgesehen.

5.3
Datenschutz in Kommunen

Im Berichtszeitraum habe ich mich mit verschiedenen datenschutzrechtlichen Thematiken in der Kommunalverwaltung befasst. 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. Im Folgen-

den möchte ich einen Überblick hinsichtlich ausgewählter Bereiche aus der Aufsichtspraxis geben.

Austausch mit dem Wiesbadener Bürgerbüro

Das Melderecht bildet einen Schwerpunkt meiner aufsichtsbehördlichen Tätigkeit im kommunalen Bereich (s. zuletzt 51. Tätigkeitsbericht, Kap. 6.2).

Um ein besseres Verständnis der Prozesse in einer Meldebehörde zu erlangen, habe ich mich im August 2023 mit Beschäftigten der Wiesbadener Meldebehörde bei einem Vor-Ort-Termin zu vielfältigen Fragen des Meldewesens und des Datenschutzes ausgetauscht.

Schwerpunktmäßig wurden Datenübermittlungen zwischen öffentlichen Stellen nach §§ 33 ff. BMG (insbesondere Datenübermittlungen zwischen den Meldebehörden nach § 33 BMG, Datenübermittlungen an andere öffentliche Stellen nach § 34 BMG und Datenweitergabe nach § 37 BMG) sowie Melderegisterauskünfte an nicht öffentliche Stellen nach §§ 44 ff. BMG (insbesondere Einfache Melderegisterauskunft nach § 44 BMG, Erweiterte Melderegisterauskunft nach § 45 BMG, Gruppenauskunft nach § 46 BMG, Melderegisterauskünfte in besonderen Fällen nach § 50 BMG und Auskunftssperren nach § 51 BMG) erörtert.

Dabei zeigte sich, dass die Berücksichtigung sowohl der Anforderungen des Bundesmeldegesetzes als auch des Datenschutzes in der Praxis mitunter schwierige Fragen aufwirft. Beispielhaft sei der Umfang der Dokumentationspflichten der Meldebehörde bei den verschiedenen Arten der Melderegisterauskunft und die damit zusammenhängende Reichweite des Auskunftsanspruchs nach Art. 15 DS-GVO der betroffenen Personen sowie die Auslegung der Vorschrift zu Melderegisterauskünften über Alters- und Ehejubiläen gemäß § 50 Abs. 2 BMG (etwa der Begriff des „Mandatsträgers“ und die Befugnis zur Veröffentlichung) genannt.

§ 50 BMG

(2) Verlangen Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde Auskunft erteilen über

1. *Familienname,*
2. *Vornamen,*
3. *Doktorgrad,*
4. *Anschrift sowie*
5. *Datum und Art des Jubiläums.*

Altersjubiläen im Sinne des Satzes 1 sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 50. und jedes folgende Ehejubiläum.

Diese und weitere Fragen aus dem Melderecht, insbesondere auch die Datenübermittlungen zwischen öffentlichen Stellen gemäß §§ 33 ff. BMG (wie etwa die Datenweitergabe innerhalb der Kommune gemäß § 37 BMG sowie Auslegungsfragen hinsichtlich der Protokollierungspflicht), werden mich weiterhin intensiv beschäftigen. Neben den bereits auf meiner Webseite abrufbaren Informationen zu Rechten der Betroffenen bei Meldebehörden[40] sowie der Handreichung –Datenschutz bei Wahl- und Abstimmungswerbung[41] – beabsichtige ich daher, zukünftig weitere Informationen für Kommunen zu Fragestellungen an der Schnittstelle zwischen Datenschutz- und Melderecht zu veröffentlichen.

Veröffentlichung im kommunalen Gremieninformationssystem

Die datenschutzrechtlichen Anforderungen bei der Veröffentlichung von Sitzungsprotokollen der Gemeindevertretung im Internet waren bereits Gegenstand in meinem 50. Tätigkeitsbericht, Kap. 8.2. Im Berichtszeitraum wurde mir ein weiterer diesbezüglicher Vorgang mitgeteilt. Diesem lag folgender Sachverhalt zugrunde:

Der Beschwerdeführer bekundete im Herbst 2019 gegenüber der Gemeinde sein Interesse an einem Grundstück. An allen weiteren Sitzungen des Gemeindevorstands wirkte der Beschwerdeführer, der zu diesem Zeitpunkt ehrenamtlicher Beigeordneter war, in dieser Angelegenheit gemäß § 25 HGO weder beratend noch entscheidend mit.

§ 25 HGO

(1) Niemand darf in haupt- oder ehrenamtlicher Tätigkeit in einer Angelegenheit beratend oder entscheidend mitwirken, wenn er

1. *durch die Entscheidung in der Angelegenheit einen unmittelbaren Vorteil oder Nachteil erlangen kann,*
2. *Angehöriger einer Person ist, die zu dem in Nr. 1 bezeichneten Personenkreis gehört,*

40 HBDI, https://datenschutz.hessen.de/datenschutz/kommunen/rechte-der-betroffenen-bei-meldebehoerden.

41 HBDI, https://datenschutz.hessen.de/datenschutz/kommunen/datenschutz-bei-wahl-und-abstimmungswerbung.

3. eine natürliche oder juristische Person nach Nr. 1 kraft Gesetzes oder in der betreffenden Angelegenheit kraft Vollmacht vertritt (Einzel- oder Gesamtvertretung),

4. bei einer natürlichen oder juristischen Person oder Vereinigung nach Nr. 1 gegen Entgelt beschäftigt ist, wenn Tatsachen die Annahme rechtfertigen, dass dadurch Befangenheit gegeben ist,

5. bei einer juristischen Person oder Vereinigung nach Nr. 1 als Mitglied des Vorstands, des Aufsichtsrats oder eines gleichartigen Organs tätig ist, es sei denn, dass er diesem Organ als Vertreter oder auf Vorschlag der Gemeinde angehört,

6. in anderer als öffentlicher Eigenschaft in der Angelegenheit tätig geworden ist.

Satz 1 gilt nicht, wenn jemand an der Entscheidung lediglich als Angehöriger einer Berufs- oder Bevölkerungsgruppe beteiligt ist, deren gemeinsame Interessen durch die Angelegenheit berührt werden.

Nach der Entscheidung des Gemeindevorstands, das Grundstück zu veräußern, unterschrieben seitens der Gemeinde die Bürgermeisterin und der damalige erste Beigeordnete die Genehmigungserklärung zum notariellen Grundstückskaufvertrag. Im Anschluss wurde die entsprechende Umschreibung im Grundbuch sowie die Kaufpreiszahlung veranlasst. Der Besitzübergang erfolgte im Februar 2020. Ein Genehmigungsbeschluss der Gemeindevertretung lag nicht vor. Vielmehr wurde seitens der Gemeinde erst ein knappes Jahr nach dem Grundstückskauf festgestellt, dass ein solcher Beschluss gemäß § 77 Abs. 2 HGO nicht eingeholt worden war.

§ 77 HGO

(2) Verträge der Gemeinde mit Mitgliedern des Gemeindevorstands und mit Gemeindevertretern bedürfen der Genehmigung der Gemeindevertretung, es sei denn, dass es sich um Verträge nach feststehendem Tarif oder um Geschäfte der laufenden Verwaltung handelt, die für die Gemeinde unerheblich sind.

Die Gemeindevertretung beschloss im Februar 2021, den Abschluss des Grundstückkaufvertrages nicht zu genehmigen. Die Parteien waren sich hinsichtlich der Wirksamkeit des Vertrages und des Eigentumserwerbs durch den Beschwerdeführer sowie der Erstattung der dem Beschwerdeführer entstandenen Kosten uneinig. Zur Erledigung der streitigen Rechtsfragen schlossen die Parteien eine Vergleichsvereinbarung. Die Gemeindevertretung erteilte zu deren Abschluss im November 2022 die Zustimmung.

Die Thematik wurde in mehreren öffentlichen Sitzungen der Gemeindevertretung behandelt. Die Sitzungsunterlagen wurden in dem Gremieninformationssystem der Gemeinde auf der kommunalen Webseite veröffentlicht. In

dem Gremieninformationssystem war überdies zeitweise der Entwurf der zu schließenden Vergleichsvereinbarung veröffentlicht.

Den Vorgang bewerte ich datenschutzrechtlich wie folgt:

Die Offenlegung der personenbezogenen Daten des Beschwerdeführers in mehreren öffentlichen Sitzungen der Gemeindevertretung sowie die Veröffentlichung der Sitzungsunterlagen in dem Gremieninformationssystem der Gemeinde war datenschutzrechtlich vertretbar. Die seitens der Gemeinde getroffene Abwägungsentscheidung war nicht ermessensfehlerhaft. Zwar hat die Allgemeinheit nach § 61 HGO grundsätzlich keinen Anspruch auf Einsicht in die Niederschriften,

§ 61 HGO

(1) Über den wesentlichen Inhalt der Verhandlungen der Gemeindevertretung ist eine Niederschrift zu fertigen. Aus der Niederschrift muss ersichtlich sein, wer in der Sitzung anwesend war, welche Gegenstände verhandelt, welche Beschlüsse gefasst und welche Wahlen vollzogen worden sind. Die Abstimmungs- und Wahlergebnisse sind festzuhalten. Jedes Mitglied der Gemeindevertretung kann verlangen, dass seine Abstimmung in der Niederschrift festgehalten wird.

(2) Die Niederschrift ist von dem Vorsitzenden und dem Schriftführer zu unterzeichnen. Zu Schriftführern können Gemeindevertreter oder Gemeindebedienstete – und zwar auch solche, die ihren Wohnsitz nicht in der Gemeinde haben – oder Bürger gewählt werden.

(3) Eine Kopie der Niederschrift ist innerhalb eines in der Geschäftsordnung festzulegenden Zeitraumes an alle Gemeindevertreter schriftlich oder elektronisch zu übersenden. Über Einwendungen gegen die Niederschrift entscheidet die Gemeindevertretung.

es spricht jedoch nichts dagegen, dass Niederschriften, die sich auf den öffentlichen Teil einer Sitzung beziehen, auch anderen Personen zugänglich gemacht werden. Insbesondere in kleinen Kommunen bedarf es einer nachvollziehbaren und interessengerechten Abwägung zwischen kommunalpolitischer Transparenz, dem Informationsbedürfnis der Bürgerinnen und Bürger, wie es dem Öffentlichkeitsgrundsatz des § 52 HGO entspricht, sowie dem individuellen Recht auf informationelle Selbstbestimmung. Dies gilt insbesondere im Falle einer Veröffentlichung im Internet.

§ 52 HGO

(1) Die Gemeindevertretung fasst ihre Beschlüsse in öffentlichen Sitzungen. Sie kann für einzelne Angelegenheiten die Öffentlichkeit ausschließen. Anträge auf Ausschluss der Öffentlichkeit werden in nichtöffentlicher Sitzung begründet, beraten und entschieden; die Entscheidung kann in öffentlicher Sitzung getroffen werden, wenn keine besondere

Begründung oder Beratung erforderlich ist. Der Vorsitzende kann im Einvernehmen mit dem Bürgermeister Gemeindebedienstete zu den nicht öffentlichen Sitzungen beiziehen.

(2) Beschlüsse, welche in nichtöffentlicher Sitzung gefasst worden sind, sollen, soweit dies angängig ist, nach Wiederherstellung der Öffentlichkeit bekannt gegeben werden.

(3) Die Hauptsatzung kann bestimmen, dass in öffentlichen Sitzungen Film- und Tonaufnahmen durch die Medien mit dem Ziel der Veröffentlichung zulässig sind.

In diesem Fall ist zu berücksichtigen, dass der Beschwerdeführer als ehemaliger Beigeordneter gemäß § 65 Abs. 1 HGO Teil des Gemeindevorstands war. Überdies sind die besonderen Umstände des Grundstückkaufvertrages mit einem Mandatsträger zu berücksichtigen. Die Regelung des § 77 Abs. 2 HGO spricht für ein erhöhtes Transparenzbedürfnis. Danach bedürfen Verträge der Gemeinde mit Mitgliedern des Gemeindevorstands und mit Gemeindevertretern grundsätzlich der Genehmigung der Gemeindevertretung. Es ist zu vermeiden, dass Mandatsträger bei Verträgen der Gemeinde gegenüber Mitbewerbern bevorzugt werden. Es handelte sich gerade nicht um einen Grundstückskaufvertrag mit einer gewöhnlichen Privatperson.

Die temporäre Veröffentlichung des Entwurfs der zu schließenden Vergleichsvereinbarung in dem Gremieninformationssystem war dagegen datenschutzrechtlich unzulässig. Insofern überwiegt das individuelle Recht des Beschwerdeführers auf informationelle Selbstbestimmung. Ich habe der Gemeinde daher einen entsprechenden Hinweis erteilt und diese aufgefordert, die beteiligten Personen für die Belange des Datenschutzes zu sensibilisieren und zu schulen.

Kommunale Bürgerbegehren

Mich erreichen immer wieder Anfragen und mitunter auch Beschwerden, die Bürgerbegehren im Sinne des § 8b HGO in den hessischen Kommunen betreffen. Diese erfassen ein inhaltlich breites Themenspektrum (beispielhaft seien die kommunale Stromversorgung, die Umbenennung einer Straße oder auch die Errichtung oder der Erhalt eines Gemeindezentrums oder eines Stadions genannt). Sowohl die Unterschriftensammlung für ein Bürgerbegehren und die weitere Verarbeitung der personenbezogenen Daten, in der Regel durch Privatpersonen, als auch die Datenverarbeitung nach Einreichung der Unterschriftenlisten bei der Gemeinde werfen teils schwierige datenschutzrechtliche Fragestellungen auf. Mit der Handreichung „Datenschutz bei Bürgerbegehren“, die mitsamt Mustern für Einwilligungserklärung und

Datenschutzinformationen auf meiner Webseite einsehbar ist,[42] möchte ich sowohl die sammelnden Personen als auch die Gemeinden bei der Umsetzung der datenschutzrechtlichen Anforderungen unterstützen.[43]

Aufsichtsmaßnahmen gegenüber Kommunen und weiteren öffentlichen Stellen

Im Vergleich zu den umfangreichen aufsichtsrechtlichen Befugnissen gegenüber nicht öffentlichen Stellen sind meine Kompetenzen im kommunalen (und generell im öffentlichen) Bereich deutlich eingeschränkt. Wenngleich sich öffentliche Stellen ganz überwiegend an die Maßgaben des Datenschutzes halten, macht sich die eingeschränkte Prüfungsbefugnis in Einzelfällen bemerkbar (s. etwa 51. Tätigkeitsbericht, Kap. 7.6). Nachfolgend sollen die geltende Rechtslage sowie europarechtliche Bedenken erläutert werden.

Meiner Behörde stehen gegenüber öffentlichen Stellen die Befugnisse gemäß Art. 58 DS-GVO und § 14 HDSIG zur Verfügung. Diese beinhalten Untersuchungs- (etwa die Anweisung der Bereitstellung von Informationen und Hinweise), Abhilfe- (etwa Verwarnungen und Anweisungen z. B. zur Änderung von Verarbeitungsvorgängen) und Genehmigungsbefugnisse (etwa Beratungen z. B. gemäß dem Verfahren der vorherigen Konsultation nach Art. 36 DS-GVO).

§ 14 HDSIG

(1) Die oder der Hessische Datenschutzbeauftragte nimmt im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 die Befugnisse nach Art. 58 der Verordnung (EU) Nr. 2016/679 wahr. Kommt die oder der Hessische Datenschutzbeauftragte zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie oder er dies der öffentlichen Stelle mit und gibt dieser vor der Ausübung der Befugnisse des Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Hessischen Datenschutzbeauftragten getroffen

42 HBDI, https://datenschutz.hessen.de/datenschutz/kommunen/datenschutz-bei-buergerbegehren.

43 Weiterführende Informationen zu der Thematik können zudem dem Beitrag von Rapp, Datenschutz bei Bürgerbegehren, Kommunaljurist (KommJur) 2023, S. 361 ff., sowie S. 401 ff., entnommen werden.

worden sind. Die Ausübung der Befugnisse nach Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 teilt die oder der Hessische Datenschutzbeauftragte der jeweils zuständigen Rechts- und Fachaufsichtsbehörde mit.

Die Ausübung der Befugnisse nach Art. 58 Abs. 2 Buchst. b–g und i–j DS-GVO teile ich gemäß § 14 Abs. 1 Satz 5 HDSIG der jeweils zuständigen Rechts- und Fachaufsichtsbehörde mit. Diese richtet sich in der Regel nach § 136 HGO und ist daher zumeist der Landrat als Behörde der Landesverwaltung.

§ 136 HGO

(1) Aufsichtsbehörde der Landeshauptstadt Wiesbaden und der Stadt Frankfurt am Main ist der Minister des Innern.

(2) Aufsichtsbehörde der sonstigen kreisfreien Städte und Sonderstatus-Städte ist der Regierungspräsident, obere Aufsichtsbehörde der Minister des Innern. Der Minister des Innern kann seine Befugnisse als obere Aufsichtsbehörde auf nachgeordnete Behörden übertragen.

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

(4) Oberste Aufsichtsbehörde ist der Minister des Innern.

Sofern die öffentliche Stelle eine verbindliche Entscheidung meiner Behörde nicht beachtet und nicht innerhalb eines Monats nach Bekanntgabe gerichtlich gegen diese vorgeht, kann ich die gerichtliche Feststellung der Rechtmäßigkeit der getroffenen verbindlichen Entscheidung beantragen, § 19 Abs. 5 Satz 2 HDSIG.

§ 19 HDSIG

(5) Behörden und sonstige öffentliche Stellen des Landes können unbeschadet anderer Rechtsbehelfe gerichtlich gegen sie betreffende verbindliche Entscheidungen der oder des Hessischen Datenschutzbeauftragten vorgehen. Wenn die Behörde oder öffentliche Stelle eine verbindliche Entscheidung der oder des Hessischen Datenschutzbeauftragten nicht beachtet und nicht innerhalb eines Monats nach Bekanntgabe gerichtlich gegen diese vorgeht, kann die oder der Hessische Datenschutzbeauftragte die gerichtliche Feststellung der Rechtmäßigkeit der getroffenen verbindlichen Entscheidung beantragen.

Die Vollstreckung der aufsichtsrechtlichen Maßnahmen ist nach § 73 HVwVG jedoch nicht zulässig.

§ 73 HVwVG

Gegen Behörden und juristische Personen des öffentlichen Rechts kann nur vollstreckt werden, soweit dies aufgrund von Rechtsvorschriften ausdrücklich zugelassen ist.

Nach § 36 Abs. 2 HDSIG werden überdies wegen eines Verstoßes gegen Art. 83 Abs. 4–6 DS-GVO gegen Behörden und sonstige öffentliche Stellen nach § 2 Abs. 1 Satz 1 HDSIG keine Geldbußen verhängt. Damit sind Geldbußen im öffentlichen Bereich ganz überwiegend ausgeschlossen.

§ 36 HDSIG

(2) Wegen eines Verstoßes gegen Art. 83 Abs. 4 bis 6 der Verordnung (EU) Nr. 2016/679 werden gegen Behörden und sonstige öffentliche Stellen nach § 2 Abs. 1 Satz 1 keine Geldbußen verhängt.

§ 2 HDSIG

(1) Öffentliche Stellen sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Landes, der Gemeinden und Landkreise oder sonstige deren Aufsicht unterstehende juristische Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Nimmt eine nicht öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

Auch wenn den datenschutzrechtlichen Aufsichtsbehörden gegenüber öffentlichen Stellen nach geltender Rechtslage mehrere Befugnisse zur Verfügung stehen, werden insbesondere aufgrund der fehlenden Möglichkeit zur Vollstreckung Zweifel an der Europarechtskonformität der Vorschriften geäußert.[44]

Kommunale Datenschutzbeauftragte

Die Art. 37 ff. DS-GVO und §§ 5 ff. HDSIG regeln detaillierte Anforderungen an die Benennung, die Stellung sowie die Aufgaben der Datenschutzbeauftragten von öffentlichen Stellen. Mit dem umfassend aktualisierten Arbeitspapier „Behördliche und betriebliche Datenschutzbeauftragte“ biete ich öffentlichen

44 S. hierzu Friedrichsen/Rapp, Aufsichtsrechtliche Maßnahmen gegenüber öffentlichen Stellen, ZD 2023, 535.

Stellen (sowie Unternehmen), Datenschutzbeauftragten und Interessierten eine Übersicht der aktuellen Rechtslage.[45]

5.4
Interessenkonflikte bei Datenschutzbeauftragten in öffentlichen Stellen

Datenschutzbeauftragte erfüllen wichtige Aufgaben bei der Kontrolle und Einhaltung des Datenschutzes in öffentlichen Stellen. Neben ihrer Tätigkeit als Datenschutzbeauftragte nehmen sie oftmals weitere Aufgaben wahr. Diese Aufgabenhäufung ist zulässig, sofern sie nicht zu einem Interessenkonflikt führt.

Behörden und öffentliche Stellen müssen im Geltungsbereich der DS-GVO nach Art. 37 Abs. 1 Buchst. a DS-GVO einen Datenschutzbeauftragten benennen. In Hessen sind sie überdies gemäß § 5 Abs. 1 HDSIG zur Benennung eines Vertreters verpflichtet.

Grundsätze zur Konfliktregelung

Eine Regelung zu Interessenkonflikten enthält § 7 Abs. 2 HDSIG:

> *§ 7 Abs. 2 HDSIG*
> *Die oder der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.*

Danach kann der Datenschutzbeauftragte andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen. Eine weitere gesetzliche Präzisierung erfährt diese Vorschrift nicht. Sie steht in einem engen Zusammenhang mit dem Erfordernis einer unabhängigen Tätigkeit des Datenschutzbeauftragten gemäß § 6 Abs. 3 Satz 1 HDSIG sowie nach § 5 Abs. 3 HDSIG der Fähigkeit zur Erfüllung seiner Aufgaben nach § 7 HDSIG.

Interessenkonflikte können vor allem bei der Ausübung von Tätigkeiten auftreten, die wesentliche Verpflichtungen der öffentlichen Stelle bei der

45 HBDI, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-10/behoerdliche_und_betriebliche_datenschutzbeauftragte_231009_1.pdf.

Umsetzung der Datenschutzvorschriften betreffen. In diesen Fällen müsste sich der Datenschutzbeauftragte selbst kontrollieren.[46] Datenschutzbeauftragte dürfen neben diesem Amt keine Position innehaben, bei der sie die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegen.[47]

Ein Interessenkonflikt kann kaum für bestimmte Aufgaben oder Positionen pauschal angenommen werden. Es ist eine Einzelfallbetrachtung vorzunehmen, ob und inwiefern Entscheidungsbefugnisse hinsichtlich Zweck und Mittel der Verarbeitung personenbezogener Daten bestehen. Der EuGH hat dazu wie folgt ausgeführt: Art. 38 Abs. 6 DS-GVO ist dahin auszulegen, „dass ein ‚Interessenkonflikt' im Sinne dieser Bestimmung bestehen kann, wenn einem Datenschutzbeauftragten andere Aufgaben oder Pflichten übertragen werden, die ihn dazu veranlassen würden, die Zwecke und Mittel der Verarbeitung personenbezogener Daten bei dem Verantwortlichen oder seinem Auftragsverarbeiter festzulegen. Ob dies der Fall ist, muss das nationale Gericht im Einzelfall auf der Grundlage einer Würdigung aller relevanten Umstände, insbesondere der Organisationsstruktur des Verantwortlichen oder seines Auftragsverarbeiters, und im Licht aller anwendbaren Rechtsvorschriften, einschließlich etwaiger interner Vorschriften des Verantwortlichen oder des Auftragsverarbeiters, feststellen.[48]

Einzelfälle

Ein Interessenkonflikt besteht in der Regel bei der Leitung einer Behörde. Diese Personen sind originär für die Rechtmäßigkeit der Datenverarbeitung in der öffentlichen Stelle verantwortlich und können sich nicht wirksam selbst kontrollieren. Ferner sind Beschäftigte für die Position des Datenschutzbeauftragten nicht geeignet, an welche die Behördenleitung Aufgaben delegiert, soweit diese Beschäftigten Datenverarbeitungsprozesse bestimmen oder wesentlich beeinflussen können.

Ein Interessenkonflikt ist in der Regel bei herausgehobenen Leitungstätigkeiten anzunehmen.[49] Dies betrifft die Leitung der Personalabteilung ebenso wie die Leitung der IT-Abteilung. Auch ist die Leitung der Rechtsabteilung mit der Tätigkeit als Datenschutzbeauftragter in der Regel nicht vereinbar. Diese

46 Wilmer, in: Roßnagel, HDSIG, 2021, § 7 Rn. 25.

47 Gola ZD 2019, 383 (388).

48 EuGH Urt. v. 9.2.2023 – C-453/21 (X-FAB Dresden GmbH & Co. KG/FC), NZA 2023, 221 (223).

49 Gola ZD 2019, 383 (388); Roßnagel, HDSIG/Wilmer, in: 2021, § 7 Rn. 26; HBDI, Behördliche und betriebliche Datenschutzbeauftragte, 9.10.2023, S. 17, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-10/behoerdliche_und_betriebliche_datenschutzbeauftragte_231009_1.pdf.

ist oftmals in die behördeninternen Prozesse derart eingebunden, dass sie nicht mehr über die notwendige Unabhängigkeit hinsichtlich der Bewertung einzelner Datenverarbeitungsprozesse verfügt.

Tätigkeiten im Beauftragtenwesen gehen häufig mit einem Interessenkonflikt einher. IT-Sicherheitsbeauftragte sind aufgrund des Interesses an umfassenden Sammlungen personenbezogener Daten zwecks Entdeckung von Missbrauch in der Regel als Datenschutzbeauftragte nicht geeignet. Vergleichbares gilt für Digitalisierungsbeauftragte. Probleme können sich auch bei Beauftragten im Bereich der Compliance, Antikorruption, Geldwäschebekämpfung, Geheimschutz und Hinweisgeberschutz ergeben.

Der Vorsitzende des Personalrates ist als Datenschutzbeauftragter nicht geeignet. Nach Vorlage an den EuGH[50] hat das BAG[51] entschieden, dass der Betriebsratsvorsitz einer Wahrnehmung der Aufgaben des Datenschutzbeauftragten typischerweise entgegensteht. Diese Maßgaben sind auf den Personalrat übertragbar. Die Frage der Vereinbarkeit der Tätigkeit einzelner Mitglieder des Betriebsrates war dagegen nicht Gegenstand des Vorlageverfahrens. Nicht vereinbar sind zudem in der Regel Mitglieder der Schwerbehindertenvertretung sowie Frauen- und Gleichstellungsbeauftragte. Die gleichzeitige Tätigkeit bei der Beschwerdestelle nach § 13 des Allgemeinen Gleichbehandlungsgesetzes (AGG) ist dagegen zulässig.

In den Gemeinden, Städten und Landkreisen sind weitere Ämter und Funktionen zu berücksichtigen. Der (Ober-)Bürgermeister und die Beigeordneten als Mitglieder des Gemeindevorstands/Magistrats nach § 65 HGO können nicht Datenschutzbeauftragte sein. Gemäß § 71 Abs. 1 HGO vertritt der Gemeindevorstand/Magistrat die Gemeinde/Stadt. Überdies werden nach § 70 Abs. 2 HGO die laufenden Verwaltungsangelegenheiten grundsätzlich von dem Bürgermeister und den zuständigen Beigeordneten selbstständig erledigt. Gleiches gilt für den Landrat und die Kreisbeigeordneten als Mitglieder des Kreisausschusses nach § 36 HKO auf Ebene der Landkreise. Ebenfalls unvereinbar mit der Tätigkeit als Datenschutzbeauftragter ist die Leitung (nachgeordneter) kommunaler Ämter, sofern damit Entscheidungsbefugnisse hinsichtlich Zweck und Mittel der Verarbeitung personenbezogener Daten bestehen. Dies betrifft z. B. die Leitung der Personalverwaltung sowie der Hauptverwaltung (sofern zum Aufgabenkreis auch die Personalverwaltung gehört).

---

50 EuGH Urt. v. 9.2.2023 – C-453/21 (X-FAB Dresden GmbH & Co. KG/FC), NZA 2023, 221 ff.

51 BAG Urt. v. 6.6.2023 – 9 AZR 383/19, NJW 2023, 3531 ff.

Interessenkonflikte können auch bei externen Datenschutzbeauftragten auftreten. Sofern diese eine öffentliche Stelle nicht nur hinsichtlich des Datenschutzes, sondern auch anderweitig beraten, ist im konkreten Einzelfall im Rahmen der anderweitigen Beratung eine grundsätzliche Unabhängigkeit zu gewährleisten. Besondere Ausnahmefälle, in denen eine Benennung trotz Interessenkonflikts erfolgen kann (etwa sofern der Bürgermeister einer kleinen Gemeinde nachweisen könnte, dass er keinen anderen Beschäftigten zum Datenschutzbeauftragten benennen könne), erscheinen angesichts der Möglichkeit der Beauftragung von externen Datenschutzbeauftragten kaum denkbar. Solche Konstellationen können allenfalls übergangsweise bis zur Benennung eines externen Dienstleisters auftreten.

Rechtsfolgen und aufsichtsrechtliche Maßnahmen

Im Falle eines bestehenden Interessenkonflikts hat der Datenschutzbeauftragte entweder die andere Tätigkeit einzustellen oder es muss eine Abberufung als Datenschutzbeauftragter erfolgen.

Im Rahmen meiner Befugnisse gegenüber öffentlichen Stellen kann ich diese auf einen Verstoß hinweisen, kann sie warnen und verwarnen und sie anweisen, Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit den datenschutzrechtlichen Anforderungen zu bringen. Davon dürfte – trotz des unklaren Wortlautes – auch die Befugnis zur Abberufung des Datenschutzbeauftragten umfasst sein.[52]

Hinweise für die Praxis

Datenschutzbeauftragte übernehmen in der Praxis (insbesondere in kleineren Behörden und Kommunen) oftmals weitere Tätigkeiten. Naheliegend ist die Benennung einer intern bereits vertrauten Führungskraft zusätzlich als Datenschutzbeauftragter. Wenngleich eine ausnahmslose und jederzeitige Abwesenheit von jedwedem Interessenkonflikt – bereits aufgrund der diversen gesetzlich vorgegebenen Beauftragten (insbesondere bei personell ohnehin unzureichend ausgestatteten Stellen) – kaum möglich erscheint, müssen öffentliche Stellen die genannten Maßgaben doch weitestgehend berücksichtigten.

---

52 S. Bergt/Herbort, in: Kühling/Buchner, DS-GVO BDSG/ 4. Aufl. 2024, Art. 37 DS-GVO Rn. 49. Nach Körffer, in: Paal/Pauly, DS-GVO BDSG, 3. Aufl. 2021, Art. 58 DS-GVO Rn. 20, sind Anweisungen zur Benennung eines Datenschutzbeauftragten nach Art. 37 DS-GVO erfasst. AA dagegen VG Köln, ZD 2022, 127 (128), nach dem die (Ab-)Berufung eines Datenschutzbeauftragten keinen Verarbeitungsvorgang i. S. d. Art. 58 Abs. 2 Buchst. d DS-GVO darstellt.

Es empfiehlt sich mitunter, „unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe“ (etwa im Rahmen der interkommunalen Zusammenarbeit) für mehrere öffentliche Stellen einen gemeinsamen Datenschutzbeauftragten gemäß § 5 Abs. 2 HDSIG zu benennen. Aus einer Zuständigkeit für mehrere öffentliche Stellen ergeben sich in der Regel keine Interessenkonflikte, sondern vielmehr Synergien. Auch kann ein externer Dienstleister beauftragt werden.

Zwecks Vermeidung von Interessenkonflikten sind (insbesondere bei größeren Behörden und Kommunen) einige Maßnahmen zu ergreifen: Es sind die Positionen zu benennen, die mit der Funktion eines Datenschutzbeauftragen nicht vereinbar sind, interne Richtlinien aufzustellen, eine allgemeine Erläuterung möglicher Interessenkonflikte vorzunehmen, zu erklären, dass sich der Datenschutzbeauftragte hinsichtlich seiner Funktion in keinem Interessenkonflikt befindet, und damit das Bewusstsein für diese Maßgabe zu schärfen sowie in die internen Richtlinien Sicherungsvorkehrungen aufzunehmen und zu gewährleisten, dass die Stellenausschreibung für die Position eines Datenschutzbeauftragten (oder der Dienstleistungsvertrag) zur Vermeidung von Interessenkonflikten entsprechend formuliert wird.

5.5
Melderegisterauskünfte bei Wahlen und Abstimmungen

Auf den Ebenen der Europäischen Union, des Bundes, der Länder und der Kommunen finden immer wieder Wahlen statt. Im Vorfeld bemühen sich die Parteien um die Aufmerksamkeit der Wählerinnen und Wähler. Soweit für ihre Wahlwerbung keine personenbezogenen Daten der Wählerinnen und Wähler verarbeitet werden, ist sie aus datenschutzrechtlicher Perspektive unproblematisch. Sofern die Parteien den Wahlberechtigten dagegen persönlich adressierte Werbeschreiben zukommen lassen, erfolgt die Verarbeitung personenbezogener Daten, weshalb die Bestimmungen des Datenschutzrechts beachtlich sind.

Insbesondere im Zuge der hessischen Landtagswahl am 8. Oktober 2023 hat das Thema Wahlwerbung einen besonderen Stellenwert eingenommen. Mich erreichten viele diesbezügliche Anfragen und Beschwerden. Bürgerinnen und Bürger bemängelten häufig, dass eine unzulässige Verarbeitung ihrer personenbezogenen Daten stattgefunden habe. Sie wollten zudem erfahren, ob und welche Möglichkeiten es gibt, um sich gegen unerwünschte Wahlwerbung zu wenden.

Wahlwerbung bezieht sich auf die verschiedenen Methoden, mit denen politische Parteien versuchen, Wählerinnen und Wähler von ihren Standpunkten, Zielen und Versprechen zu überzeugen. Ziel ist es, die Botschaft und die Vor-

haben der Partei zu vermitteln, um Unterstützung zu gewinnen. Die folgenden Maßgaben gelten ebenfalls für Abstimmungswerbung (Sachentscheidungen in Abgrenzung zu Wahlen als Personalentscheidungen).

Grundlagen der Wahlwerbung

Die Grundlagen für Wahlwerbung durch Parteien lassen sich aus dem Grundgesetz (GG) ableiten. Die grundsätzliche Zulässigkeit folgt insbesondere aus der Meinungs- und Informationsfreiheit (Art. 5 Abs. 1 GG) und aus dem Parteienprivileg (Art. 21 GG; s. zudem das Parteiengesetz). Die Wahlgrundsätze des Art. 38 GG in Verbindung mit Art. 28 GG für freie Wahlen erfordern insbesondere, dass Wählerinnen und Wähler über die von den Parteien vertretenen Positionen entsprechend informiert sind.

Art. 5 GG

(1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.

(2) Diese Rechte finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre.

Art. 21 GG

(1) Die Parteien wirken bei der politischen Willensbildung des Volkes mit. Ihre Gründung ist frei. Ihre innere Ordnung muss demokratischen Grundsätzen entsprechen. Sie müssen über die Herkunft und Verwendung ihrer Mittel sowie über ihr Vermögen öffentlich Rechenschaft geben.

(…)

(5) Das Nähere regeln Bundesgesetze.

Art. 38 GG

(1) Die Abgeordneten des Deutschen Bundestages werden in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl gewählt. Sie sind Vertreter des ganzen Volkes, an Aufträge und Weisungen nicht gebunden und nur ihrem Gewissen unterworfen.

(…)

Art. 28 GG

(1) Die verfassungsmäßige Ordnung in den Ländern muss den Grundsätzen des republikanischen, demokratischen und sozialen Rechtsstaates im Sinne dieses Grundgesetzes entsprechen. In den Ländern, Kreisen und Gemeinden muss das Volk eine Vertretung haben, die aus allgemeinen, unmittelbaren, freien, gleichen und geheimen Wahlen hervorgegangen ist. Bei Wahlen in Kreisen und Gemeinden sind auch Personen, die die Staatsangehörigkeit eines Mitgliedstaates der Europäischen Gemeinschaft besitzen, nach Maßgabe von Recht der Europäischen Gemeinschaft wahlberechtigt und wählbar. In Gemeinden kann an die Stelle einer gewählten Körperschaft die Gemeindeversammlung treten.

(…)

Um Informationen zur Entscheidungsfindung bei den Bürgerinnen und Bürgern zu verteilen, werden unterschiedliche Kanäle zur Verbreitung eingesetzt. Relevant ist auch im digitalen Zeitalter weiterhin die Wahlwerbung per Briefpost.

Arten der Wahlwerbung

Es ist zwischen der personalisierten und der nicht personalisierten Bereitstellung von Wahlwerbung zu unterscheiden.

Nicht personalisierte Werbemaßnahmen (Flyer, Broschüren, Wahlplakate), die nicht direkt an eine bestimmte Person adressiert sind und auch keine personenbezogenen Daten enthalten, gelten aus datenschutzrechtlicher Sicht als unproblematisch. Hierbei findet keine Verarbeitung von personenbezogenen Daten statt. Auch werden im Rahmen des Haustürwahlkampfes grundsätzlich keine personenbezogenen Daten verarbeitet.

Demgegenüber steht die personalisierte Wahlwerbung in Form von persönlich adressierten Anschreiben. Hierbei sind insbesondere die Vorschriften der DS-GVO sowie des Bundesmeldegesetzes (BMG) zu berücksichtigen.

Die Zulässigkeit der Datenübermittlung

Postalische Wahlwerbung ist (neben der Möglichkeit, personenbezogene Daten bei Adresshändlern für Werbezwecke zu erhalten) in Folge von Auskünften aus dem Melderegister zulässig. Die rechtliche Grundlage ergibt sich aus Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO in Verbindung mit § 50 Abs. 1 BMG. Wahlwerbung ist eine Aufgabe, die im öffentlichen Interesse liegt, da Wahlwerbung zur politischen Willensbildung und damit zur Funktionsfähigkeit der Demokratie beiträgt.

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;

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(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.

(…)

§ 50 BMG

(1) Die Meldebehörde darf Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Wahlen und Abstimmungen auf staatlicher und kommunaler Ebene in den sechs der Wahl oder Abstimmung vorangehenden Monaten Auskunft aus dem Melderegister über die in § 44 Absatz 1 Satz 1 bezeichneten Daten von Gruppen von Wahlberechtigten erteilen, soweit für deren Zusammensetzung das Lebensalter bestimmend ist. Die Geburtsdaten der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. Die Person oder Stelle, der die Daten übermittelt werden, darf diese nur für die Werbung bei einer Wahl oder Abstimmung verwenden und hat sie spätestens einen Monat nach der Wahl oder Abstimmung zu löschen oder zu vernichten.

(…)

(5) Die betroffene Person hat das Recht, der Übermittlung ihrer Daten nach den Absätzen 1 bis 3 zu widersprechen; hierauf ist bei der Anmeldung nach § 17 Absatz 1 sowie einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen. § 36 Absatz 2 Satz 2 gilt entsprechend.

Danach dürfen die Meldebehörden Parteien (sowie Wählergruppen und anderen Trägern von Wahlvorschlägen) im Zusammenhang mit Wahlen auf staatlicher und kommunaler Ebene in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister insbesondere über Familiennamen, Vornamen und derzeitige Anschriften von Gruppen von Wahlberechtigten erteilen. Möglich ist etwa die Auskunftserteilung über die Gruppe der 18- bis 25-Jährigen (ohne die Geburtsdaten selbst mitzuteilen). Die Daten dürfen nur für die Werbung bei einer Wahl verwendet werden und müssen spätestens

einen Monat nach der Wahl gelöscht oder vernichtet werden. Darauf sollte die Meldebehörde die Partei ausdrücklich hinweisen.

Sonstige Formen der Wahlwerbung (insbesondere Online-Wahlwerbung)

Neben postalischer Wahlwerbung gibt es weitere Mittel für Parteien, um auf ihre Anliegen aufmerksam zu machen. Besonders im Zeitalter der Digitalisierung spielt Online-Wahlwerbung eine immer größere Rolle. Social Media-Plattformen wie Facebook, Twitter und Instagram bieten Möglichkeiten, direkt mit den Wählerinnen und Wählern zu interagieren und gezielt bestimmte Bevölkerungsgruppen anzusprechen. Auch dabei müssen die Anforderungen der DS-GVO vollumfänglich berücksichtigt werden (insbesondere hinsichtlich der gemeinsamen Verantwortlichkeit gemäß Art. 26 DS-GVO sowie der Drittstaatenübermittlung nach Art. 44 ff. DS-GVO), was bei vielen Diensten wie zum Beispiel Facebook derzeit schwierig bis unmöglich erscheint.[53] Wahlwerbung per Telefon oder E-Mail ist in der Regel unzulässig, sofern keine ausdrückliche Einwilligung hierfür vorliegt.

Rechte der Betroffenen

Erwähnenswert ist, aus aktuellem Anlass der Landtagswahlen, die Beschwerde über ein personalisiertes Schreiben einer Partei. Im Raum stand der Verstoß gegen die Informationspflichten nach Art. 14 DS-GVO infolge einer Dritterhebung der personenbezogenen Daten. Hierbei ist zu beachten, dass die Parteien der Informationspflicht nach Art. 14 DS-GVO vollumfänglich nachkommen müssen, sofern diese nicht ausnahmsweise (etwa nach Abs. 5) ausgeschlossen ist. Die Frist für die Informationserteilung ergibt sich aus Abs. 3:

Art. 14 DS-GVO

(3) Der Verantwortliche erteilt die Informationen gemäß den Absätzen 1 und 2

a) unter Berücksichtigung der spezifischen Umstände der Verarbeitung der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erlangung der personenbezogenen Daten, längstens jedoch innerhalb eines Monats,

b) falls die personenbezogenen Daten zur Kommunikation mit der betroffenen Person verwendet werden sollen, spätestens zum Zeitpunkt der ersten Mitteilung an sie, oder,

53 HBDI, https://datenschutz.hessen.de/datenschutz/internet-und-medien/facebook-seiten-von-oeffentlichen-stellen-auf-dem-pruefstand.

c) falls die Offenlegung an einen anderen Empfänger beabsichtigt ist, spätestens zum Zeitpunkt der ersten Offenlegung.

(…)

(5) Die Absätze 1 bis 4 finden keine Anwendung, wenn und soweit

a) die betroffene Person bereits über die Informationen verfügt,

b) die Erteilung dieser Informationen sich als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde; (…). In diesen Fällen ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung dieser Informationen für die Öffentlichkeit,

c) die Erlangung oder Offenlegung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen der Verantwortliche unterliegt und die geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsehen, ausdrücklich geregelt ist (…).

Betroffene Personen haben insbesondere gemäß § 50 Abs. 5 BMG das Recht, der Übermittlung ihrer Daten nach § 50 Abs. 1 BMG zu widersprechen. Sie können zudem ihr Auskunftsrecht nach Art. 15 DS-GVO sowie ggf. weitere Betroffenenrechte, wie insbesondere das Recht auf Löschung gemäß Art. 17 DS-GVO sowie das Widerspruchsrecht des Art. 21 DS-GVO, gegenüber der werbenden Partei geltend machen. Zudem kann nach Art. 77 DS-GVO eine Beschwerde bei meiner Behörde eingelegt werden.

Die datenschutzrechtliche Qual im Wahlprozess

Wahlwerbung stellt einen relevanten Teil des politischen Meinungsbildungsprozesses dar. Die Bürgerinnen und Bürger müssen verschiedene Quellen konsultieren und die Positionen der Parteien kritisch prüfen können, um schließlich eine fundierte Entscheidung zu treffen. Der Datenschutz gewährleistet die Sicherung der personenbezogenen Daten der Wählerinnen und Wähler und nimmt damit auch bei der Wahlwerbung eine wichtige Rolle ein.

Ich unterstütze diese Zielsetzung durch die Handreichung zum Datenschutz bei Wahl- und Abstimmungswerbung, die sowohl für die Adressaten wie auch die Parteien weiterführende Informationen zu den datenschutzrelevanten Rechten und Pflichten enthält. Sie kann als Kurz- und Langfassung auf meiner Webseite abgerufen werden.[54]

54 HBDI, https://datenschutz.hessen.de/datenschutz/kommunen/datenschutz-bei-wahl-und-abstimmungswerbung; s. zudem den Beitrag von Rapp/Roßnagel/Franke, Datenschutz bei Wahl- und Abstimmungswerbung, ZD 2023, 247 ff.

5.6
Datenschutz bei Vorschlagslisten für Schöffen

Im Jahr 2023 wurden bundesweit die Schöffen für die Amtszeit von 2024 bis 2028 gewählt. § 36 des Gerichtsverfassungsgesetzes (GVG) enthält datenschutzrechtliche Maßgaben hinsichtlich des Inhalts und der Veröffentlichung der Vorschlagsliste für Schöffen. Es wird geregelt, welche personenbezogenen Daten erhoben werden dürfen und wie die Auflegung in der Gemeinde zu erfolgen hat.

Wahl der Schöffen

Die Regelung des § 36 GVG wurde im Berichtszeitraum in den meisten hessischen Kommunen berücksichtigt. Gleichwohl erreichten mich mehrere Beschwerden, welche die Erhebung personenbezogener Daten auf der Vorschlagsliste sowie deren Veröffentlichung im Internet zum Gegenstand hatten. Nachfolgend soll eine der Beschwerden dargestellt werden.

§ 36 GVG

(1) Die Gemeinde stellt in jedem fünften Jahr eine Vorschlagsliste für Schöffen auf. Für die Aufnahme in die Liste ist die Zustimmung von zwei Dritteln der anwesenden Mitglieder der Gemeindevertretung, mindestens jedoch der Hälfte der gesetzlichen Zahl der Mitglieder der Gemeindevertretung erforderlich. Die jeweiligen Regelungen zur Beschlussfassung der Gemeindevertretung bleiben unberührt.

(2) Die Vorschlagsliste soll alle Gruppen der Bevölkerung nach Geschlecht, Alter, Beruf und sozialer Stellung angemessen berücksichtigen. Sie muss Familienname, Vornamen, gegebenenfalls einen vom Familiennamen abweichenden Geburtsnamen, Geburtsjahr, Wohnort einschließlich Postleitzahl sowie Beruf der vorgeschlagenen Person enthalten; bei häufig vorkommenden Namen ist auch der Stadt- oder Ortsteil des Wohnortes aufzunehmen.

(3) Die Vorschlagsliste ist in der Gemeinde eine Woche lang zu jedermanns Einsicht aufzulegen. Der Zeitpunkt der Auflegung ist vorher öffentlich bekanntzumachen.

(4) In die Vorschlagslisten des Bezirks des Amtsgerichts sind mindestens doppelt so viele Personen aufzunehmen, wie als erforderliche Zahl von Haupt- und Ersatzschöffen nach § 43 bestimmt sind. Die Verteilung auf die Gemeinden des Bezirks erfolgt durch den Präsidenten des Landgerichts (Präsidenten des Amtsgerichts) in Anlehnung an die Einwohnerzahl der Gemeinden.

Aufstellung der Schöffenliste

Gemäß § 28 GVG werden für die Verhandlung und Entscheidung der zur Zuständigkeit der Amtsgerichte gehörenden Strafsachen, soweit nicht der Strafrichter entscheidet, bei den Amtsgerichten Schöffengerichte gebildet. Das Schöffengericht besteht gemäß § 29 Abs. 1 GVG aus dem Richter beim

Amtsgericht als Vorsitzenden und zwei Schöffen. Das Amt eines Schöffen ist nach § 31 GVG ein Ehrenamt.

Nach § 36 Abs. 1 GVG stellt die Gemeinde (für den Schöffenwahlausschuss des Amtsgerichts gemäß §§ 40 ff. GVG) in jedem fünften Jahr eine Vorschlagsliste für Schöffen auf. Für die Aufnahme in die Liste ist die Zustimmung der Gemeindevertretung erforderlich.

Die Vorschlagsliste soll alle Gruppen der Bevölkerung nach Geschlecht, Alter, Beruf und sozialer Stellung angemessen berücksichtigen. Sie muss Familienname, Vornamen, gegebenenfalls einen vom Familiennamen abweichenden Geburtsnamen, Geburtsjahr, Wohnort einschließlich Postleitzahl sowie Beruf der vorgeschlagenen Person enthalten.

Gemäß § 36 Abs. 3 GVG ist die Vorschlagsliste in der Gemeinde eine Woche lang zu jedermanns Einsicht aufzulegen.

Veröffentlichung im Internet

In einer hessischen Stadt wurde die Vorschlagsliste von der Stadtverordnetenversammlung am 2. Juni 2023 beschlossen. Die Vorschlagsliste war sodann in dem Gremieninformationssystem auf der städtischen Website einsehbar und lag im Stadthaus während der Dienststunden zu jedermanns Einsicht aus. Auf der Vorschlagsliste waren neben den in § 36 Abs. 2 GVG genannten personenbezogenen Daten auch die Straße und Hausnummer, die genauen Geburtsdaten sowie die Telefonnummer enthalten. Die Kandidatinnen und Kandidaten hatten bei ihrer Bewerbung ein Formular unterschrieben und sich damit einverstanden erklärt, dass „notwendige Daten“ mit der Auflegung der Vorschlagsliste veröffentlicht werden. Die Vorschlagsliste wurde erst am 12. Juni 2023 aus dem städtischen Gremieninformationssystem im Internet entfernt.

Beschränkung auf die gesetzlich geforderten Daten

Nach den Grundsätzen für die Verarbeitung personenbezogener Daten benötigt, nach Art. 5 Abs. 1 Buchst. a und Art. 6 DS-GVO, jede Datenverarbeitung eine Rechtsgrundlage. Diese ist hier Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO („Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt“), in Verbindung mit § 36 GVG (Vorschlagsliste Schöffen).

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:

(…)

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;

(…)

Die auf der Vorschlagsliste aufzunehmenden personenbezogenen Daten sind in § 36 Abs. 2 Satz 2 GVG abschließend bestimmt. Weitere Daten (etwa Straßen, exakte Geburtsdaten sowie Telefonnummern) dürfen nicht verarbeitet werden. Deren Aufnahme auf der Vorschlagsliste ist daher datenschutzwidrig.

Ein „Einverständnis" der Kandidatinnen und Kandidaten, dass „notwendige Daten" mit der Auflegung der Vorschlagslisten veröffentlicht werden, ist überdies nicht erforderlich. Die betroffenen Personen sind lediglich entsprechend Art. 13 und 14 DS-GVO über die Datenverarbeitung zu informieren.[55]

Gemäß § 36 Abs. 3 GVG ist lediglich eine öffentliche Bekanntmachung des „Zeitpunkts der Auslegung" zulässig. Diese Bekanntmachung darf keine personenbezogenen Daten der Kandidatinnen und Kandidaten enthalten. Eine darüber hinausgehende Veröffentlichung der Vorschlagsliste im Internet ist nicht geregelt. Diese wäre angesichts des überwiegenden Persönlichkeitsschutzinteresses der Kandidatinnen und Kandidaten auch nicht im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. e DSGVO erforderlich.

Ein derartiger Vorfall muss gemäß Art. 33 DS-GVO mir als Verletzung des Schutzes personenbezogener Daten gemeldet werden. Da aufgrund der mit der Ausübung des Amtes verbundenen Gefahren ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Kandidatinnen und

55 S. DSK, Kurzpapier Nr. 10 – Informationspflichten bei Dritt- und Direkterhebung, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf.

Kandidaten nicht auszuschließen ist, sind diese überdies nach Art. 34 DS-GVO zu benachrichtigen.[56]

Ich habe die Stadt darauf hingewiesen, dass das zuständige Fachamt und der behördliche Datenschutzbeauftragte die handelnden Personen sowohl hinsichtlich der Anforderungen des Gerichtsverfassungsgesetzes als auch des Datenschutzes schulen und sensibilisieren muss. Die Stadt sollte zudem einen Prozess etablieren, der sicherstellt, dass sich derartige Verstöße zukünftig nicht wiederholen.

5.7
Datenübermittlung von einer Sozialbehörde und einem Veterinäramt

Anlässlich einer an mich gerichteten Beratungsanfrage durch den behördlichen Datenschutzbeauftragten einer hessischen Großstadt habe ich mich mit der Möglichkeit und (datenschutz-)rechtlichen Zulässigkeit einer Datenübermittlung von einer städtischen Sozialbehörde an das städtische Veterinäramt befasst. Diese etwas kurios klingende Fragestellung geht zurück auf eine vom Veterinäramt umzusetzende EU-Kontrollverordnung zur amtlichen Lebensmittelkontrolle. Im Ergebnis ist die angefragte, aus einer eher ungewöhnlichen Fallkonstellation heraus resultierende Datenübermittlung als (sozial-)datenschutzrechtlich zulässig einzuordnen.

Übermittlungswunsch

Der behördliche Datenschutzbeauftragte einer hessischen Großstadt wandte sich mit einer Beratungsbitte an mich, nachdem ihn stadtintern eine schwierige Fragestellung erreicht und er selbst bereits umfassende Vorarbeiten geleistet hatte: Das dortige städtische Veterinäramt habe die städtische Sozialbehörde um die Übermittlung personenbezogener Daten von Kindertagespflegepersonen gebeten. Konkret sei es dabei um deren Namen und Vornamen sowie um die Frage gegangen, ob die Tagespflegeperson ihre Tätigkeit im Rahmen eines Zusammenschlusses mehrerer Tagespflegepersonen, der insgesamt mehr als fünf Kinder betreut, ausübe.

Hintergrund und gleichzeitig Ausgangspunkt der Anfrage des Veterinäramtes war, dass Kindertagespflegepersonen nach Ansicht des Veterinäramtes der VO (EU) 2017/625 (EU-Kontrollverordnung) unterfallen würden. Nach dieser europäischen Verordnung gelten seit Ende 2019 neue harmonisierende Regelungen für die amtliche Lebensmittelkontrolle.

56 S. DSK, Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf.

Erster Anknüpfungspunkt der Anfrage des Veterinäramtes war folgende rechtliche Vorgabe:

Artikel 10 Abs. 2 VO (EU) 2017/625

(2) Unbeschadet der Vorschriften für bestehende Listen oder Register, die auf der Grundlage der Vorschriften gemäß Artikel 1 Absatz 2 erstellt wurden, erstellen die zuständigen Behörden eine Liste von Unternehmern und halten sie auf dem neuesten Stand. Derartige Listen und Register, die bereits für andere Zwecke erstellt wurden, können auch für die Zwecke dieser Verordnung verwendet werden.

Art. 1 Abs. 2 VO (EU) 2017/625

(2) Diese Verordnung gilt für die amtlichen Kontrollen, mit denen die Einhaltung der Vorschriften überprüft werden soll, die entweder auf Unionsebene oder von den Mitgliedstaaten zur Anwendung von Unionsrecht in diesen Bereichen erlassen wurden:

a) Lebensmittel und Lebensmittelsicherheit, Lauterkeit und gesundheitliche Unbedenklichkeit auf allen Stufen der Produktion, der Verarbeitung und des Vertriebs von Lebensmitteln, darunter Vorschriften zur Gewährleistung fairer Handelspraktiken und über den Schutz der Interessen und der Information der Verbraucher, sowie Vorschriften über die Herstellung und Verwendung von Materialien und Gegenständen, die dazu bestimmt sind, mit Lebensmitteln in Berührung zu kommen;

(…)

Artikel 15 Abs. 5 VO (EU) 2017/625 führt weiter zu Art. 10 Abs. 2 VO 2017/625 aus:

Artikel 15 Abs. 5 VO (EU) 2017/625

(5) Für die Zwecke des Artikels 10 Absatz 2 und vorbehaltlich des Artikels 10 Absatz 3 stellen die Unternehmer den zuständigen Behörden zumindest die folgenden aktualisierten Angaben zur Verfügung:

a) ihren Namen und ihre Rechtsform und

b) ihre spezifischen Tätigkeiten, einschließlich der im Wege der Fernkommunikation durchgeführten Tätigkeiten, und die Orte unter ihrer Verantwortung.

Dass Tagespflegepersonen Unternehmer im Sinne dieser Vorschriften sind, ergibt sich aus der Definition in Art. 3 Nr. 29 VO (EU) 2017/625:

Art. 3 Nr. 29 VO (EU) 2017/625

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

29. „Unternehmer" alle natürlichen oder juristischen Personen, für die eine oder mehrere Pflichten nach den Vorschriften gemäß Artikel 1 Absatz 2 gelten;

(…)

Art. 1 Abs. 2 VO (EU) 2017/625 nennt, s. o., unter anderem Vorschriften über Lebensmittel und Lebensmittelsicherheit. Zu diesen Vorschriften wiederum gehört etwa die Verordnung EG Nr. 178/2002, die den Begriff Lebensmittelunternehmen in deren Art. 3 Nr. 2 wie folgt definiert:

Art. 3 Nr. 2 VO (EG) 178/2002

Im Sinne dieser Verordnung bezeichnet der Ausdruck

2. „Lebensmittelunternehmen" alle Unternehmen, gleichgültig, ob sie auf Gewinnerzielung ausgerichtet sind oder nicht und ob sie öffentlich oder privat sind, die eine mit der Produktion, der Verarbeitung und dem Vertrieb von Lebensmitteln zusammenhängende Tätigkeit ausführen;

(…)

Unter Betrachtung all dieser genannten Vorschriften hatte der behördliche Datenschutzbeauftragte keinen Zweifel daran, dass das Veterinäramt die Daten der Tagespflegepersonen verarbeiten dürfe, um sie in die besagte Liste aufzunehmen, auch wenn Art. 15 Abs. 5 VO (EU) 2017/625 explizit nur eine Rechtsgrundlage über die Erhebung der Daten bei den Unternehmen enthalte. Er teilte insbesondere die ihm gegenüber geäußerte Befürchtung des Veterinäramtes, dass sich nicht alle Tagespflegepersonen auf freiwilliger Basis und von sich aus dort zur Umsetzung der Aufgaben nach der VO (EU) 2017/625 melden würden. Ein rechtlicher Ansatz, diese zu einer Meldung beim Veterinäramt zu verpflichten, werde nicht gesehen. Im Hinblick auf das Wohl der Kinder, die zumindest im Kleinkindalter als Personen mit nicht vollständig ausgebildetem Immunsystem, besonders von unhygienischen Verhältnissen in Küchen betroffen sein könnten, müsse ein solcher Datenaustausch aber doch möglich sein.

Nicht ganz eindeutig zu beantworten sei aus seiner Sicht allerdings dann die Frage, ob eine Weitergabe der Daten an das Veterinäramt durch die Sozialbehörde erfolgen dürfe. Daher bat er um meine Beratung und die Beantwortung der Fragen,

– ob es bei den genannten Daten der Tagespflegepersonen aus meiner Sicht um Sozialdaten handele, soweit diese von der Sozialbehörde übermittelt würden,
– ob ich dann, falls bejahend, eine Rechtsgrundlage für die Datenübermittlung der Sozialbehörde an das Veterinäramt sehe und/oder
– ob mir ggf. sonst noch eine praktikable Möglichkeit einfalle, den Datentransfer zulässig zu gestalten.

Rechtfertigung der Übermittlung

Ich habe diese umfangreiche und ungewöhnliche Beratungsanfrage wie folgt beantwortet:

Zur ersten Fragestellung habe ich deutlich klarstellend festgehalten, dass die Daten der Kindertagespflegepersonen, die bei der dortigen Sozialbehörde verarbeitet werden, Sozialdaten sind. Diese (Sozial-)Daten unterfallen gemäß § 35 Abs. 1 SGB I dem Sozialgeheimnis.

§ 35 Abs. 1 SGB I

Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 2 Zehntes Buch) von den Leistungsträgern nicht unbefugt verarbeitet werden (Sozialgeheimnis). Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. (…)

Da die bei der Sozialbehörde im Kontext ihrer Aufgabenerfüllung vorhandenen Daten Sozialdaten sind (§ 67 Abs. 2 SGB X), ist das HDSIG nicht anwendbar, weil gemäß § 35 Abs. 2 SGB I die Vorschriften des Zweiten Kapitels des SGB X und der übrigen Bücher des SGB die Verarbeitung von Sozialdaten abschließend regeln. Die §§ 21 und 22 HDSIG fallen daher als mögliche Rechtsgrundlagen für den Datentransfer aus.

Für eine rechtskonforme Datenübermittlung von der Sozialbehörde an das Veterinäramt kommen aus datenschutzrechtlicher Sicht daher nur die Vorschriften des § 69 Abs. 5 in Verbindung mit § 67c Abs. 3 Satz 1 SGB X in Betracht.

§ 69 Abs. 5 SGB X

(1) Die Übermittlung von Sozialdaten ist zulässig für die Erfüllung der gesetzlichen Aufgaben der Rechnungshöfe und der anderen Stellen, auf die § 67c Absatz 3 Satz 1 Anwendung findet.

§ 67c Abs. 3 SGB X

(3) Eine Speicherung, Veränderung oder Nutzung von Sozialdaten ist zulässig, wenn sie für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für den Verantwortlichen oder für die Wahrung oder Wiederherstellung der Sicherheit und Funktionsfähigkeit eines informationstechnischen Systems durch das Bundesamt für Sicherheit in der Informationstechnik erforderlich ist. Das gilt auch für die Veränderung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit nicht überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

Nach § 69 Abs. 5 SGB X ist also die Übermittlung von Sozialdaten zulässig für die Erfüllung der gesetzlichen Aufgaben der Rechnungshöfe und anderer Stellen, auf die § 67c Abs. 3 S. 1 Anwendung findet. Gemäß § 67c Abs. 3 Satz 1 SGB X ist eine Speicherung, Veränderung oder Nutzung von Sozialdaten zulässig, wenn sie für die Wahrnehmung von Aufsichts-, Kontroll- und Disziplinarbefugnissen, der Rechnungsprüfung erforderlich ist.

Im Fall der Aufsichts-, Kontroll- und Disziplinarbefugnisse, der Rechnungs- und Prüfungstätigkeit dient die Regelung des § 67 Abs. 3 Satz 1 SGB X dem Interesse einer funktionsfähigen Verwaltung. In diesem Fall ist eine Speicherung, Veränderung und Nutzung unabhängig vom Erhebungszweck des Abs. 1 Satz 1 und vom Speicherungszweck des Abs. 1 Satz 2 zulässig. Im konkreten Fall ist die Datenverarbeitung auch zur Wahrnehmung dieser Aufgaben erforderlich, weil die für die Aufgabenerfüllung des Veterinäramtes benötigten Angaben kaum vollständig auf freiwilliger Grundlage oder auf der Basis einer Bitte oder eines Appells, seitens der nummerisch großen Gruppe von Kindertagespflegepersonen, zu erhalten sind.

Zusammenfassend kann festgehalten werden, dass eine innerstädtische Datenübermittlung von der Sozialbehörde an das Veterinäramt auf der Grundlage von § 69 Abs. 5 in Verbindung mit § 67c Abs. 3 S. 1 SGB X zulässig ist, wenn sie für gesetzlich festgelegte Kontrollaufgaben erforderlich ist.

6. Schule, Hochschulen und Archive

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. In guter Zusammenarbeit begleite und berate ich das Ministerium in der datenschutzgerechten Umsetzung dieser Projekte und ihrer rechtlichen Regulierung. In diesem Zusammenhang habe ich das Ministerium beim Erlass der neuen Schuldatenschutz-Verordnung beraten (Kap. 6.1), das Datenschutzkonzept für das Schulportal Hessen bewertet (Kap. 6.3) und an der Erstellung eines Online-Datenschutzkurses für Lehrkräfte mitgewirkt (Kap. 6.5). Auch die Schulträger habe ich hinsichtlich ihres rechtlichen Verhältnisses zu den Schulen (Kap. 6.2) und hinsichtlich des Einsatzes von Microsoft 365 in Schulen beraten (Kap. 6.4). Die „Arolsen Archives", das internationale Zentrum über NS-Verfolgung mit dem weltweit umfassendsten Archiv zu den Opfern und Überlebenden des Nationalsozialismus, habe ich geprüft und hinsichtlich ihrer autonomen Regelungen zum Datenschutz beraten (Kap. 6.6).

6.1
Die neue Schuldatenschutz-Verordnung

Mit der am 16. Dezember 2023 in Kraft getretenen neuen Schuldatenschutz-Verordnung ist ein seit Jahren vakantes Regelungsdefizit durch das HKM behoben worden. Im Sinne der Schulen sowie der Schulverwaltungsbehörden sind nun Normen in Kraft, die den Vorgaben der DS-GVO gerecht werden und die Digitalisierung im Schulbereich angemessen berücksichtigen. Im Sinne des Datenschutzes hat das Hessische Kultusministerium damit einen überfälligen Schritt vollzogen.

Der bis zum 16. Dezember 2023 gültige Zustand

Den schulischen Datenschutz in seinen Details regelte die Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen, die seit dem 4. Februar 2009 (ABl. 2009, S. 131 ff.) in Kraft war. Die Grundlage hierfür bildete § 83 Abs. 9 des Hessischen Schulgesetzes (HSchG), wonach „Umfang und Einzelheiten der personenbezogenen Datenverarbeitung in der Schule" näher in einer Rechtsverordnung zu regeln waren. So fand man z. B. die Bedingungen, unter denen Lehrkräfte auf privaten PC außerhalb der Schule personenbezogene Daten der Schüler verarbeiten dürfen, in dieser Verordnung geregelt.

Mit dem Wirksamwerden der Datenschutz-Grundverordnung (DS-GVO) war der Gesetzgeber gefordert, in der Verordnung rechtliche Anpassungen vorzunehmen und vor allem dem Aspekt der Digitalisierung der Schulen Rechnung zu tragen. Spätestens mit dem Beginn der Pandemie und der Schließung der Schulen zeigte sich, dass die damalige Verordnung den rechtlichen Erfordernissen nicht mehr entsprach. So war der Einsatz von Videokonferenzsystemen (VKS) in und außerhalb der Schule nicht geregelt – mit der Konsequenz, dass in diesem Bereich datenschutzrechtlich ein Wildwuchs entstand. Sowohl im Hessischen Schulgesetz als auch in der neuen Schuldatenschutz-Verordnung sind jetzt Regelungen enthalten, auf welche Weise ein datenschutzkonformer, auf VKS-gestützter Distanzunterricht erfolgen kann.

Datenschutz-Regelungen nun in einer neu erstellten Verordnung verankert

Sowohl das HKM als auch ich haben erkannt, dass es mit einer Modifizierung der alten Verordnung nicht mehr getan sein konnte. Zu viele Sachverhalte bedurften einer neuen oder an die DS-GVO angepassten Regelung, so dass es angezeigt schien, eine neue Verordnung zu erlassen, die zudem auch eine klare, nach inhaltlichen Aspekten geordnete Struktur aufweisen musste. Die neue Verordnung ist in verschiedene Abschnitte unterteilt. Zunächst legt Teil I allgemeine Grundlagen der Datenverarbeitung fest, bevor Teil II Datenverarbeitungsprozesse im schulischen Bereich regelt. Teil III behandelt die Schulgesundheitspflege und den Schulpsychologischen Dienst. Teil IV regelt Erhebungen an Schulen für die Bereiche der Bildungsplanung, der Bildungsberichterstattung, der Evaluierung sowie der amtlichen Statistik.

Bestimmte Sachverhalte wurden komplett neu in die Verordnung aufgenommen. So werden in § 5 (Organisation des Datenschutzes) den Schulen eine Reihe von Pflichten auferlegt, die einen Bezug zur DS-GVO beinhalten: Erstellung von Verarbeitungsverzeichnissen, Abschluss von Verträgen zur Auftragsverarbeitung, soweit Dritte Datenverarbeitungsprozesse für die Schule übernehmen, und die Informationspflichten gegenüber Eltern und Schülern. Erstmals sind die datenschutzrechtlichen Pflichten der Schulen umfassend definiert. Auch das Institut des schulischen Datenschutzbeauftragten wird (in § 7) nun angemessen gewürdigt. Besonders interessant ist Abs. 4. Danach dürfen Schulen in Abstimmung mit dem zuständigen Staatlichen Schulamt (SSA) aus Mitteln des Schulbudgets externe, zertifizierte Dienstleister für die Belange des Datenschutzes beauftragen.

In § 8 sind Regelungen u. a. zur Schülerakte enthalten sowie zur Verarbeitung von Gesundheitsdaten. Als Neuerung ist in § 10 die Nutzung des Schulpor-

tals Hessen (SPH) festgehalten. Eine eigene Regelung hat nun auch die Akteneinsicht in die Schülerakte (§ 16) erhalten. Die Vorschriften zu den Aufbewahrungsfristen, der Löschung von Daten und der Vernichtung von Akten sind in § 17 normiert.

Zu begrüßen ist auch, dass die Nutzung von VKS nunmehr geregelt ist (§ 18), auch wenn ich an einigen Stellen noch einen Bedarf an Ergänzung und Konkretisierung sehe (so z. B. § 18 Abs. 2 Satz 2), soweit es um die Mitarbeit von Eltern und anderen Personen im Unterricht geht, bei denen allgemeine Regelungen zu beachten sind. Hilfreich ist grundsätzlich, dass datenschutzrechtlich eine Differenzierung der Datenverarbeitung durch Lehrkräfte auf dienstlichen und privaten Endgeräten erfolgt (§§ 19 und 20). Bei der Nutzung von privaten Endgeräten fehlt es allerdings an der Vorgabe, dienstliche Daten ausschließlich auf einem mobilen Speichergerät wie z. B. Stick oder Wechselfestplatte zu speichern (s. hierzu auch die Hinweise in Kap. 14.8).

Neu ist ebenfalls, dass nun für die Datenverarbeitung im Zusammenhang mit dem Religionsunterricht, zur Dokumentation der Kindeswohlgefährdung, und beim Besuch einer Schule für Kranke eigene Normen geschaffen wurden.

Nicht zuletzt hat auch die Datenverarbeitung durch die Elternvertretungen Eingang in die Schuldatenschutz-Verordnung gefunden.

Dass nun auch die Schulgesundheitspflege mit einer eigenständigen Norm (§ 31) legitimiert ist, schafft für deren spezifische Art der Datenverarbeitung die erforderliche Rechtssicherheit.

Kurzum: Auch wenn es aus meiner Sicht weiteren Ergänzungs- und Verbesserungsbedarf gibt, so hat die neue Schuldatenschutz-Verordnung einen Mehrwert für die schulische Datenverarbeitung geschaffen, die sich nun auf umfassende und präzise Regelungsinhalte stützen kann. Gleichwohl handelt es sich hier um einen dynamischen Prozess: Eine stetige, sich fortentwickelnde Anpassung an die Realitäten der Datenverarbeitung in der Schule, muss weiterhin der Anspruch für das Kultusministerium sein.

6.2
Datenschutzrechtliches Verhältnis zwischen Schulen und Schulträgern

Auf meine Initiative hin wurde Mitte des Jahres 2023 eine Arbeitsgruppe eingerichtet, die sich mit dem Thema der datenschutzrechtlichen Verantwortlichkeit in dem Verhältnis zwischen Schulen und Schulträgern des Landes Hessen befasst. Der Arbeitsgruppe gehören neben meinen Mitarbeitern auch Vertreterinnen und Vertreter des Hessischen Kultusministeriums (HKM), des Landkreis- und Städtetages sowie der Schulträger an. Ziel der Arbeitsgruppe

ist es, den Beteiligten Mustervorlagen zur Verfügung zu stellen, auf deren Grundlage die datenschutzrechtliche Verantwortlichkeit, bezogen auf die tatsächlichen Verhältnisse zwischen den Schulen und Schulträgern vor Ort, geregelt werden kann.

Rechtliche Ausformungen datenschutzrechtlicher Verantwortung

Die DS-GVO sieht unterschiedliche Arten von datenschutzrechtlicher Verantwortlichkeit vor, die mit unterschiedlichen Rechten, Pflichten und Rechtsfolgen verbunden sind.

Normadressat der DS-GVO ist in erster Linie der Verantwortliche. Die DS-GVO unterscheidet zwischen den Rechtsinstituten der alleinigen Verantwortlichkeit, der gemeinsamen Verantwortlichkeit und der Auftragsverarbeitung. Wer Verantwortlicher im Sinne der DS-GVO ist, definiert Art. 4 Nr. 7 DS-GVO. Nach dieser Norm ist „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Im Unterschied zu dem Verantwortlichen entscheidet der Auftragsverarbeiter nicht selbst über die Zwecke und Mittel der Verarbeitung, sondern setzt die Weisungen des Verantwortlichen um. Sind mehrere Personen oder Stellen an einer Verarbeitung beteiligt, regeln Vereinbarungen zwischen den Beteiligten die Verantwortlichkeit.

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel zur Verarbeitung fest, so sind sie gemäß Art. 26 Abs. 1 DS-GVO gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtungen gemäß der DS-GVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht und wer welchen Informationspflichten gemäß den Art. 13 und 14 DS-GVO nachkommt. Gemäß Art. 26 Abs. 2 DS-GVO muss die Vereinbarung die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber betroffenen Personen gebührend widerspiegeln.

Von der gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO ist die Auftragsverarbeitung nach Art. 28 DS-GVO abzugrenzen. „Auftragsverarbeiter" ist nach Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Obwohl der Auftragsverarbeiter tatsächlich die Datenverarbeitung durchführt, bleibt der Verantwortliche für diese allein verantwortlich. Art. 28 Abs. 1 DS-GVO regelt, dass wenn eine Verarbeitung im Auftrag eines Verantwortlichen erfolgt, dieser nur mit solchen Auftragsverarbeitern arbeitet, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt

werden, dass die Verarbeitung im Einklang mit den Anforderungen der DS-GVO erfolgt und den Schutz der Rechte der betroffenen Personen gewährleistet. Gemäß Art. 28 Abs. 3 DS-GVO erfolgt die Verarbeitung durch einen Auftragsverarbeiter unter anderem auf der Grundlage eines Vertrags, der den Auftragsverbarbeiter an den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien der betroffenen Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

Die datenschutzrechtliche Verantwortlichkeit zwischen Schulen und Schulträgern

Die hessischen Schulträger sind gemäß § 158 HSchG für die Ausstattung der hessischen Schulen zuständig. Hierzu gehören neben der Zurverfügungstellung von Schulgebäuden und Lehrmitteln beispielsweise auch die Bereitstellung von elektronischen Endgeräten wie Laptops und Tablets für Lehrkräfte und Schülerinnen und Schüler sowie auch Software, die in der Schule verwendet wird. Im schulischen Alltag arbeiten Schulen und Schulträger mithin eng zusammen, um dem schulischen Bildungs- und Erziehungsauftrag nachzukommen. Es ist somit von grundsätzlichem Interesse der Schulen und Schulträger in Hessen, eine nachvollziehbare Regelung hinsichtlich der datenschutzrechtlichen Verantwortlichkeit zwischen diesen Institutionen zu finden. Bereits im Jahr 2019 haben meine Mitarbeiter gegenüber den beteiligten Stellen, bestehend aus dem HKM, dem Landkreis- und Städtetag sowie den Schulträgern, kommuniziert, dass es nach der DS-GVO notwendig ist, die datenschutzrechtlichen Verhältnisse zwischen den Schulen und Schulträgern in Form von Verträgen zu regeln. Aufgrund der Komplexität dieser Aufgabe hat meine Behörde schon zum damaligen Zeitpunkt ihre Unterstützung bei der Erarbeitung passender Verträge angeboten. Aufgrund der Corona-Pandemie ist diese Thematik seinerzeit in den Hintergrund getreten. Im Berichtsjahr wurde das Thema wiederaufgenommen und im Rahmen einer Auftaktveranstaltung der eingerichteten Arbeitsgruppe ein inhaltliches Konzept erarbeitet. Dazu wurde der Ist-Zustand bei den Schulträgern, bezogen auf bereits vorhandene Vereinbarungen, erfragt und das Ziel der Arbeitsgruppe, das Erarbeiten von Mustervorlagen für die Regelung der datenschutzrechtlichen Verantwortlichkeiten im Verhältnis zwischen hessischen Schulen und Schulträgern, festgelegt. In einem nächsten Schritt wird den Schulträgern ein Fragenkatalog übermittelt. Die Antworten auf die gestellten Fragen sollen die faktischen Gegebenheiten vor Ort aufzeigen und als Grundlage für den weiteren Austausch in der Arbeitsgruppe und der Erstellung der Mustervorlagen dienen. Mit Arbeitsergebnissen in Form von Mustervorlagen, die den

Schulen und Schulträgern in Hessen zur Verfügung gestellt werden können, ist im Laufe des kommenden Berichtsjahres zu rechnen.

6.3
Bewertung des Datenschutzkonzepts zum Schulportal Hessen

Bereits im 50. und 51. Tätigkeitsbericht habe ich über meine Beratungstätigkeiten bezogen auf das Schulportal Hessen (SPH) berichtet. Im zurückliegenden Berichtsjahr hat nun die datenschutzrechtliche Bewertung des SPH durch mich stattgefunden.

Beratung zum Datenschutzkonzept des SPH

Das SPH ist in der hessischen Schullandschaft ein Digitalisierungsprojekt, dem aufgrund seines nahezu flächendeckenden Einsatzes an hessischen Schulen besondere Bedeutung zukommt. Über das Portal wird der Schulgemeinschaft ein breites Spektrum an Diensten für Pädagogik und Schulverwaltung zur Verfügung gestellt und es werden umfangreiche, teilweise auch besonders schützenswerte personenbezogene Daten verarbeitet. Dies macht es im Sinne des Schutzes der Rechte und Freiheiten der das SPH nutzenden Schülerinnen und Schüler, Lehrkräfte, Eltern und anderer schulbezogener Nutzer erforderlich, die im SPH verarbeiteten personenbezogenen Daten auf einem entsprechend hohen Schutzniveau zu schützen. Aus diesem Grund habe ich in den letzten Jahren das HKM und die ihm nachgeordnete Lehrkräfteakademie (LA) bei der Entwicklung eines Datenschutzkonzepts für das SPH beratend begleitet. So habe ich z. B. bezogen auf die einzelnen Bestandteile des Datenschutzkonzepts – wie etwa der getroffenen technischen und organisatorischen Maßnahmen oder der Prozesse zur Umsetzung von Betroffenenrechten aus Art. 12 ff. DS-GVO – jeweils angemerkt, welche Änderungen dazu beitragen könnten, dem Datenschutz noch besser Rechnung zu tragen.

Beratungsabschluss mit Bewertung

Aus Sicht des Datenschutzes stellt sich das SPH als komplexes digitales Werkzeug mit einer Fülle von Verarbeitungstätigkeiten dar. Da das SPH regelmäßig an neue und sich ändernde Anforderungen des Schulbetriebs angepasst wird, entwickeln sich auch die Verarbeitungstätigkeiten ständig weiter. Aus diesem Grund wurde die Bewertung des Datenschutzkonzepts zu einem konkreten Zeitpunkt anhand der dann vorliegenden Unterlagen vorgenommen. Nachträgliche Weiterentwicklungen und Veränderungen waren von der Prüfung nicht umfasst.

Fazit der Bewertung und Ausblick

Mit meiner umfangreichen Bewertung habe ich gegenüber dem HKM und der LA zum Ausdruck gebracht, dass das Datenschutzkonzept der Mächtigkeit des Datenverarbeitungsprojekts SPH bereits grundsätzlich entspricht. Ein datenschutzrechtlicher Mehrwert für das SPH ergibt sich aus dem technischen Aufbau der Plattform. Die Verwendung von Open Source Software (OSS), angefangen vom Identitätsmanagement LemonLDAP und weitergehend u. a. zu den pädagogischen Werkzeugen Moodle oder Mahara, bis hin zu Vertretungsplan oder elektronischem Klassenbuch: Die Unabhängigkeit von den großen Digitalunternehmen ist begrüßenswert und damit bundesweit wohl einmalig. Das SPH ist ein Vorbild für digitale Souveränität. Gleichwohl hat meine Bewertung nicht unerhebliche Mängel hinsichtlich der Dokumentation sowie der Umsetzung einzelner Datenverarbeitungsprozesse zu Tage gefördert, so dass hier noch in einem erheblichen Maß nachgesteuert werden musste. So war etwa das Löschkonzept zum Zeitpunkt der Bewertung noch unzureichend.

In den vergangenen beiden Jahren hat es zu dem Thema SPH einen umfangreichen Austausch zwischen HKM und meiner Behörde gegeben, der sich durch eine Fülle von Schreiben, Dokumenten und auch Sitzungsprotokollen nachvollziehen lässt. Eine konstruktive Herangehensweise war durch die kooperative Zusammenarbeit des HKM und der LA mit mir möglich. Das Ergebnis entspricht grundsätzlich den Anforderungen des Datenschutzrechts. Gleichwohl war noch ein erheblicher, zum Teil akuter Nachholbedarf festzustellen. Darüber hinaus sind HKM und LA gefordert, Modifikationen und Erweiterungen des SPH nachvollziehbar zu dokumentieren und die erforderlichen datenschutzrechtlichen Maßnahmen den Verarbeitungsprozessen anzupassen. In diesem Kontext ist auch meine Bewertung zu verstehen, die deutlich macht, in welchem Bereich Defizite erkennbar sind, und entsprechende Handlungserfordernisse formuliert.

Auch in Zukunft werde ich das HKM bei der Bewältigung von datenschutzrechtlichen Herausforderungen im Zusammenhang mit dem SPH entsprechend der Aufgaben der Datenschutzaufsichtsbehörde unterstützen.

6.4
Schulträger und Microsoft 365 an hessischen Schulen

Auf Grundlage der §§ 155 ff. des Hessischen Schulgesetzes stellen die Schulträger in Hessen den in ihrem Bereich ansässigen Schulen unter anderem auch digitale Werkzeuge zur Nutzung zur Verfügung. Viele Schulträger gehen in ihrer Unterstützung über das hinaus, was ihnen per Gesetz an

Aufgabenzuweisung übertragen worden ist. Die Schulträger haben in diesem Rahmen aber auch eine besondere Verantwortung. Bei den begrüßenswerten Bemühungen, die Schulen auf ihrem Weg der Digitalisierung zielgerichtet zu unterstützen, ist auch der Blick auf die Rechtmäßigkeit der Datenverarbeitung erforderlich. Der Verwendung von Microsoft 365 (MS 365) im schulischen Kontext begegneten im Berichtsjahr auf der Grundlage des europäischen Datenschutzrechts, insbesondere der DS-GVO sowie der Rechtsprechung des Europäischen Gerichtshofs (EuGH, z. B. Schrems II-Entscheidung), rechtliche Bedenken. Dies habe ich zum Anlass genommen, hierzu eine umfassende datenschutzrechtliche Beratung der hessischen Schulträger durchzuführen.

Videokonferenz mit den Schulträgern

Um die hessischen Schulträger über ihre Rechte und Pflichten insbesondere im Zusammenhang mit der Bereitstellung von MS 365 für die Schulen in Hessen zu informieren, habe ich die Schulträger zu einer gemeinsamen Videokonferenz eingeladen. Das Interesse der Schulträger an dieser Veranstaltung war groß. Aus Kapazitätsgründen musste die Veranstaltung auf zwei Videokonferenzen aufgeteilt werden. Insgesamt nahmen ca. 100 Personen teil. Auch Vertreterinnen und Vertreter des Hessischen Kultusministeriums waren anwesend. In der Konferenz habe ich den Teilnehmenden auf Grundlage der Festlegung der DSK vom 24. November 2022[57] erläutert, dass die Nutzung von MS 365 durch öffentliche Stellen und damit auch in Schulen, nicht datenschutzkonform erfolgen kann. Dies habe ich an den folgenden sieben Punkten festgemacht:

1. Die datenschutzrechtlich verantwortlichen Stellen, wie beispielsweise die Schulen, dürfen personenbezogene Daten nur verarbeiten, soweit eine Rechtsgrundlage dies erlaubt. Es ist deshalb zwingend erforderlich, dass die verantwortlichen Stellen als Auftraggeber Microsoft als Auftragnehmer vorgeben können, welche personenbezogenen Daten der Schülerinnen und Schüler, Eltern und Beschäftigten für welchen Zweck von Microsoft im Rahmen des Auftrags verarbeitet werden. Die Umsetzung dieser Vorgaben wurde von Microsoft bislang weder den Schulträgern noch den Schulen zugesichert.
2. Als Auftragnehmer darf Microsoft keine personenbezogenen Daten der Schülerinnen und Schüler, Eltern und Beschäftigten aus dem Auftragsverhältnis zu seinen eigenen Zwecken (etwa zur Weiterentwicklung seiner

57 DSK, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKBeschluessePositionspapiere/104DSK-Festlegung-Microsoft-Onlinedienste.pdf?__blob=publicationFile&v=1

Produktpalette oder für sonstige Geschäftstätigkeiten) verarbeiten. Die Schulträger bzw. Schulen als öffentliche Stellen können eine solche Verarbeitung aufgrund von Art. 6 Abs. 1 UAbs. 2 DS-GVO nämlich nicht auf ein berechtigtes Interesse stützen. Die Schulträger bzw. Schulen sollten sich zusichern lassen, dass Microsoft solche Daten nicht zu eigenen Zwecken verarbeitet. Sollte Microsoft diese Zusicherung nicht geben, muss geprüft werden, ob die Schulen Microsoft die Daten aufgrund einer Rechtsgrundlage wie z. B. § 22 Abs. 2 und 3 des HDSIG übermitteln dürfen. Diese Prüfung kann nur durchgeführt werden, wenn Microsoft zunächst folgende Fragen beantwortet hat:

   a. Um welche Daten handelt es sich hierbei im Einzelnen (bspw. auch besondere Datenkategorien nach Art. 9 DS-GVO)?
   b. Für jeweils welche festgelegten Zwecke werden die personenbezogenen Daten verwendet?
   c. Auf welcher Rechtsgrundlage basiert die Verarbeitung jeweils?

3. Weder die Schulträger noch die Schulen können nach den Vorschriften der DS-GVO Microsoft eine Erlaubnis dazu geben, personenbezogene Daten der Schülerinnen und Schüler, Eltern und Beschäftigten nach gesetzlichen US-Normen (z. B. Cloud-Act, FISA 702) z. B. US-Sicherheitsbehörden offenzulegen. Sollten in den Vereinbarungen mit Microsoft derartige Klauseln enthalten sein, muss darauf hingewirkt werden, dass diese Klauseln gestrichen werden.
4. Die datenschutzrechtlich verantwortliche Stelle, z. B. die Schule, muss nach der DS-GVO sicherstellen, dass alle personenbezogenen Daten, die ein Produktanbieter im Rahmen des schulischen Einsatzes verarbeitet, den von Art. 32 DS-GVO geforderten Schutzmaßnahmen zur Sicherheit der Verarbeitung unterliegen. Sollte dies in den Verträgen mit Microsoft zu MS 365 nicht ausreichend geregelt sein, muss von Microsoft eingefordert werden, dass dies ausnahmslos umgesetzt wird.
5. Nach Art. 28 Abs. 2 und 4 DS-GVO darf die Einschaltung von Unterauftragsverarbeitern erst nach Zustimmung der datenschutzrechtlich verantwortlichen Stelle, wie z. B. der Schule, erfolgen. Sollte in den Verträgen mit Microsoft zu MS 365 hierzu nichts oder etwas Gegenteiliges geregelt sein, muss ein solches Verfahren von Microsoft eingefordert werden. Dem Schulträger oder den Schulen gegenüber müssen die Unterauftragsverarbeiter im Einzelnen benannt werden. Dies umfasst auch eine Informationspflicht, wenn die eingesetzten Unterauftragsverarbeiter sich ändern, z. B. wegfallen oder neue hinzukommen. Darüber hinaus muss ihnen gegenüber dargelegt werden, welche personenbezogenen Daten

zu welchen Zwecken, durch welchen dieser Unterauftragsverarbeiter, in welchen Staaten verarbeitet werden.

6. Zum Zeitpunkt der Konferenz mit den Schulträgern durften personenbezogene Daten aufgrund eines fehlenden Angemessenheitsbeschlusses der EU-Kommission für die USA nur aus einem Auftragsverarbeitungsverhältnis in die USA übermittelt werden, soweit der Auftragsverarbeiter gemäß Art. 46 DS-GVO zusätzliche Maßnahmen in erforderlichem Umfang im Sinne der Rechtsprechung des EuGH (Schrems II) traf und der Empfehlung des Europäischen Datenschutzausschusses 1/2020 gegen Zugriffe von US-Behörden nachkam. Um das geltende europäische Datenschutzrecht zu erfüllen, musste Microsoft eine solche Zusicherung im Rahmen der zwischen den Schulen und Schulträgern und Microsoft geschlossenen Verträgen zu MS 365 geben. Seit dem Juli des Berichtsjahres kann eine solche Datenübermittlung wieder auf den zwischenzeitlich von der EU-Kommission verabschiedeten neuen Angemessenheitsbeschluss gemäß Art. 45 DS-GVO gestützt werden (s. dazu Kap. 2.2).
7. In dem Fall, dass ein Vertrag mit einem Auftragnehmer endet, muss vereinbart werden, dass die von der verantwortlichen Stelle an diesen übertragenen personenbezogenen Daten entweder gelöscht oder zurückgegeben und gelöscht werden. Im Rahmen der Verträge mit Microsoft muss Microsoft den Schulen und Schulträgern zusichern, dass sämtliche personenbezogenen Daten nach Ende des Datenverarbeitungsvertrages im Sinne von Art. 28 Abs. 3 lit. g DS-GVO gelöscht oder an die Schulen zurückgegeben und dann gelöscht werden.

Brief an die Schulträger

Zur weiteren Unterstützung bei der Durchsetzung ihrer Rechte gegenüber Microsoft habe ich den Schulträgern einen Brief zukommen lassen, in dem ich meine Aussagen noch einmal schriftlich erläutert habe. Dies soll die Schulträger dabei unterstützen, ihre Rechte gegenüber Microsoft geltend zu machen und im Rahmen der Datenverarbeitung den Ansprüchen des europäischen Datenschutzrechts gerecht zu werden.

6.5
Online-Datenschutzkurs für Lehrkräfte

In einem gemeinsamen Projekt haben Expertinnen und Experten der Hessischen Lehrkräfteakademie für die Erstellung von Lernvideos zusammen mit mir einen Online-Datenschutzkurs für Lehrkräfte in Hessen entwickelt.

Entstehung des Online-Datenschutzkurses

Sowohl der Hessischen Lehrkräfteakademie als auch mir, ist es ein Anliegen, die Lehrkräfte im Land Hessen optimal bei ihrer täglichen Arbeit zu unterstützen. Nicht erst seit dem Inkrafttreten der Datenschutz-Grundverordnung gehört zum Arbeitsalltag der Lehrkräfte auch ein sicherer Umgang mit dem Datenschutz. Wir waren uns darüber einig, dass dieses Wissen den Lehrkräften niederschwellig und jederzeit abrufbar zur Verfügung stehen sollte. So kann sowohl eine Lehrkraft im Vorbereitungsdienst als auch eine erfahrene Lehrkraft ihr Wissen für den Arbeitsalltag im Bereich des Datenschutzes niederschwellig aufbauen oder auffrischen. Im Mai 2022 entstand die Idee, einen Online-Selbstlernkurs speziell für Lehrkräfte im Rahmen eines interdisziplinären Projekts zu kreieren und den Lehrkräften über das Internet jederzeit abrufbar zur Verfügung zu stellen. Ab diesem Zeitpunkt trafen sich Vertreterinnen und Vertreter der Lehrkräfteakademie sowie meine Mitarbeiter zu regelmäßigen Projektsitzungen. Während die Lehrkräfteakademie ihre Expertise hinsichtlich der Erstellung von Videos zur Verfügung stellte, lieferten meine Mitarbeiter das datenschutzrechtliche Wissen. Durch diese interdisziplinäre Zusammenarbeit ist ein ansprechender Selbstlernkurs entstanden, der den Lehrkräften kurzweilig und rechtlich fundiert Basiswissen im Datenschutz liefert, das sie im schulischen Arbeitsalltag anwenden können.

Inhalt des Online-Selbstlernkurses

Bislang besteht der Selbstlernkurs aus neun Modulen, deren Kern ein jeweils ein- bis dreiminütiges Video beinhaltet, in dem der jeweilige Themenkomplex kurz und prägnant erklärt wird. Während das Modul 1 den Lehrkräften die „Grundlagen des Datenschutzes“ vermittelt, behandeln die Module 2 und 3 die Themenfelder „Rechte und Verantwortung“ und die „Einwilligung“ im schulischen Kontext. In den Modulen 4 bis 9 erfährt die Lehrkraft, wie aus datenschutzrechtlicher Sicht im schulischen Alltag mit der Schülerakte, dem Klassenbuch oder Bild- und Tonaufnahmen umgegangen werden muss. Außerdem erlernt sie die richtige Bewertungskommunikation, wie beispielsweise die datenschutzkonforme Bekanntgabe von Noten gegenüber Schülerinnen und Schülern sowie die datenschutzkonforme Nutzung sowohl privater IT-Systeme wie auch von Social Media- und Messenger-Diensten.

Fazit

Viele Lehrkräfte haben bislang Berührungsängste mit dem Datenschutz oder haben dieses Thema als überfordernd wahrgenommen. Mit dem Online-Datenschutzkurs für Lehrkräfte ist über den Zeitraum von eineinhalb Jahren in behördenübergreifender Zusammenarbeit ein inhaltlich niederschwelliger,

gleichwohl gut verständlicher Selbstlernkurs entstanden, der für Lehrkräfte seit September 2023 über die Homepage der Hessischen Lehrkräfteakademie abrufbar ist. Er bringt den Lehrkräften den Datenschutz näher und zeigt, dass dieser auch im Arbeitsalltag gut handhabbar sein kann. Damit verbunden ist die Hoffnung, dass künftig weitere Projekte dieser Art umgesetzt werden können, um den Datenschutz in hessischen Schulen weiter voranzubringen.

6.6
Arolsen Archives regeln den Datenschutz in eigener Zuständigkeit

Nach Gesprächen mit Vertretern der Arolsen Archives hat die Internationale Organisation den Datenschutz in eigener Verantwortung geregelt. Der Internationale Ausschuss hat im Rahmen einer Sitzung in Brüssel Richtlinien für die Datenverarbeitung durch die Arolsen Archives erlassen sowie ein Komitee für den Datenschutz eingesetzt.

Die Arolsen Archives

Die Arolsen Archives (AA) sind das internationale Zentrum über NS-Verfolgung mit dem weltweit umfassendsten Archiv zu den Opfern und Überlebenden des Nationalsozialismus. Die Sammlung mit Hinweisen zu rund 17,5 Millionen Menschen gehört zum UNESCO-Weltdokumentenerbe. Sie beinhaltet Dokumente zu den verschiedenen Opfergruppen des NS-Regimes und ist eine wichtige Wissensquelle für die heutige Gesellschaft.

Der Internationale Ausschuss

Träger der AA sind die Staaten Belgien, Frankreich, Deutschland, Griechenland, Israel, Italien, Luxemburg, Niederlande, Polen, Großbritannien und die Vereinigten Staaten von Amerika. Regierungsvertreter dieser elf Mitgliedstaaten bilden den Internationalen Ausschuss (IA), der die Arbeit der AA im Sinne der ehemals Verfolgten überwacht. Der IA legt seit dem Bonner Abkommen von 1955 den Rahmen für die Arbeit der Institution fest. Jeweils ein Jahr lang hat einer der Mitgliedstaaten den Vorsitz – 2023/24 ist das die Bundesrepublik Deutschland.

Datenschutzrechtliche Zuständigkeit

In der Vergangenheit gingen die AA davon aus, dass hinsichtlich der datenschutzrechtlichen Normen die DS-GVO anzuwenden sei. Die ITS (International Tracing Service) bezeichnete sich als Verantwortlicher für die Datenverarbeitung, als Datenschutzbeauftragte war eine externe Rechtsanwaltsgesell-

schaft benannt. Als Rechtsgrundlage für die Datenverarbeitung wurden, je nach Sachverhalt, die Konstellationen aus Art. 6 Abs. 1 DS-GVO benannt:

– für das Abonnement des Newsletters Buchst. a),
– für die Bereitstellung und Nutzung der Website Buchst. f),
– für das Kontaktformular für Angehörige u. a. Buchst. a),
– für Forschungsanträge Buchst. a),
– für die Weitergabe von personenbezogenen Daten lit Buchst. a), b), c) und f),
– für den Einsatz von Cookies lit Buchst. a) und f),
– für das Tracking und Analysetools Buchst. a).

Gemäß der Protokollerklärung der Bundesrepublik Deutschland[58] findet das BDSG auf den Internationalen Suchdienst (Arolsen Archives) keine Anwendung. Da der Internationale Suchdienst und seine Tätigkeit auf einer völkerrechtlichen Übereinkunft beruhen, könne er nicht als „öffentlich-rechtlich organisierte Einrichtung des Bundes" angesehen werden. Ebenso wenig könne er als „nicht-öffentliche Stelle" nach § 2 Abs. 4 BDSG angesehen werden. Zu beachten war jedoch, dass die Protokollerklärung lange vor Inkrafttreten der DS-GVO abgegeben worden war.

Ausweislich des Übereinkommens über den Internationalen Suchdienst vom 9. Dezember 2011,[59] das die rechtliche Grundlage für die Arbeit des ITS bildet, handelt es sich um eine Organisation mit internationalem Charakter und Rechts- und Geschäftsfähigkeit in Deutschland (vgl. Art 13 des Übereinkommens). Institutioneller Partner ist das Bundesarchiv.

Normen hinsichtlich der Datenverarbeitung ergeben sich aus Art. 11 Buchst. c) des Übereinkommens über den Internationalen Suchdienst: „Die Nutzung personenbezogener Daten auf der Grundlage von Informationen aus den vom Internationalen Suchdienst in Bad Arolsen zur Verfügung gestellten Originalarchiven und -unterlagen, einschließlich ihrer Verbreitung durch Veröffentlichungen, unterliegt einem Regelwerk, das in vom Internationalen Ausschuss einstimmig beschlossenen Richtlinien niedergelegt wird. Diese Richtlinien berücksichtigen gebührend die Interessen der in Betracht kommenden Person oder Personen und ihrer nahen Angehörigen ebenso wie die Förderung von Forschung und Wissen in Bezug auf den Zeitraum und die Ereignisse, die von den vom Internationalen Suchdienst aufbewahrten Archiven und Unterlagen erfasst werden." Allerdings sind diese Richtlinien nach wie vor noch nicht verabschiedet.

---

58 Anlage A zur Denkschrift zum oben erwähnten Übereinkommen; BR Drs. 179/12, http://dipbt.bundestag.de/dip21/brd/2012/0179-12.pdf.

59 BGBl. 2012 II Nr. 31, S. 1090 ff.

Memorandum des AA und daraus folgende Gespräche

Ein mir vom AA vorgelegtes Memorandum kam auf der Grundlage von Vorgesprächen mit mir nun zu dem Ergebnis, dass die DS-GVO nicht anwendbar ist, weil es sich bei den AA um eine internationale Organisation handelt.

Ich sah das unter Berücksichtigung des Art. 96 DS-GVO grundsätzlich ebenso.

Art. 96 DS-GVO

Internationale Übereinkünfte, die die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen mit sich bringen, die von den Mitgliedstaaten vor dem 24. Mai 2016 abgeschlossen wurde und die im Einklang mit dem an diesem Tage geltenden Unionsrecht stehen, bleiben in Kraft, bis sie geändert, ersetzt oder gekündigt werden.

Allerdings stellte ich im Hinblick auf Art. 11 Buchst. c) des Berliner Abkommens fest, dass es erforderlich ist, Datenverarbeitungsregelungen zu erlassen. Entsprechend dem Abkommen aus dem Jahre 2011 sollte der IA Richtlinien zum Datenschutz erlassen.

Internationaler Ausschuss erlässt Richtlinien und bestimmt Aufsicht

Auf der Grundlage der mit dem AA geführten Gespräche erließ der IA im Rahmen einer Sitzung in Brüssel „Richtlinien zur Datenverarbeitung durch die Arolsen Archives“. Zusätzlich wurde ein Komitee für den Datenschutz eingerichtet, das auf der Grundlage eine Geschäftsordnung tätig ist.

Damit wurde dem Erfordernis, verbindliche und nachvollziehbare Regelungen im Rahmen der Datenverarbeitung durch das internationale Archiv zu schaffen, in nachhaltiger Weise Rechnung getragen.

7. Beschäftigungsverhältnisse

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. Nicht nur diese neuen Bedingungen des Arbeitens in Beschäftigungsverhältnissen fordert eine umfassende Regulierung des Beschäftigtendatenschutzes (Kap. 7.1). Auch ein Urteil des EuGH fordert spezifische Regelungen zum Schutz der Grundrechte der Beschäftigten (Kap. 7.2). Informationstechnik eröffnet auch neue Arbeitsmöglichkeiten und Erleichterungen in der Erbringung von Arbeitsleistungen – wie z. B. beim mobilen Arbeiten –, fordert aber auch neue Datenschutzmaßnahmen (Kap. 7.3). Ebenso ergeben sich im Rahmen des traditionellen Verhältnisses zwischen Beschäftigungsgebern und Beschäftigten neue Datenschutzfragen (Kap. 7.4).

7.1 Neue Regelungen für einen modernen Beschäftigtendatenschutz

Forderungen nach einer umfassenden Kodifizierung des Beschäftigtendatenschutzrechts sind fast so alt wie das Volkszählungsurteil des BVerfG, das in diesem Jahr seinen vierzigsten Geburtstag feiert. Trotz mehrfacher Anläufe gibt es bis heute kein eigenes Beschäftigtendatenschutzgesetz. Die Notwendigkeit der Überarbeitung des aktuellen Rechts ist dabei nicht erst durch die Entscheidung des EuGH in der Rechtssache C-34/21 (s. Kap. 7.2) offenkundig, sondern versteht sich vor dem Hintergrund einer immer schneller voranschreitenden Digitalisierung der Arbeitswelt von selbst.

Zu diesem Ergebnis kommt sowohl der Beirat zum Beschäftigtendatenschutz in seinem Bericht von 2022[60] als auch die DSK. Letztere hatte bereits in ihrer 2014 veröffentlichten Entschließung „Beschäftigtendatenschutzgesetz jetzt!“[61] Regelungen zum Beschäftigtendatenschutzgesetz gefordert und

60 https://www.bmas.de/DE/Service/Presse/Meldungen/2022/bmas-veroeffentlicht-ergebnisse-des-beirats-zum-beschaeftigtendatenschutz.html.

61 https://www.datenschutzkonferenz-online.de/media/en/20140327_en_Beschaeftigtendatenschutzgesetz.pdf.

diese Forderung sodann mit der Entschließung vom 29. April 2022 „Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!"[62] noch einmal erneuert.[63]

Ich begrüße daher, dass das Bundesministerium für Arbeit und Soziales (BMAS) und das Bundesinnenministerium (BMI) im April 2023 erste Vorschläge für einen modernen Beschäftigtendatenschutz vorgelegt haben. Unter den Leitgedanken „Innovation ermöglichen – Persönlichkeitsrechte schützen – Rechtsklarheit schaffen" sollen die im aktuellen Recht bestehenden Probleme und Defizite durch klare, übersichtliche, ausgewogene und technologieneutrale Vorschriften gelöst und behoben werden. Die Vorschläge von BMAS und BMI identifizieren insgesamt zwölf regelungsbedürftige Themenkomplexe:

Sachlicher und persönlicher Anwendungsbereich sollen im Verhältnis zum aktuellen Recht erweitert werden. Für die Eröffnung des sachlichen Anwendungsbereichs soll zukünftig der funktionale Zusammenhang zum Beschäftigungskontext entscheidend sein. Der persönliche Anwendungsbereich soll auch solo-selbstständige Plattformtätige umfassen.

Vor dem Hintergrund der Entscheidung des EuGH in der Rechtssache C-34/21[64] (s. näher Kap. 7.2) sowie der Kritik am generalklauselartigen Charakter des § 26 Abs. 1 Satz 1 BDSG (bzw. des § 23 Abs. 1 Satz 1 HDSIG) sollen in einem neuen Beschäftigtendatenschutzgesetz konkrete Kriterien, etwa zu den Begriffen legitime Zwecke, Dauer, Häufigkeit, Art und Umfang der Verarbeitung und betroffene Beschäftigte festgelegt werden.

Mehr Rechtssicherheit soll bei Einwilligungen durch klare Maßstäbe für die Freiwilligkeit in Abhängigkeit von der jeweiligen Verarbeitungssituation sowie durch die Aufnahme von Fallbeispielen geschaffen werden. Einen ähnlichen Ansatz verfolgen auch die Vorschläge zur Verarbeitung besonderer Kategorien personenbezogener Daten. Auch hier soll anhand typischer Fallgruppen geregelt werden, wann Arbeitgeber sensible Informationen ihrer Beschäftigten verarbeiten dürfen.

In Bewerbungsverfahren sollen klare Anforderungen und praxisnahe Fallbeispiele einen fairen Ausgleich zwischen den Beteiligten bewirken. Die zum Fragerecht des Arbeitgebers von der Rechtsprechung entwickelten Fallgruppen sollen gesetzlich normiert und Voraussetzungen für Tests und Untersuchungen festgeschrieben werden. Erlaubt sein soll lediglich, was für die Feststellung der Eignung erforderlich ist und zudem anerkannten Qua-

62 https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/DSK/2022/2022-DSK-Entschliessung-Beschaeftigtendatenschutz.pdf

63 S. hierzu auch 51. Tätigkeitsbericht, Kap. 11.1 und Horlbeck, Beschäftigtendatenschutz – Brennpunkte und Lösungsansätze, DuD, 2022, 567 ff.

64 EuGH, Urt. v. 30. März 2023 – C-34/21, NZA 2023, 487.

litätsstandards entspricht. Für Informationen zur Eignung und Qualifikation soll der Grundsatz der Direkterhebung gelten.

Medizinische Untersuchungen sollen nur zulässig sein, wenn sie für die Ausübung einer Tätigkeit notwendig oder gesetzlich vorgeschrieben sind. Außerdem wird klargestellt, dass Arbeitgeber einzig über das Ergebnis (geeignet/nicht geeignet) informiert werden sollen.

Für Leistungs- und Verhaltenskontrollen wird die Notwendigkeit der Abwägung zwischen dem berechtigten Interesse des Arbeitgebers (z. B. an der effektiven Aufsicht über den Betrieb) und dem Persönlichkeitsschutzinteresse der Beschäftigten hervorgehoben. Auch hier sollen Beispiele für Abwägungskriterien mehr Rechtssicherheit bewirken und die Handhabung für die Praxis vereinfachen. Konkret benannt werden etwa Abwägungskriterien für dauerhafte Überwachungen. Diese sollen nur ausnahmsweise und unter engen Voraussetzungen möglich sein. Punktuell erforderliche Datenerhebungen in Echtzeit sollen ebenso wie nachvollziehbare Praktiken (z. B. die Erfassung von Lenk- und Ruhezeiten, die Koordinierung wechselnder Arbeitseinsätze oder Disposition) möglich bleiben. Lückenlose Bewegungs- und Leistungsprofile zur Bewertung von Beschäftigten sollen dagegen unzulässig sein. Verdeckte Überwachungsmaßnahmen sollen in Übereinstimmung mit den von der Rechtsprechung entwickelten Grundsätzen möglich bleiben, wenn es keine andere Möglichkeit gibt, den konkreten Verdacht einer Straftat aufzuklären. Für offene Überwachungsmaßnahmen (etwa Videoüberwachung oder Ortung) sollen klare Bedingungen geschaffen werden, z. B. Rückzugsorte und -zeiten ohne Beobachtung. Mit Blick auf die zunehmende Bedeutung von KI in der Arbeitswelt (etwa bei der Bewerberauswahl, Leistungsbeurteilung oder Aufgabenzuweisung) und die mit dem Einsatz einhergehenden Vorteile (Entlastung der Beschäftigten, höhere Effizienz etc.), aber auch Gefahrenpotenziale (z. B. Intransparenz, Diskriminierung oder die Verarbeitung großer Datenmengen) sollen die bestehenden Gestaltungsspielräume ausgeschöpft und Datenschutzrisiken vor allem mit Transparenzregeln begegnet werden.

Zu Fragen des konzerninternen Datentransfers sollen durch die Normierung praxisrelevanter Fallgruppen Rechtssicherheit, Flexibilität und Transparenz gefördert werden. Geprüft wird auch, ob und in welchem Umfang die Nutzung eigener Geräte zur betrieblichen Aufgabenerfüllung (Bring Your Own Device) eigener gesetzlicher Regelungen bedarf, um mehr Rechtssicherheit zu erreichen.

Die Rechte der Betroffenen sollen in Anbetracht der Art. 12 bis 22 DS-GVO punktuell, etwa durch die Festlegung von Löschpflichten für Bewerberdaten, ergänzt werden. Zudem wird über Regelungen zu prozessualen Verwertungsverboten im Falle von unzulässigen Datenverarbeitungen nachgedacht.

Abschließend befassen sich die Vorschläge von BMAS und BMI mit der Fortentwicklung der Mitbestimmung und der Gestaltungsrechte der Beschäftigten. Insbesondere wird die Bedeutung von Betriebsvereinbarungen als betriebsnahes und praxisgerechtes Regelungsinstrument betont und es soll untersucht werden, ob gesetzliche Klarstellungen und Konkretisierungen notwendig sind.

Die im April 2023 von BMAS und BMI vorgestellten Vorschläge befassen sich mit wesentlichen Themenkomplexen, die bereits im Bericht des Beirats zum Beschäftigtendatenschutz und den Entschließungen der DSK adressiert worden sind und Schwerpunkte meiner aufsichtsbehördlichen Praxis bilden. Ich erwarte daher mit Spannung den Entwurf des angekündigten Gesetzes.

7.2
Unionsrechtskonformität der Generalklausel des § 23 Abs. 1 Satz 1 HDSIG?

Am 30.3.2024 entschied der EuGH, dass eine nationale Vorschrift zum Beschäftigtendatenschutz nicht mehr angewendet werden darf, wenn diese nicht mit Art. 88 DS-GVO vereinbar ist. Die nationale Vorschrift, über die der EuGH zu urteilen hatte, war § 23 Abs. 1 Satz 1 HDSIG, der mit § 26 Abs. 1 Satz 1 BDSG identisch ist.

Im Jahr 2020 legte das Hessische Kultusministerium (HKM) fest, dass Schülerinnen und Schüler während der Covid-19-Pandemie per Videokonferenz-Livestream am Unterricht teilnehmen konnten. Die betroffenen Schülerinnen und Schüler bzw. deren Eltern wurden gebeten, eine datenschutzrechtliche Einwilligungserklärung abzugeben. Für die Lehrkräfte war eine solche Einwilligung hingegen nicht vorgesehen. Der Hauptpersonalrat der Lehrerinnen und Lehrer des HKM erhob dagegen Klage und machte geltend, es sei auch eine Einwilligung der betroffenen Lehrkräfte erforderlich. Das HKM äußerte hingegen die Auffassung, dass die Verarbeitung der personenbezogenen Daten von Beschäftigten ohne Einwilligung auf der Grundlage des § 23 Abs. 1 Satz 1 HDSIG erfolgen könne.

§ 23 Abs. 1 Satz 1 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.

Das Verwaltungsgericht Wiesbaden zweifelte an der Vereinbarkeit des § 23 Abs. 1 Satz 1 HDSIG mit Art. 88 DS-GVO und legte dem EuGH die folgenden beiden Fragen zur Vorabentscheidung vor:[65]

> „Ist Art. 88 Abs. 1 DS-GVO dahin auszulegen, dass eine Rechtsvorschrift, um eine spezifischere Vorschrift zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigtenkontext im Sinne des Art. 88 Abs. 1 DS-GVO zu sein, die an solche Vorschriften nach Art. 88 Abs. 2 DS-GVO gestellten Anforderungen erfüllen muss?
>
> Kann eine nationale Norm, wenn diese die Anforderungen nach Art. 88 Abs. 2 DS-GVO offensichtlich nicht erfüllt, trotzdem noch anwendbar bleiben?“

Der Schutz personenbezogener Daten wird in der DS-GVO verbindlich für alle Mitgliedstaaten der EU geregelt. Die Mitgliedstaaten dürfen aber bestimmte Fallgestaltungen aufgrund sogenannter Öffnungsklauseln selbst eigenmächtig regeln. Zu diesen Öffnungsklauseln gehört Art. 88 DS-GVO:

Art. 88 Abs. 1 und 2 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.

65 VG Wiesbaden, Beschluss vom 21. Dezember 2020, AZ 23 K 360/20.WI.PV; https://www.rv.hessenrecht.hessen.de/bshe/document/LARE210000164.

Der EuGH urteilte, dass Art. 88 DS-GVO dahingehend auszulegen ist, dass eine nationale Rechtsvorschrift keine „spezifischere Vorschrift" im Sinne von Abs. 1 dieser Vorschrift sein kann, wenn sie nicht die Vorgaben von Abs. 2 dieses Artikels erfüllt.[66] § 23 Abs. 1 Satz 1 HDSIG wiederholt nach Ansicht des Gerichts lediglich die in Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO aufgestellte Bedingung, dass die Datenverarbeitung für die Erfüllung eines Vertrags erforderlich ist. Sie fügt aber keine spezifischere Vorschrift im Sinne des Art. 88 Abs. 1 DS-GVO hinzu. Außerdem trifft § 23 Abs. 1 Satz 1 HDSIG keine dem Maßstab des Art. 88 Abs. 2 DS-GVO entsprechenden Vorgaben. § 23 Abs. 5 HDSIG verweist zudem – ebenso wie § 26 Abs. 5 BDSG – darauf, dass der Verantwortliche geeignete Maßnahmen ergreifen muss, um sicherzustellen, dass insbesondere die in Art. 5 DS-GVO genannten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden. Eine bloße Wiederholung der Bestimmungen der DS-GVO erfüllt jedoch nicht die Vorgaben des Art. 88 Abs. 2 DS-GVO.[67]

Der EuGH stellt allerdings klar, dass es Sache des nationalen Gerichts ist zu beurteilen, ob § 23 Abs. 1 Satz 1 HDSIG die in Art. 88 DS-GVO vorgegebenen Voraussetzungen und Grenzen beachtet. Eine Entscheidung des aufgrund einer Änderung des HPVG nunmehr zuständigen VG Frankfurt über die Anwendbarkeit von § 23 Abs. 1 Satz 1 HDSIG bleibt abzuwarten.

Um öffentlichen und nichtöffentlichen Stellen im Land Hessen eine Orientierung für die Verarbeitung der personenbezogenen Daten ihrer Beschäftigten zu geben, habe ich meine Rechtsauffassung in der Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023, C-34/21,[68] ausgeführt.[69]

Das Urteil des EuGH macht deutlich, dass ausführlichere gesetzliche Regelungen zum Beschäftigtendatenschutz geboten sind. Vor diesem Hintergrund ist es zu begrüßen, dass die Bundesregierung in ihrem Papier „Fortschritt durch Datennutzung" angekündigt hat, das seit langem geplante Beschäf-

66 Urteil vom 30. März 2023, C-34/21, Rn. 75 – Hauptpersonalrat der Lehrerinnen und Lehrer, https://curia.europa.eu/juris/document/document.jsf?text=&docid=272066&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1.

67 Urteil vom 30. März 2023, Rs. C-34/21 Rn. 65.

68 https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-05/handreichung_beschaeftigtendatenschutz_eugh-urteil.pdf.

69 S. hierzu auch ausführlich Roßnagel/Wetzstein/Horlbeck, Unionsrechtliche Vorgaben für das Recht des Beschäftigtendatenschutzes – Auswirkungen des EuGH-Urteils vom 30.3.2023, Datenschutz und Datensicherheit (DuD) 2023, 429–434.

tigtendatenschutzgesetz nun zeitnah umzusetzen.[70] Weitere Informationen zu einem neuen Beschäftigtendatenschutzgesetz sind in Kap. 7.1 zu finden.

7.3
Arbeitnehmer allein zu Haus? – Datenschutzkonformes Arbeiten im hauseigenen Büro

Nach Veröffentlichungen des Statistischen Bundesamtes arbeiten fast ein Viertel aller Erwerbstätigen von zu Hause. Auch das mobile Arbeiten gewinnt in der modernen Arbeitswelt zunehmend an Bedeutung. Dabei gilt: Die Gewährleistung einer datenschutzkonformen Datenverarbeitung ist keine Frage des Arbeitsortes, sondern muss vom Verantwortlichen ortsunabhängig gewährleistet werden. Im Berichtszeitraum habe ich auf meiner Webseite datenschutz.hessen.de eine Handreichung veröffentlicht, die Verantwortlichen und Beschäftigten insoweit Hilfestellung geben soll.

Für das Arbeiten im Homeoffice und das mobile Arbeiten gelten die Regelungen der DS-GVO und des BDSG. Spezielle Regelungen gibt es nicht. Arbeitgeberinnen und Arbeitgeber bleiben beim Arbeiten im Homeoffice und beim mobilen Arbeiten daher Verantwortliche im Sinne der DS-GVO und sind für die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten rechenschaftspflichtig. Dem Grundsatz der Integrität und Vertraulichkeit kommt dabei besondere Bedeutung zu: Personenbezogene Daten müssen durch geeignete technische und organisatorische Maßnahmen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

In meiner Handreichung habe ich Tipps und weiterführende Informationen zu technischen und organisatorischen Maßnahmen zusammengestellt, um im Zusammenhang mit dem Arbeiten im Homeoffice und dem mobilen Arbeiten ein dem Risiko angemessenes Schutzniveau zu gewährleisten.[71]

---

70 Roadmap Datenstrategie bis Q4/2024, https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.pdf;jsessionid=E4FDCBFB0B3BEB794831DDFAFCF41315.1_cid350?__blob=publicationFile&v=2, S. 37.

71 https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2024-01/handreichung_zum_mobilen_arbeiten_231221.pdf.

7.4
Datenschutzrechtliche Grenzen für mitteilsame Arbeitgeber

Auch in streitigen Arbeitsverhältnissen besteht eine Wohlwollenspflicht des Arbeitgebers. Eine datenschutzrechtliche Grenze wird dann überschritten, wenn eine Mitteilung an die Belegschaft in das Persönlichkeitsrecht eines Mitarbeiters eingreift.

Ein Beschäftigter bat mich um datenschutzrechtliche Prüfung und Bewertung einer von seinem Arbeitgeber an die Beschäftigten versandten E-Mail. Sinngemäß enthielt die Nachricht des Arbeitgebers folgenden Inhalt:

> „Geschätzte Kolleginnen und Kollegen,
>
> wir sind kurzfristig und bis zum Abschluss des Kündigungsschutzverfahrens durch ein Urteil des Arbeitsgerichts (…), gegen das Berufung eingelegt wurde, verpflichtet worden, Herrn (…) weiter zu beschäftigen. Seine Arbeitsaufträge wird er ausschließlich von (…) erhalten und alleine ausführen. Diese Nachricht dient lediglich Eurer Information.
>
> Freundliche Grüße (…)“

Der Betroffene fühlte sich in seinen Rechten verletzt. Er führte insbesondere aus, dass kein Erfordernis bestanden habe, die Kolleginnen und Kollegen über Details des Arbeitsgerichtsverfahrens zu informieren. Aufgrund der Beschwerde habe ich den Arbeitgeber angehört und zur Stellungnahme aufgefordert. Hierbei habe ich ausgeführt, dass ich die Bedenken des Betroffenen teile, und nach Sinn und Zweck der streitgegenständlichen E-Mail an das Kollegium gefragt.

Der Verantwortliche räumte auf meine Anhörung hin ein, dass der Hinweis auf den Ausgang des Arbeitsgerichtsverfahrens gegenüber den Kollegen nicht erforderlich gewesen sei. Wegen massiver persönlicher Vorkommnisse habe zur Wahrung des Betriebsfriedens vorläufig jedoch der Kontakt zum „alten Team“ vermieden werden sollen. Daher sei die betroffene E-Mail an die Beschäftigten versandt 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“). Zu diesen Grundprinzipien gehört gemäß Art. 5 Abs. 1 Buchst. a DS-GVO auch der Grundsatz der Rechtmäßigkeit. Daher war zum einen zu prüfen, ob die Datenverarbeitung auf eine Rechtsgrundlage gestützt werden konnte.

Dies ist dann der Fall, wenn mindestens einer der in Art. 6 Abs. 1 UAbs. 1 Buchst. a bis f DS-GVO genannten Erlaubnistatbestände Anwendung findet.

Meine Prüfung ergab, dass als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten des Betroffenen entweder Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO (Erforderlichkeit der Verarbeitung zur Erfüllung eines Vertrags) oder Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO (Wahrung berechtigter Interessen des Verantwortlichen) in Betracht kam.

Die aufgrund der Öffnungsklausel des Art. 88 DS-GVO für Beschäftigte erlassene spezifische Rechtsvorschrift des § 26 Abs. 1 Satz 1 BDSG wurde nicht geprüft, da mit Blick auf das Urteil des EuGH vom 30. März 2023 (C-34/21) (s. Kap. 7.2) die Europarechtskonformität der Norm umstritten ist.

Art. 6 Abs. 1 DS-GVO

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

(…)

b) Die Verarbeitung ist für die Erfüllung eines Vertrags (…) erforderlich (…)

(…)

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 (…).

Zwar erfolgte die Verarbeitung der personenbezogenen Daten des Betroffenen (hier in Form des Versandes der E-Mail an die Kollegen) zur Durchführung des mit dem Betroffenen bestehenden Arbeitsverhältnisses und damit in Erfüllung eines Vertrages im Sinne von Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO. Die Verarbeitung war aber zur Erfüllung dieses Zwecks nicht erforderlich, da etwa eine entsprechende Anweisung an den Betroffenen selbst sowie eine adäquate Auswahl der Arbeitsaufträge ebenso geeignet gewesen wären, den seitens des Arbeitgebers verfolgten Zweck zu erreichen. Hier bestand kein Erfordernis, die Beschäftigten über den Ausgang des Arbeitsgerichtsverfahrens und darüber, dass der Mitarbeiter seine Arbeitsaufträge künftig alleine auszuführen habe, zu unterrichten.

Bei jeder Prüfung der Erforderlichkeit ist außerdem eine Abwägung zwischen dem Persönlichkeitsrecht des Betroffenen sowie die Auswirkungen der Datenverarbeitung hierauf einerseits und den berechtigten Interessen des Verantwortlichen andererseits. Durch die Mitteilung wurde der Mitarbeiter diskreditiert und an den Pranger gestellt, wodurch ihm die Fortführung des Beschäftigungsverhältnisses durchzuführen gehörig erschwert wurde. Die

E-Mail bedeutete insoweit einen erheblichen Eingriff in sein Persönlichkeitsrecht und einen schweren Start für einen Neuanfang.

Liegen schon die Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO mangels Erforderlichkeit der Datenverarbeitung nicht vor, können auch die insoweit höheren Anforderungen des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO nicht gegeben sein. Die Vorschrift verlangt nämlich nicht nur, dass die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich ist, sondern zusätzlich, dass die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, nicht überwiegen.

Insgesamt war die E-Mail als rechtswidrig zu bewerten. Die Beschwerde wurde mit einer Verwarnung gem. Art. 58 Abs. 2 Buchst. b DS-GVO gegenüber dem Arbeitgeber als Verantwortlichem abgeschlossen. Beschäftigte dürfen darauf vertrauen, dass sie von mir Unterstützung erfahren, wenn durch rechtswidrige Mitteilungen an unberechtigte Dritte ihr Persönlichkeitsrecht verletzt wird.

8. Internet und Medien

Die Bedeutung des Internets für das gesellschaftliche Zusammenleben, für die wirtschaftliche Betätigung und die Erfüllung von Verwaltungsaufgaben wird immer wichtiger. Daher nimmt auch die Bedeutung des Datenschutzes in der virtuellen Welt zu. Diese wird durch die Nutzung von Künstlicher Intelligenz und insbesondere von selbstlernenden Systemen wie Large Language Models tiefgreifend verändert. Erste Eindrücke der Chancen, aber auch der Risiken durch Künstliche Intelligenz lassen sich am Beispiel von ChatGPT gewinnen (Kap. 8.1). Um Datenschutzprobleme ihrer invasiven Datenerhebung und -verarbeitung zu umgehen, bieten Social Networks Abo-Modelle als Alternative ohne Werbung an (Kap. 8.2). Aber auch eigentlich geklärte Fragen des Datenschutzes im Internet wie etwa die Pflicht zur Transport-Verschlüsselung bei Datenerhebung im WWW (Kap. 8.3) oder die Pflicht zu einer elektronischen Auskunftserteilung im Falle elektronischer Antragstellung (Kap. 8.4) stellen sich für die Datenschutzaufsicht immer wieder neu. Betroffenen Personen fällt es oft schwer nachzuvollziehen, warum bestimmte Datenschutzregelungen gegenüber Medien nicht gelten. Art. 85 DS-GVO fordert jedoch für die Medien rechtliche Sonderbehandlungen, um einen Ausgleich zwischen den Grundrechten auf Medienfreiheit und Datenschutz zu gewährleisten (Kap. 8.5).

8.1 Datenschutz bei generativer Künstlicher Intelligenz

Ende 2022 hat das Unternehmen OpenAI den Dienst ChatGPT für die Öffentlichkeit verfügbar gemacht und damit einen regelrechten Hype ausgelöst. Die Fähigkeiten von generativer Künstlicher Intelligenz (KI) wie z. B. ChatGPT sind zumindest auf den ersten Blick sehr beeindruckend. Allerdings bringt deren Einsatz auch verschiedene tatsächliche und rechtliche Schwierigkeiten mit sich – eine davon ist die Erfüllung datenschutzrechtlicher Pflichten.

Generative Künstliche Intelligenz

Der Begriff der Künstlichen Intelligenz, der bis in die 1950er Jahre zurückreicht, ist nicht einheitlich definiert und umfasst ein sehr weites Feld unterschiedlicher Algorithmen, IT-Anwendungen und IT-Dienste. Bereits dies erschwert den Umgang mit KI auch aus datenschutzrechtlicher Sicht, da von unterschiedlichsten IT-Anwendungen gesprochen werden kann, wenn es um den Einsatz von KI geht. Allen Definitionen gemeinsam ist, dass das Ziel von KI im Wesentlichen die Annäherung der Datenverarbeitung an die menschliche Intelligenz aus Sicht des menschlichen, rationalen Denkens und Handelns

ist. Um dieses weite Themenfeld einzugrenzen, konzentriere ich mich im Folgenden auf Verfahren des maschinellen Lernens und insbesondere auf die derzeit in der öffentlichen Diskussion stehenden, auf neuronalen Netzen aufbauenden generativen KIs und großen Sprachmodellen (Large Language Models – LLM). Diese Konzepte unterscheiden sich grundlegend von der klassischen Vorstellung der Datenverarbeitung, die im Wesentlichen darauf basiert, Eingaben zu verarbeiten, die in einem vorgegebenen und vorhersehbaren Rahmen angenommen werden, und mit vorher programmierten Ausgaben darauf zu reagieren.

LLMs werden mit riesigen Mengen bereits bestehender Texte z. B. aus dem Internet trainiert. Jeder Satz, der während des Trainings verwendet wird, sorgt dafür, dass im Lernprozess die sogenannten Parameter zwischen den einzelnen, der unzähligen künstlichen Neuronen in den neuronalen Netzen, die aus vielen Schichten miteinander verbundener sogenannter Neuronen bestehen, verändert und angepasst werden. Durch Hunderte von Milliarden solcher Parameter werden sowohl die Position in einem Satz als auch die Gewichtung einzelner Worte berücksichtigt, so dass Eigenarten des Aufbaus, der Zusammensetzung von Texten und der jeweiligen Sprache berücksichtigt werden. Die gelernten (personenbezogenen) Daten sind somit nicht als solche irgendwo gespeichert, können von der KI aber anhand der erlernten Parameter generell wieder reproduziert werden.

Anders als bei klassischen datenbankbasierten Anwendungen speichert eine generative KI die gelernten Daten – wie z. B. Namen oder Sätze – nicht in herkömmlicher Weise ab. Vielmehr ermittelt sie mathematisch unter Berücksichtigung der semantischen Zusammenhänge der Eingabe die Wahrscheinlichkeit des jeweils nächsten Wortes. Sie würde z. B. ermitteln, dass im Zusammenhang mit klassischer Musik das Wort „Ludwig“ vorkommt und wiederum mit extrem hoher Wahrscheinlichkeit darauf das Wort „van“ und darauf „Beethoven“ folgt. Der Name „Ludwig van Beethoven“ als Ganzes wäre hingegen nicht buchstäblich im neuronalen Netz der LLM gespeichert. Das System hat kein Weltwissen. Es weiß weder, was Musik ist, noch, wer Beethoven war. Es hat aber gelernt, menschliche Sprache anhand statistischer Wahrscheinlichkeiten so zu imitieren, dass es mit uns über die Musik Beethovens „sprechen“ kann.

Zusammen mit weiteren, in den IT-Anwendungen der LLMs eingesetzten Algorithmen befähigt diese Fähigkeit die Anwendungen dazu, frei formulierte Eingaben eines Nutzers richtig zu interpretieren und als Antwort darauf passende, teilweise auch sehr lange und komplexe Texte zu generieren. Deren Inhalt basiert wiederum auf den im Training zum jeweiligen Kontext hergestellten Verknüpfungen.

Entsprechende Anwendungen bieten ungeheures Potenzial zur Automatisierung aller möglichen text- oder sprachbasierten Tätigkeiten, vom Abfassen von journalistischen Texten oder dienstlichen Vermerken über die Kommunikation z. B. im Kundendienst bis hin zur Erstellung grundlegend neuer Ideen und Konzepte. Dementsprechend viele mögliche Anwendungsfälle sind denkbar und dementsprechend gefragt sind vergleichbare Anwendungen bereits jetzt.

Mit diesen Fähigkeiten gehen aber auch zum Teil erhebliche Probleme einher. Da für die Adressaten oftmals nicht erkennbar ist, dass sie einen generierten Text lesen, besteht eine große Gefahr für Manipulation und Desinformation. So besteht insbesondere die Gefahr, dass falsche oder durch sogenannte Halluzinationen erzeugte Informationen durch die KI dem menschlichen Nutzer überzeugend dargestellt und damit als richtig suggeriert werden. Sind in den Trainingsdaten – offen oder versteckt – Vorurteile eingebettet, besteht eine hohe Wahrscheinlichkeit, dass auch die Antworten des Sprachmodells unzulässige Diskriminierungen enthalten. Da eine KI weder Emotionen noch ethische Werte kennt, können auch stark beleidigende oder gar hasserfüllte Ausgaben erfolgen, solange dies nur bestimmten, von der KI erlernten Mustern folgt. Und nicht zuletzt können je nach Inhalt und Qualität der Trainingsdaten auch Verarbeitungen erfolgen, die auf unzulässiger Nutzung von beispielsweise urheberrechtlich geschützten Werken oder personenbezogenen Daten basieren.

Datenschutzrechtliche Fragestellungen

Im Zuge der fortschreitenden Digitalisierung und des vermehrten Einsatzes Künstlicher Intelligenz (KI) sind datenschutzrechtliche Fragestellungen von essenzieller Bedeutung. Die Datenschutzaufsichtsbehörde hat im aktuellen Berichtszeitraum verstärkt den Fokus auf die Herausforderungen gerichtet, die mit dem Einsatz von KI-Technologien einhergehen. Insbesondere stellen sich Fragen zur Transparenz und Nachvollziehbarkeit von KI-Entscheidungen, da komplexe Algorithmen oft schwer verständlich sind. Auch die rechtmäßige Verarbeitung personenbezogener Daten im Kontext von KI-Anwendungen erfordert besondere Aufmerksamkeit, um sicherzustellen, dass Datenschutzprinzipien wie Zweckbindung und Datenminimierung gewahrt bleiben. Ein weiterer zentraler Aspekt ist die Sicherheit der Datenverarbeitung, um potenzielle Risiken für die informationelle Selbstbestimmung der Betroffenen zu minimieren. Die Datenschutzaufsichtsbehörde hat in diesem Berichtszeitraum verstärkte Anstrengungen unternommen, Unternehmen und Organisationen bei der Implementierung von Datenschutzmaßnahmen im Kontext von Künstlicher Intelligenz zu unterstützen und auf bestehende rechtliche Rahmenbedingungen hinzuweisen. Der Schutz der Privatsphäre

und die Einhaltung datenschutzrechtlicher Vorgaben sind in einer zunehmend von KI geprägten Welt von entscheidender Bedeutung, und die Datenschutzaufsichtsbehörde wird auch zukünftig proaktiv agieren, um diesen Herausforderungen gerecht zu werden.

Generative KI ist, zumindest als praktisch nutzbare und breit verfügbare Anwendung, noch sehr jung. Da sich die Verarbeitung von Daten dabei recht grundlegend von der herkömmlichen, auf Datenbanken basierenden Verarbeitung unterscheidet, sind viele datenschutzrechtliche Fragen bisher noch nicht hinreichend beantwortet.

Eine rechtlich wie auch technisch spannende Frage, die zugleich die Anwendbarkeit des Datenschutzrechts an sich betrifft, ist die Frage, ob die beim Training einer generativen KI verwendeten personenbezogenen Daten von der KI gespeichert oder anderweitig verarbeitet werden. Angesichts der weiten Definition der Verarbeitung von Daten in Art. 4 Nr. 2 DS-GVO spricht aber vieles dafür, dass auch die oben beschriebene Form der Verarbeitung grundsätzlich gemäß Art. 2 Abs. 1 DS-GVO vom Datenschutzrecht erfasst ist.

Schwierig ist zudem auch die Frage nach der datenschutzrechtlichen Verantwortlichkeit. Die Entwicklung und das Training von KI-Basis-Modellen verantworten zweifellos deren Entwickler und Anbieter. Auf diesen Basis-Modellen bauen wiederum verschiedene Dienste auf, die zu der jeweiligen Basis zusätzliche Fähigkeiten, Einschränkungen oder sonstige Besonderheiten ergänzen und damit Einfluss auf die Datenverarbeitung durch die KI nehmen. Schließlich lösen auch die Nutzenden Verarbeitungsvorgänge aus, die mit personenbezogenen Daten verbunden sind, indem sie solche in Anfragen an die KI eingeben oder als Antworten auf ihre jeweiligen Anfragen erhalten. Wie sich das Zusammenspiel dieser Akteure in rechtlicher Form bezüglich der Verantwortlichkeit abbildet, hängt vom jeweiligen Einzelfall und von der technischen Gestaltung der KI sowie der rechtlichen Gestaltung im Nutzungsverhältnis ab. Dabei kann es sowohl einen einzelnen Verantwortlichen geben, möglich sind aber auch gemeinsame Verantwortlichkeiten der Beteiligten sowie Auftragsverarbeitungsverhältnisse.

Fraglich ist weiterhin auch der Umgang mit den Betroffenenrechten, also beispielsweise mit den Rechten auf Berichtigung, Löschung oder Auskunft von personenbezogen Daten. Die Tatsache, dass die zum Training verwendeten, ggf. auch personenbezogenen Daten nicht in abstrakt nachvollziehbarer Form gespeichert werden und damit nicht einfach abgerufen, geändert oder gelöscht werden können, erschwert die Geltendmachung von Betroffenenrechten erheblich. Die einer KI einmal antrainierten Daten im Nachhinein zu beeinflussen, ist schwer möglich, da sich mit dem Training neuronale Verknüpfungen gebildet haben, die sich in aller Regel nicht vollständig rück-

gängig machen lassen dürften. Eine denkbare Lösung für dieses Problem wäre jedoch das sog. AI-Alignment. Entsprechende Verfahren zielen darauf ab, KI-Systeme so zu lenken, dass sie im Einklang mit menschlichen Zielen, Präferenzen oder ethischen Grundsätzen handeln. Auf diese Weise könnten das Training und die Ausgaben der KI vorab beeinflusst oder nachträglich abgeändert werden, um zumindest die Wiedergabe unangemessener oder beispielsweise datenschutzrechtlich unzulässiger Inhalte zu verhindern.

Auch noch weitgehend ungeklärt, letztlich aber auch von der Gestaltung des jeweiligen Dienstes abhängig ist der Umgang mit den bei der Nutzung der KI anfallenden Daten der sie Nutzenden. Da die KI zur Weiterentwicklung und Verbesserung auf beständiges Training mit neuen Texteingaben angewiesen ist, dürfte es für viele Anbieter naheliegen, auch die Eingaben der Nutzenden zu diesem Zweck zu verwenden. Zudem ermöglicht dieses Vorgehen auch, die Antworten der KI mit der Zeit zu individualisieren und stärker auf die Vorstellungen der einzelnen Nutzenden abzustimmen. Auch die Anfragen enthalten aber häufig personenbezogene Daten und lassen unter Umständen weitgehende Rückschlüsse auf die nutzende Person und deren Lebensumstände zu. Äußerst problematisch wäre es beispielsweise, wenn häufige Eingaben einer Person und entsprechendes Lernen der KI dazu führen würden, dass die gelernten Informationen auch anderen Nutzenden in Form von generiertem Text zur Verfügung gestellt würden.

Umgang mit diesen Herausforderungen

Angesichts der vielen offenen Fragen im Zusammenhang mit generativer KI habe ich, gemeinsam und inhaltlich abgestimmt mit mehreren anderen deutschen Datenschutzaufsichtsbehörden, im Berichtszeitraum eine Prüfung des Dienstes ChatGPT und dessen Anbieters OpenAI eingeleitet. Da das Unternehmen im Berichtszeitraum seinen einzigen Sitz in den USA hatte und von dort aus seine Dienste auch Nutzern in der EU anbot, waren alle europäischen Datenschutzaufsichtsbehörden gleichermaßen zuständig, die Rechtmäßigkeit der Datenverarbeitung durch das Unternehmen zu überprüfen.

Dem Unternehmen wurden weitreichende Fragen gestellt, um die Hintergründe der Datenverarbeitung und den Umgang mit personenbezogenen Daten bei dem Dienst besser einschätzen und rechtlich bewerten zu können. Die Prüfung war zum Ende des Berichtszeitraums noch nicht abgeschlossen, es zeigten sich jedoch bereits einige Eigenschaften, die weiteres kritisches Nachfragen erfordern.

Durch die in der DS-GVO geregelte enge und koordinierte Zusammenarbeit der europäischen Datenschutzbehörden ist ein konsistentes weiteres Vorgehen auch dann sichergestellt, wenn das Unternehmen eine Niederlassung in

der EU gründet, welche die Verarbeitung der Daten europäischer Nutzender verantwortet.

Wer generative KI in seinem Arbeitsumfeld einsetzen möchte, sei es in einem Unternehmen oder auch in öffentlichen Stellen, ist mit der schwierigen Aufgabe konfrontiert, dies in einem datenschutzrechtlich verantwortbaren Rahmen zu tun. Nicht nur, aber auch aus datenschutzrechtlicher Sicht sind viele Fragen zur Nutzung von KI und den dadurch möglicherweise entstehenden Folgen noch nicht abschließend geklärt. Sie können damit auch von den ggf. rechtlich verantwortlichen KI-Nutzenden selbst (noch) nicht hinreichend beantwortet werden und bergen rechtliche Risiken. Dies gilt neben dem Datenschutzrecht auch für andere Rechtsgebiete wie z. B. die gewerblichen Schutzrechte, das Zivil- oder das Arbeitsrecht. Insofern ist grundsätzlich zu einem umsichtigen und bedachten Vorgehen zu raten.

In jedem Fall sollte beim Einsatz von LLM durch geeignete und angemessene Maßnahmen den o. g. Risiken adäquat begegnet und so das Risiko für das Persönlichkeitsrecht auf ein akzeptables Maß reduziert werden. So sollten schon bei der Auswahl eines bestimmten KI-Anbieters datenschutzrechtliche Fragen von Anfang an bedacht und darauf geachtet werden, ob dieser zufriedenstellende Antworten auf die o. g. Problembereiche geben kann. Wenn grundsätzliche Bedenken bei Fragen der Rechtmäßigkeit der Datenverarbeitung, der Verantwortlichkeit, dem Umgang mit Nutzerdaten oder Betroffenenrechten oder auch der Übermittlung von Daten in Drittstaaten außerhalb der EU bestehen, sollte vom Einsatz einer solchen Anwendung bis zur Klärung der offenen Fragen abgesehen werden.

Auch bei der Gestaltung des Rechts- bzw. Nutzungsverhältnisses mit dem Anbieter der KI ist auf datenschutzrechtliche Belange zu achten. So sollte beispielsweise die datenschutzrechtliche Verantwortlichkeit in angemessener Form zwischen den Beteiligten verteilt und die mögliche Geltendmachung von Betroffenenrechten gewährleistet sein. Ebenso ist sicherzustellen, dass Nutzerdaten nicht in unzulässiger Weise erhoben und verarbeitet werden und der Umfang der Datenverarbeitung für die Nutzer transparent und nachvollziehbar dargestellt wird. Innerhalb der KI-Anwendung sollten möglichst datenschutzfreundliche Einstellungen getroffen werden.

Um datenschutzrechtlichen und weiteren rechtlichen Risiken zu begegnen, sollten die Ergebnisse der KI in jedem Fall einer hinreichenden und dem Risiko der jeweiligen Verarbeitung angemessenen menschlichen Kontrolle unterzogen werden. Beim derzeitigen Entwicklungsstand von KI-Anwendungen ist dies dringend erforderlich, um falsche, unangemessene oder auch rechtlich angreifbare Ergebnisse der KI zumindest korrigieren zu können. Zu Recht verbietet Art. 22 Abs. 1 DS-GVO ausdrücklich, dass Personen

einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen werden, wenn sie ihnen gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Bei nicht nur nebensächlichen Dingen sollte niemand ohne ein menschliches Korrektiv der alleinigen Entscheidung einer Maschine ausgesetzt sein, mag sie auch noch so intelligent erscheinen.

Quod erat demonstrandum

Haben Sie bemerkt, welcher Teil dieses Beitrags von einer generativen KI geschrieben wurde? Es ist der erste Absatz unter der Überschrift „Datenschutzrechtliche Fragestellungen" – von „Im Zuge der fortschreitenden Digitalisierung …" bis „… um diesen Herausforderungen gerecht zu werden". Generiert wurde dieser Absatz von ChatGPT auf die Aufforderung hin:

> *„Schreibe einen Absatz über ca. 10 Zeilen für einen Beitrag in einem Tätigkeitsbericht einer Datenschutzaufsichtsbehörde zu der Frage, welche datenschutzrechtlichen Fragestellungen sich beim Einsatz von Künstlicher Intelligenz ergeben."*

Sicherlich ist dieser Absatz inhaltlich etwas unspezifisch und generalisierend. Dennoch muss man anerkennen, dass die darin von der KI getroffenen Aussagen nicht grundsätzlich falsch sind. Da ChatGPT glücklicherweise nicht über die genauen Tätigkeiten meiner Behörde informiert ist, kann es keine spezifischen Aussagen zur Tätigkeit der „Datenschutzbehörde im Berichtszeitraum" treffen. Die diesbezüglichen Aussagen sind jedoch so allgemein gehalten, dass sie im Ergebnis wiederum weitgehend zutreffen. Tatsächlich bildeten der Umgang mit KI, die Prüfung von ChatGPT und die entsprechende Beratung von (insbesondere) öffentlichen Stellen durchaus einen Schwerpunkt meiner Tätigkeit im Berichtszeitraum.

Zweifellos wird das Thema Künstliche Intelligenz auch die zukünftige Tätigkeit des HBDI maßgeblich beeinflussen.

8.2
Abo-Modelle für Social Networks?

Social Networks bieten neuerdings – ähnlich wie in der elektronischen Presse – Abo-Modelle an, um Nutzenden eine Alternative zu ihrem bisherigen Geschäftsmodell zu bieten, das Verhalten der Nutzenden im Internet zu tracken, die Verhaltensdaten zu Persönlichkeitsprofilen zusammenzuführen und unter Verwendung dieser Profile den Nutzenden individualisierte Werbung

anzuzeigen. Sie erhoffen sich damit eine Legitimation ihrer Datenverarbeitung durch eine Einwilligung der betroffenen Personen. Diese Hoffnung ist jedoch datenschutzrechtlich unbegründet.

Schon seit vielen Jahren Dauerbrenner in der Praxis der Datenschutzaufsicht sind der Einsatz von Cookies und die Einbindung von Drittanbieter-Diensten in Telemedien. Die meisten Anbieter binden in ihre Websites und Apps verschiedene von anderen Unternehmen erbrachte Dienste ein, die vor allem der Webanalyse, der Einbindung bestimmter Inhalte (z. B. Karten, Videos, Social-Media-Postings) und dem Ausspielen von Werbung dienen. Dies ist immer auch mit der Verarbeitung von personenbeziehbaren Daten und oft auch mit der Bildung von Nutzerprofilen verbunden und erfordert somit eine datenschutzrechtliche Rechtsgrundlage. Als solche kommt, auch vor dem Hintergrund des § 25 TTDSG, in aller Regel nur eine Einwilligung in Betracht, die üblicherweise mittels eines Cookie-Banners eingeholt wird. In diesem Zusammenhang ergeben sich verschiedene datenschutzrechtliche Fragen und Probleme, beispielsweise zur Erforderlichkeit der Einwilligung, zu ihrer konkreten Ausgestaltung und Reichweite, zur Zulässigkeit des Einsatzes bestimmter Dienste, zur optischen Gestaltung des Cookie-Banners oder zu Einzelheiten der jeweiligen technischen Umsetzung.

Dieses datenschutzrechtliche Problem hat insofern eine neue Ausprägung gefunden, als zunehmend Abo-Modelle als Alternative zur datenschutzrechtlichen Einwilligung angeboten werden. Betreiber von Websites, insbesondere Medienunternehmen, sind seit einiger Zeit dazu übergegangen, den Inhalt ihrer Websites und Nachrichtenportale entweder gegen eine Einwilligung in Tracking und personalisierte Werbung oder gegen den Abschluss eines kostenpflichtigen Abonnements (sog. Pur-Abonnement) anzubieten. Soweit sich die Besucher der Seiten für den Abschluss eines Pur-Abos entscheiden, entfällt das Tracking zu Werbezwecken, das bei vielen Angeboten die Grundlage für ihre Finanzierung bildet.

Soweit zum Angebot einer individuellen Werbeansprache personenbezogene Daten verarbeitet werden, ist eine Kontrolle mit Blick auf datenschutzrechtliche Anforderungen angezeigt. Nachdem sich eine Arbeitsgruppe des Arbeitskreises Medien der DSK intensiv mit den Abo-Modellen von Medienunternehmen auseinandergesetzt hatte, hat die DSK in ihrem Beschluss vom 22. März 2023[72] eine Bewertung dieser Modelle vorgenommen und die datenschutzrechtlichen Anforderungen an diese Modelle erläutert. Eine datenschutzrechtlich zulässige Umsetzung des Abo-Modells ist danach

72 https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf.

grundsätzlich möglich, erfordert aber die Beachtung einiger Vorgaben. So muss beispielsweise sichergestellt sein, dass der Umfang der Einwilligung für die Nutzer klar erkennbar und transparent ist und dass verschiedene Zwecke nicht in unzulässiger Weise miteinander verknüpft werden.

Auch der Internetkonzern Meta, der u. a. die sozialen Netzwerke Facebook und Instagram betreibt, ist im Berichtszeitraum dazu übergegangen, seinen Nutzern werbefreie Zugänge für diese Netzwerke gegen die Zahlung einer monatlichen Abo-Gebühr anzubieten. Alternativ besteht weiterhin die Möglichkeit zur kostenlosen Nutzung, wenn eine Einwilligung in die Verarbeitung der Nutzerdaten zu Werbezwecken erteilt wird. Damit reagiert Meta auf eine Entscheidung der irischen Datenschutzaufsicht (DPC), die für die europäischen Aktivitäten von Meta zuständig ist. Die DPC hatte Meta untersagt, im Wege von Allgemeinen Geschäftsbedingungen die Verarbeitung von personenbezogenen Daten für personalisierte Werbung zu einer von den Nutzern ausdrücklich gewünschten und vertraglich vereinbarten Dienstleistung zu erklären. Allerdings stellt diese Form der Datenverarbeitung tatsächlich einen wesentlichen Anteil des Geschäftsmodells von Meta dar. Das Angebot zum Abschluss eines werbefreien Abonnements soll daher den Verlust von Einnahmen aus dem Werbegeschäft reduzieren. Im Gegensatz zu den Erwartungen der Nutzer trackt Meta aber auch bei Abschluss eines werbefreien Abonnements das Verhalten der Nutzer, so dass das kostenreiche Abo keinen datenschützenden Vorteil bietet. Da Meta über diese Konsequenz nicht ausdrücklich und unmissverständlich informiert, ist die „Einwilligung" datenschutzrechtlich unwirksam.

Die weitere Entwicklung dieses Themas werde ich, auch im Wege der Zusammenarbeit mit anderen europäischen Aufsichtsbehörden sowie im Rahmen von eigenen Prüfungen, eng begleiten.

8.3
Pflicht zur Transport-Verschlüsselung bei Datenerhebung im WWW

Die DS-GVO verpflichtet seit nunmehr über fünf Jahren Verantwortliche dazu, den Grundsatz der Integrität und Vertraulichkeit bei der Verarbeitung personenbezogener Daten zu beachten. Zudem wird in der DS-GVO konkret festgelegt, dass die Verschlüsselung personenbezogener Daten als technische Maßnahme zur Einhaltung dieses Grundsatzes geeignet ist und unter bestimmten Bedingungen zur Anwendung gelangen soll. Dennoch erheben einige Anbieter von Telemedien online über Kontakt-, Registrierungs- und Anmeldeformulare im WWW immer noch aktiv Daten von Nutzern, ohne eine TLS-Transportverschlüsselung in ihr Online-Angebot zu implementieren.

Viele Anbieter von Websites erheben im Rahmen ihres Online-Angebots über Online-Formulare personenbezogene Daten zu Zwecken der Registrierung, der persönlichen Anmeldung oder um den Nutzern die Möglichkeit zu geben, Fragen zu Produkten und Dienstleistungen zu äußern. Bei diesen Datenerhebungen über Kontakt-, Registrierungs- oder Anmeldeformulare im WWW werden immer auch personenbezogene Daten wie z. B. Namen, E-Mail-Adressen, Postanschriften, Geburtsdaten und Zugangsdaten der Seitennutzer verarbeitet. Dabei sind die Vorgaben der DS-GVO zur Datensicherheit, insbesondere zur Integrität und Vertraulichkeit aus Art. 5 Abs. 1 Buchst. f DS-GVO von den Anbietern zu beachten. Dieser Grundsatz wird durch die Sicherheitsvorgaben in Art. 32 Abs. 1 Buchst. a DS-GVO konkretisiert:

Art. 5 DS-GVO

(1) Personenbezogene Daten müssen

(…)

f) 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“)

(…)

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;

(…)

Die Implementierung eines entsprechenden Zertifikats für das Angebot von Datenerhebungsformularen auf Websites und somit die Verschlüsselung der Datenübermittlung zwischen Seitennutzer und Anbieterserver mittels eines TLS-Protokolls, entspricht dem Stand der Technik und wird auch vom Bundesamt für die Sicherheit in der Informationstechnik (BSI) empfohlen. Trotz dieser Rechtslage und obwohl Zertifikate für die Online-Transportverschlüsselung keine sonderlichen Kosten mehr verursachen, stoße ich bei der Bearbeitung von Hinweisen und Beschwerden gegen Online-Anbieter

eher zufällig immer wieder auf Online-Datenerhebungsformulare, bei denen das Schloss-Symbol am Anfang der Adresszeile des WWW-Browsers nicht geschlossen ist, bei denen also keine Maßnahme zur geschützten Datenübermittlung mittels Transportverschlüsselung der Daten von den Anbietern ergriffen wurde.

Diese Telemedien-Anbieter mache ich dann stets auf dieses Sicherheitsdefizit in ihrem Online-Angebot aufmerksam und weise dabei darauf hin, dass sie mit der fehlenden Transportverschlüsselung von Daten, die mittels Online-Formularen erhoben werden, einen Tatbestand aus Art. 83 Abs. 4 Buchst. a DS-GVO erfüllen, der mit einer Geldbuße von bis zu 10.000.000 € oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres, je nachdem welcher Betrag höher ist, geahndet werden kann.

Die Reaktionen der angesprochenen Online-Anbieter darauf waren so unterschiedlich und vielfältig wie die Angebote selbst. Die größeren gewerblichen Anbieter entschuldigten sich in der Regel für den Fehler, der dort oftmals nur einzelne Websites mit Sonderaktionen wie Gewinnspiele, Weihnachts- und Advents-Sonderseiten, zeitlich begrenzte Rückrufaktionen oder Ähnliches betraf, die nicht professionell in ein ansonsten verschlüsseltes Online-Angebot integriert wurden. Es wurde in diesen Fällen immer umgehend durch die Hinterlegung eines geeigneten TLS-Zertifikates Abhilfe geschaffen.

Einzelne kleinere Anbieter wurden erst durch meine Ansprache darauf aufmerksam, dass sie zwar bei ihrem Provider bereits jahrelang für eine Verschlüsselung bezahlen, diese von dem jeweiligen Provider allerdings nicht aktiviert wurde. Ich bin auch auf Online-Anbieter kleiner sog. „Web-Visitenkarten“ gestoßen, die mir mitteilten, dass sie seit Jahren noch nie eine Nachricht über ihr Online-Kontaktformular erhalten hätten und es nach meinem Hinweis der Einfachheit halber aus ihrem Telemedien-Angebot entfernt haben. Eine TLS-Transportverschlüsselung ist ohne aktive Datenerhebung nicht mehr erforderlich.

Nur ein einziger gewerblicher Online-Anbieter kam meinen Aufforderungen zur Implementierung einer TLS-Transportverschlüsselung für die Datenerhebungsformulare auf seinen Websites über ein Jahr lang trotz anfänglicher Zusage nicht nach, weshalb ich die Verschlüsselung gemäß Art. 58 Abs. 2 Buchst. d DS-GVO angeordnet und dem Unternehmen zur Durchsetzung der Anordnung ein Zwangsgeld angedroht und es auch festgesetzt habe. Nachdem ich dann auch noch eine Geldbuße gemäß Art. 83 Abs. 4 Buchst. a DS-GVO verhängte, hat er meine Forderungen endlich erfüllt.

Und obwohl man mit Fug und Recht davon überzeugt sein kann, dass gerade öffentliche Stellen in besonderem Maße zur Einhaltung geltenden Rechts

verpflichtet sind und mit gutem Beispiel vorangehen sollten, war es eine kleine Gemeinde aus dem Schwalm-Eder-Kreis, die meine Aufforderung zur Verschlüsselung der Online-Formulare in ihrem Web-Angebot mehrere Monate lang hartnäckig ignorierte. Dass eine Kommune, die in vielen kommunalen Zusammenhängen selbst die Einhaltung rechtlicher Vorschriften überprüft und durchsetzt, auf meine Hinweise auf die Verstöße gegen gesetzliche Datensicherheitsbestimmungen nicht reagiert, ist erstaunlich und geradezu unverständlich. Erst durch die Einschaltung des Landrats des Schwalm-Eder-Kreises konnte die Gemeinde mit Unterstützung durch die dortige Kommunalaufsicht dazu bewegt werden, den deutlich vorliegenden, andauernden Verstoß gegen Art. 5 Abs. 1 Buchst. f und Art. 32 DS-GVO zu unterlassen. Die Online-Datenerhebungsformulare wurden von der Gemeinde unter Hinweis auf mangelnde finanzielle Ressourcen und die angeblich zu hohen Kosten für ein TLS-Zertifikat gelöscht.

Festzuhalten ist, dass immer noch Anbieter von Telemedien aktiv Daten von Nutzern im WWW erheben, ohne eine TLS-Transportverschlüsselung in ihr Online-Angebot zu implementieren, was zu einer ungeschützten Übermittlung von Daten zwischen den Endgeräten der Nutzer und den Servern der Anbieter führt. Ich gehe solchen Verstößen gegen grundlegende gesetzliche Sicherheitsvorgaben stets nach und weise darauf hin, dass bei Nichtbeachtung Maßnahmen nach Art. 58 Abs. 2 DS-GVO ergriffen werden können und sogar Geldbußen drohen.

8.4
Elektronische Auskunftserteilung im Falle elektronischer Antragstellung

Wer elektronisch eine Auskunft begehrt, hat ein Recht, auch eine elektronische Antwort zu erhalten. Dabei muss der Verantwortliche aber eine Reihe von Anforderungen beachten.

Mit dem Auskunftsrecht nach Art. 15 DS-GVO wird dem Betroffenen ein essenzielles Betroffenenrecht zugestanden. Demzufolge sind betroffene Personen berechtigt, von dem für die Datenverarbeitung Verantwortlichen Auskunft über die zu ihrer Person gespeicherten personenbezogenen Daten zu verlangen.

Wie eine betroffene Person ihr Auskunftsrecht geltend macht, ist dem Grunde nach an wenige Anforderungen geknüpft. Vor allen Dingen ist der Auskunftsanspruch regelmäßig nicht an eine bestimmte Form gebunden. Grundsätzlich steht es der betroffenen Person somit frei, ob sie ihr Begehren

postalisch, elektronisch, telefonisch oder sogar persönlich vor Ort an den Verantwortlichen richtet.

Ein Betroffener wandte sich an mich, weil er sich auf Grund einer postalischen Werbesendung per E-Mail an den verantwortlichen Adresshändler mit einem Auskunftsbegehren gerichtet und innerhalb der gesetzlichen Frist von einem Monat nach Art. 12 Abs. 3 DS-GVO keine Antwort erhalten hatte. Im Rahmen des aufsichtsbehördlichen Verfahrens hat sich sodann herausgestellt, dass der Betroffene entgegen den eigenen Ausführungen eine Auskunft nach Art. 15 DS-GVO erhalten hatte, allerdings auf postalischem Wege an die im Unternehmen hinterlegte Adresse. Die Auskunft konnte dem Betroffenen allerdings nicht erfolgreich zugestellt werden, da diese an seine ehemalige Wohnanschrift übermittelt wurde.

Ich wies den Verantwortlichen darauf hin, dass entsprechend Art. 12 Abs. 3 Satz 4 DS-GVO die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen sind, wenn die betroffene Person wie im vorliegenden Fall den Antrag auf Auskunftserteilung elektronisch stellt.

Allerdings ist bei der Erteilung von datenschutzrechtlichen Auskünften stets zu beachten, dass ein unberechtigter Zugriff durch Dritte auf personenbezogene Daten strikt zu vermeiden ist. Dies gilt umso mehr bei der elektronischen Auskunftserteilung. Hierbei hat der Verantwortliche dafür Sorge zu tragen, dass die Auskunft nur an die betroffene Person oder eine bevollmächtigte Stelle erteilt wird und die Schutzpflichten Art. 5 Abs. 1 Buchst. f DS-GVO beachtet werden.

Dabei ist jedoch zu berücksichtigen, dass im Bereich des Adresshandels und der Neukundengewinnung kein direktes Kundenverhältnis zu der betroffenen Person besteht und die Verifizierung einer E-Mail-Adresse kaum möglich ist. Würde der Verantwortliche als weitere Legitimationsstufe ein Legitimationsdokument wie einen Ausweis oder eine Vollmacht fordern, könnte dies von der betroffenen Person als Hindernis und erweitertes Datensammeln durch einen Adresshändler verstanden werden.

Aus diesem Grund wies ich den Verantwortlichen auf den Erwägungsgrund 63 Satz 4 DS-GVO hin, wonach ein vom Verantwortlichen eingerichteter sicherer Fernzugriff auf die eigenen Daten eine Option für die Auskunftserteilung darstellt.

Da der Verantwortliche auf Grund des hohen Datenbestandes die Speicherung und Verarbeitung von personenbezogenen Daten in einem vollständig vom Außennetz isolierten IT-Verbund durchführt, setzte er, in aktiver Absprache mit mir, den Gedanken des Erwägungsgrundes 63 Satz 4 DS-GVO insofern um, als betroffene Personen, die ihr Auskunftsrecht elektronisch geltend

machen, eine direkte elektronische Rückmeldung erhalten, die den Medienwechsel von elektronisch auf postalisch transparent ankündigt und eine für die betroffene Person nachvollziehbare Begründung (Sicherheitsbedenken gegenüber Web-Portalen und einer unzulänglichen Legitimations- und Identitätsprüfung) liefert. Dem sodann postalisch übermittelten Auskunftsschreiben wird ein eindeutiges Aktenzeichen samt leicht verständlichem Hinweistext aufgedruckt. Sollte die betroffene Person weiterhin eine elektronische Kopie ihrer im Unternehmen gespeicherten personenbezogenen Daten benötigen, kann sie unter Verwendung des eindeutigen Aktenzeichens jederzeit die elektronische Kopie beim Verantwortlichen anfordern.

Mit der ursprünglichen Adresse des postalischen Werbeschreibens, der verwendeten Anschrift des Auskunftsschreibens und der Nennung des Aktenzeichens ist der Verantwortliche zweifelsfrei in der Lage, die Identität der auskunftssuchenden Person zu identifizieren und folglich eine elektronische Kopie ihrer Daten zur Verfügung zu stellen.

Festzuhalten ist, dass der Verantwortliche zu einer elektronischen Auskunft verpflichtet sein kann und dass er dafür technisch-organisatorische Vorkehrungen treffen muss, die ihm ermöglichen, die Berechtigung des Empfängers zu überprüfen und die Auskunft dem überprüften Empfänger elektronisch zugänglich zu machen.

8.5
Die datenschutzrechtlichen Privilegien der Medien

Immer wieder erreichen mich Beschwerden gegen Veröffentlichungen in Print- oder Onlinemedien. Bei der Bearbeitung dieser Beschwerden sind die „Medienprivilegien“ mit ihren Auswirkungen für die Datenschutzaufsicht zu beachten. Denn über Art. 85 Abs. 2 DS-GVO sind zum Schutz der Medienfreiheiten zahlreiche Ausnahmen von der DS-GVO für Datenverarbeitungen zu journalistischen Zwecken möglich.

Ausgleich zwischen Medienfreiheit und Datenschutz

Immer wieder rügen betroffene Personen die Veröffentlichung (beispielsweise) ihres Namens oder von Fotos in einem Online-Artikel. Außerdem wird oftmals die Erteilung einer unvollständigen Auskunft durch den Hessischen Rundfunk oder über den Beitragsservice im Rahmen des Einzugs des Rundfunkbeitrags bemängelt. Allerdings sind oftmals keine datenschutzrechtlichen Verstöße gegeben. Hintergrund für diese Einordnung sind die sog. datenschutzrechtlichen „Privilegien“ der Medien.

Die DS-GVO enthält eine Vielzahl von Voraussetzungen für Datenverarbeitungen sowie umfangreiche Rechte der betroffenen Personen, die im Bereich journalistischer Arbeit angesichts der Rundfunk- und Pressefreiheit und deren Erfordernisse nicht sachgerecht umzusetzen sind. Um dem zu begegnen, enthält die DS-GVO in Art. 85 Abs. 2 einen Regelungsauftrag für die Mitgliedstaaten. Sie sollen Ausnahmen von der Verordnung vorsehen, wenn die Verarbeitung zu journalistischen oder literarischen Zwecken erfolgt und diese erforderlich sind, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.[73]

Dieser Regelungsauftrag darf jedoch nicht als Primat für die Medienfreiheiten verstanden werden. Die in Umsetzung des Auftrags ergangenen nationalen Vorschriften stellen vielmehr das Ergebnis einer Abwägung zwischen dem Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) sowie den Medienfreiheiten (Rundfunkfreiheit, Pressefreiheit, Art. 5 Abs. 1 Satz 2 GG) dar.

Nach Art. 85 Abs. 2 DS-GVO sehen die Mitgliedstaaten Abweichungen oder Ausnahmen von Kapitel II (Grundsätze), Kapitel III (Rechte der betroffenen Person), Kapitel IV (Verantwortlicher und Auftragsverarbeiter), Kapitel V (Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen), Kapitel VI (Unabhängige Aufsichtsbehörden), Kapitel VII (Zusammenarbeit und Kohärenz) und Kapitel IX (Vorschriften für besondere Verarbeitungssituationen) vor. Soweit also eine nationale Vorschrift etwa Kapitel VI (Unabhängige Aufsichtsbehörden) für nicht anwendbar erklärt, findet keine Aufsicht durch die staatlichen Landesdatenschutzbehörden statt. Damit sind im Übrigen auch die in Kapitel VIII (Rechtsbehelfe, Haftung und Sanktionen) aufgeführten Art. 77, 78 und 83 DS-GVO unanwendbar, weil sie die Aufsichtsbehörden betreffen.[74]

Im Folgenden sollen Regelungen aus dem Medienstaatsvertrag (MStV) und dem Rundfunkbeitragsstaatsvertrag (RBStV) sowie dem Hessischen Pressegesetz (HPresseG), die in Umsetzung des Art. 85 Abs. 2 DS-GVO ergangen sind, näher erläutert werden. Da Rundfunk Ländersache ist, schließen die Bundesländer bi- oder multilaterale Staatsverträge. Durch die Zustimmungsgesetze der Landesparlamente werden die Staatsverträge in den Rang eines Landesgesetzes erhoben.

---

73 Wedekind, in: Gersdorf/Paal, Informations- und Medienrecht, 2. Aufl. 2021, LMedienG BW, § 49 Rn. 3.

74 S. Hessischer Landtag, Drs. 19/5728, S. 177.

Journalistische Datenverarbeitung

Sonderregelungen zum Datenschutz im Medienbereich sind deshalb erforderlich, weil Rundfunk und Presse in der Lage sein müssen, im Rahmen der journalistischen Tätigkeit personenbezogene Daten ohne Aufsicht einer Aufsichtsbehörde zu verarbeiten. Würde das Datenschutzrecht vollumfänglich auf journalistische Datenverarbeitungen Anwendung finden, müsste etwa angesichts des Gesetzesvorbehalts für jede journalistische Datenverarbeitung (digitale Recherche mit Personenbezug, digitale Artikel oder deren Archivierung) eine Einwilligung oder sonstige Rechtsgrundlage aus Art. 6 Abs. 1 DS-GVO gegeben sein. Von einer Berichterstattung betroffene Personen könnten hinsichtlich der journalistischen Datenverarbeitung datenschutzrechtliche Auskunfts-, Informations-, Widerspruchs- oder Berichtigungsrechte geltend machen, was etwa mit Blick auf den Informantenschutz problematisch wäre.

Die redaktionelle Datenverarbeitung erstreckt sich dabei von der Beschaffung der Information über die Speicherung und Verarbeitung in der Redaktion bis hin zur Veröffentlichung. Der Begriff des Journalismus ist nach Erwägungsgrund 153 Satz 7 der DS-GVO „weit auszulegen“, „um der Bedeutung des Rechts auf freie Meinungsäußerung in einer demokratischen Gesellschaft Rechnung zu tragen“. Da sich das Medienprivileg ausschließlich auf Verarbeitungstätigkeiten zu journalistischen Zwecken bezieht, gilt der Ausschluss der genannten Regeln der DS-GVO nur für Datenverarbeitungen zu diesen Zwecken, so dass Verarbeitungstätigkeiten zu anderen Zwecken in den Anwendungsbereich der DS-GVO fallen. Abgrenzungsschwierigkeiten bereitet die sog. „Mischdatenverarbeitung“. So könnte die Reisekostenabrechnung eines Journalisten etwa zur administrativen Datenverarbeitung zählen. Dient sie jedoch etwa Recherchezwecken, könnte es sich um eine journalistische Datenverarbeitung handeln. Es ist also stets im Einzelfall zu prüfen, welchen Zwecken die jeweilige Datenverarbeitung konkret dient.

Der Medienstaatsvertrag (MStV)

Der Medienstaatsvertrag regelt in erster Linie die Veranstaltung von Rundfunk und das Angebot von Telemedien sowie deren Verbreitung über Plattformen und Intermediäre.

§ 12 MStV enthält für den öffentlich-rechtlichen sowie den privaten Rundfunk Regelungen für die Datenverarbeitung zu journalistischen Zwecken. Die Vorschrift schränkt unter dem Gesichtspunkt des Medienprivilegs die Vorgaben der DS-GVO ein und ersetzt diese für die Verarbeitung zu journalistischen Zwecken weitgehend durch Regeln, die den verfassungsrechtlichen Vorgaben der Rundfunkfreiheit Rechnung tragen sollen. Betroffene Personen besitzen im Anwendungsbereich daher – entgegen Kapitel III – nur die Rechte aus

§ 12 Abs. 2 und 3 MStV. Diese sind etwa Gegendarstellungen angesichts journalistischer Datenverarbeitungen (Abs. 2) oder ein Auskunftsrecht bei Beeinträchtigung der Persönlichkeitsrechte durch eine Berichterstattung (Abs. 3).

Das Recht auf Auskunft ist im Falle einer Verarbeitung zu journalistischen Zwecken für den Rundfunk in § 12 Abs. 3 Satz 1 MStV geregelt. Voraussetzung hierfür ist, dass die die Auskunft begehrende betroffene Person durch eine Berichterstattung in ihren Persönlichkeitsrechten beeinträchtigt wurde. Nach § 12 Abs. 3 Satz 2 MStV kann die Auskunft trotz Vorliegens der genannten Voraussetzungen verweigert werden, soweit durch die Auskunftserteilung auf die in den Nr. 1 und 2 genannten Personen geschlossen werden könnte oder die Auskunftserteilung die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigen würde (Nr. 3). Diese Verweigerung der Auskunft nach einer die Persönlichkeitsrechte der betroffenen Person beeinträchtigenden Berichterstattung darf allerdings nicht generell, sondern nur nach Abwägung mit den schutzwürdigen Interessen der Beteiligten erfolgen.

§ 12 Abs. 4 MStV weist die Aufsicht über die Einhaltung der datenschutzrechtlichen Bestimmungen beim Rundfunk dem Landesrecht zu. In Hessen übe ich nach § 1 Abs. 4 HDSIG im Bereich des öffentlich-rechtlichen Rundfunks die Aufsicht über die administrative Datenverarbeitung beim Hessischen Rundfunk aus. Für die Datenverarbeitung zu journalistischen Zwecken hat der Hessische Rundfunk nach § 28 Abs. 2 HDSIG einen Datenschutzbeauftragten zu bestellen. Soweit meine Zuständigkeit für Datenverarbeitungen der hessischen privaten Rundfunkveranstalter besteht, ist nach § 46 f. HPMG die Medienanstalt des Landes Hessen im Rahmen von Aufsichtsverfahren zu beteiligen.

Die Datenverarbeitung zu journalistischen Zwecken bei Telemedien des öffentlich-rechtlichen Rundfunks, privater Rundfunkunternehmen oder der Presse ist ähnlich in § 23 MStV geregelt.

§ 23 Abs. 2 Satz 1 MStV gibt Personen, die von einer journalistischen Datenverarbeitung durch Anbieter von Telemedien „in ihrem Persönlichkeitsrecht beeinträchtigt“ werden, einen Anspruch auf Auskunft über die zugrundeliegenden, zu ihrer Person gespeicherten Redaktionsdaten. Nur für den entsprechenden Anspruch gegenüber Rundfunkangeboten wurde das begrenzende Erfordernis der Beeinträchtigung durch eine Berichterstattung eingeführt. Damit können Recherchen von Presse und Rundfunk für Telemedien auch ohne Veröffentlichung weiterhin einen Auskunftsanspruch auslösen, während dieselben Recherchen für ein Rundfunkprogramm erst im Veröffentlichungsfall Ansprüche begründen können. Auch hier kann die Auskunft gemäß § 23 Abs. 2 Satz 2 MStV verweigert werden, wenn sie Rückschlüsse auf Mitwirkende

oder Quellen erlauben oder die journalistische Aufgabe durch Ausforschung beeinträchtigen würde. Der Auskunfts- und Berichtigungsanspruch nach § 23 Abs. 2 MStV besteht zudem gemäß § 23 Abs. 2 Satz 5 MStV nicht, soweit Telemedien der Presse an der Selbstkontrolle des Presserates teilnehmen.

Zuständige Aufsicht im Falle einer redaktionellen Datenverarbeitung durch Telemedien von Rundfunkanbietern sind nach § 113 Satz 2 MStV diejenigen Stellen, die diese redaktionelle Aufsicht auch gegenüber den Landesrundfunkanstalten bzw. Rundfunkveranstaltern ausüben.

§ 10 HPresseG

§ 10 HPresseG schränkt die Anwendbarkeit der DS-GVO bei der Datenverarbeitung zu journalistischen oder literarischen Zwecken, mit Ausnahme von Datensicherheit und Datengeheimnis, weitgehend ein. Eine aufsichtsbehördliche Kontrolle findet nicht statt. Betroffenen Personen bleibt die Möglichkeit zur Sanktionierung mittels gerichtlich einklagbarer Unterlassungs- und Schadensersatzansprüche. Diese werden ergänzt um die Beschwerdemöglichkeit beim Deutschen Presserat als Selbstkontrolle des Redaktionsdatenschutzes, soweit sich das jeweilige Medienunternehmen dieser freiwilligen Kontrolle unterworfen hat. Damit betont der Gesetzgeber das verfassungs- und europarechtlich unverzichtbare Erfordernis, zur Ausübung einer journalistischen Tätigkeit der Presse mit der hierfür erforderlichen Verarbeitung personenbezogener Daten ohne staatliche Einfluss- und Kontrollmöglichkeiten.[75]

Der Auskunftsanspruch nach § 11 Abs. 8 Rundfunkbeitragsstaatsvertrag

Oftmals erreichen mich Beschwerden mit Blick auf Auskunftserteilungen durch den ARD ZDF Deutschlandradio Beitragsservice (seit 2013 Nachfolger der Gebühreneinzugszentrale). Sie thematisieren regelmäßig die Unvollständigkeit der Auskunft.

Der Beitragsservice ist gemäß § 10 Abs. 7 S. 1 RBStV eine nichtrechtsfähige Stelle, die als öffentlich-rechtliche Verwaltungsgemeinschaft gemeinsam von den öffentlich-rechtlichen Landesrundfunkanstalten betrieben wird. Demzufolge ist der Beitragsservice unselbstständiger Teil der jeweils zuständigen Landesrundfunkanstalt. Dessen Aufgabe ist die Einziehung der Rundfunkbeiträge, im Fall von Beitragsschuldnern mit (Wohn-)Sitz in Hessen für den

75 S. Hessischer Landtag, Drs. 19/5728, S. 177 f.

Hessischen Rundfunk.[76] Daher tritt für den Rundfunkbeitragsschuldner erkennbar der Beitragsservice nach außen auf, so dass dieser regelmäßig Adressat von Auskunftsbegehren ist. Da es sich beim Einzug des Rundfunkbeitrags nicht um eine journalistische Tätigkeit handelt, ist meine Zuständigkeit als Aufsichtsbehörde in diesen Fällen gegeben.

Der Gesetzgeber hat das Auskunftsrecht aus Art. 15 DS-GVO nach Art. 23 Abs. 1 Buchst. e DS-GVO beschränkt, um über die Auskunftspflichten der Landesrundfunkanstalten das Ziel der Datenverarbeitung und die Erfüllung des damit verfolgten öffentlichen Interesses nicht zu gefährden. Die Erhebung des Rundfunkbeitrags und die damit einhergehende Erhebung und Verarbeitung personenbezogener Daten erfolgt zur Erfüllung einer Aufgabe, die im öffentlichen Interesse liegt.[77]

Infolgedessen wird der Umfang des datenschutzrechtlichen Auskunftsanspruches gem. § 11 Abs. 8 RBStV konkretisiert. Nach dieser Regelung besteht ein Auskunftsrecht betroffener Personen (lediglich) über:

„1. die in § 8 Abs. 4 genannten, sie betreffenden personenbezogenen Daten,
2. das Bestehen, den Grund und die Dauer einer sie betreffenden Befreiung oder Ermäßigung im Sinne der §§ 4 und 4a,
3. sie betreffende Bankverbindungsdaten und
4. die Stelle, die die jeweiligen Daten übermittelt hat."

Die in § 8 Abs. 4 RBStV genannten Daten sind:

§ 8 Abs. 4 RBStV

(…)

1. *Vor- und Familienname sowie frühere Namen, unter denen eine Anmeldung bestand,*
2. *Tag der Geburt,*
3. *Vor- und Familienname oder Firma und Anschrift des Beitragsschuldners und seines gesetzlichen Vertreters,*
4. *gegenwärtige Anschrift jeder Betriebsstätte und jeder Wohnung, einschließlich aller vorhandenen Angaben zur Lage der Wohnung, sowie im Falle der Befreiung nach § 4a die Angabe, bei welcher Wohnung es sich um die Haupt- oder Nebenwohnung handelt,*

76 S. § 2 der Satzung des Hessischen Rundfunks über das Verfahren zur Leistung der Rundfunkbeiträge.

77 S. Hessischer Landtag, Drs. 20/1774 S. 19.

5. letzte der Landesrundfunkanstalt gemeldete Anschrift des Beitragsschuldners,
6. vollständige Bezeichnung des Inhabers der Betriebsstätte,
7. Anzahl der Beschäftigten der Betriebsstätte,
8. Beitragsnummer,
9. Datum des Beginns des Innehabens der Wohnung, der Betriebsstätte oder des beitragspflichtigen Kraftfahrzeugs,
10. Zugehörigkeit zu den Branchen und Einrichtungen nach § 5 Abs. 2 Satz 1 Nr. 1 und Abs. 3 Satz 1,
11. Anzahl der beitragspflichtigen Hotel- und Gästezimmer und Ferienwohnungen und
12. Anzahl und Zulassungsort der beitragspflichtigen Kraftfahrzeuge.

Daten, die nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, sind nach § 11 Abs. 8 a. E. RBStV vom datenschutzrechtlichen Auskunftsanspruch nicht umfasst.

Im Vergleich mit Art. 15 DS-GVO wird daher deutlich, dass der Umfang des Auskunftsanspruchs nach Art. 11 Abs. 8 RBStV deutlich reduziert ist. Die Eingaben bei mir mit Blick auf eine Unvollständigkeit der Auskunft sind daher durchaus nachvollziehbar, wenn auch in aller Regel unbegründet, da der Beitragsservice bei der Erteilung von Auskünften die nur für ihn geltende Spezialregelung beachtet.

Zusammenfassend kann festgehalten werden, dass die DS-GVO den Datenschutz bei der Datenverarbeitung in Medien nicht selbst regelt, sondern den Mitgliedstaaten aufgibt, durch eigene Regelungen einen Ausgleich zwischen den Interessen der Medien und der betroffenen Personen zu finden. In Erfüllung dieses Auftrags führen diese Regelungen zur Gewährleistung der gesellschaftlichen Funktion freier Medien zu einer Einschränkung der Rechte der betroffenen Personen.

9. Werbung und Adresshandel

Werbeunternehmen und Adresshändler verarbeiten gewerblich viele personenbezogene Daten und verursachen durch die Menge der personenbezogenen Daten und die Zielsetzung der Verarbeitung besondere datenschutzrechtliche Risiken. Diesen korrespondieren besondere Pflichten und ein hohes Maß an Verantwortung. Dies zeigt sich z. B. an erforderlichen technisch-organisatorischen Maßnahmen, um Werbewidersprüchen (Kap. 9.1) und anderen Rechten von betroffenen Personen (Kap. 9.4) gerecht zu werden, an Begrenzung der Erhebung personenbezogener Daten zu Werbezwecken (Kap. 9.2) und an den Voraussetzungen einer freiwilligen Werbeeinwilligung (Kap. 9.3).

9.1 Werbewidersprüche erfordern technisch-organisatorische Maßnahmen

Für die Datenverarbeitung zu Werbezwecken muss nicht immer eine Einwilligung vorliegen. Bei Bestandskunden kann auch die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO als Rechtsgrundlage dienen. Wenn Kunden aber von ihrem Recht nach Art. 21 Abs. 2 DS-GVO Gebrauch machen und der einwilligungsfreien Werbung widersprechen (Werbewiderspruch gegen Direktwerbung), muss dies von den werbetreibenden Unternehmen nach Art. 21 Abs. 3 DS-GVO unverzüglich umgesetzt und nachhaltig beachtet werden.

Außer einer Einwilligung der betroffenen Person nach Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DS-GVO kann auch eine Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO als Rechtsgrundlage für die Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung dienen. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein und die Interessen der betroffenen Person dürfen nicht überwiegen. Nach Erwägungsgrund (ErwG) 47 kann bei Direktwerbung an Bestandskunden Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO grundsätzlich tragfähig sein, da dort u. a. ausgeführt wird:

> *ErwGr 47 Satz 2 DS-GVO*
>
> *Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht.*

ErwGr 47 Satz 7 DS-GVO

Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

Im Berichtsjahr wandte sich ein Kunde einer großen Autohaus-Kette, die mehrere Niederlassungen im Rhein-Main-Gebiet unterhält, an mich, dessen personenbezogene Daten aufgrund dieser Interessenabwägung zunächst zulässigerweise von dem Unternehmen zu Werbezwecken per Briefpost und E-Mail verwendet wurden. Der Betroffene beschwerte sich nun darüber, dass er zwar sowohl der Post-Werbung als auch der E-Mail-Werbung widersprochen hatte, von dem Unternehmen aber dennoch trotz Bestätigung seines Werbewiderspruchs durch das Unternehmen im Sinne von Art. 12 Abs. 2 DS-GVO weiterhin Briefwerbung und Werbe-E-Mails erhielt. Diese Datenverwendung zu Werbezwecken, trotz Werbewiderspruchs verstößt klar gegen Art. 21 Abs. 2 und 3 DS-GVO:

Art. 21 Abs. 2 und 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.

Bei der Bearbeitung seiner Beschwerde und während der Nachforschungen zum Sachverhalt in dem Unternehmen stellte sich heraus, dass der Kunde mit seinem Fahrzeug auch noch eine andere Niederlassung des Autohauses aufgesucht hatte als die Niederlassung, in der er das Fahrzeug ursprünglich erworben hatte. Aus nicht mehr nachvollziehbaren Gründen (wahrscheinlich aus Versehen) wurde dabei in der zweiten Niederlassung ein zweiter Datensatz mit abweichender Schreibweise seines Namens und einer anderen Kundennummer für ihn angelegt. Die beiden Datensätze wurden nicht zusammengeführt. Die für ihn aufgrund seines Werbewiderspruchs gesetzte Werbesperre war dann nur in einem der Datensätze vermerkt worden, weshalb seine Daten aus dem zweiten Datensatz unzulässigerweise weiterhin zu Werbezwecken genutzt wurden.

Es liegt im Verantwortungsbereich des Unternehmens, dafür Sorge zu tragen, dass es im Rahmen einer ordnungsgemäßen Datenverarbeitung nicht zu Schreibfehlern und Doubletten in seiner Kundendatenbank kommt. Das

Unternehmen ist auch dafür verantwortlich, dass ein Werbewiderspruch umfassend im Sinne von Art. 21 Abs. 3 DS-GVO beachtet wird. Es muss beim Setzen von Werbesperren sorgfältig überprüft werden, ob zu einem Betroffenen – weshalb auch immer – möglicherweise mehrere Datensätze existieren oder ob in einer seiner Niederlassungen einem Mitarbeiter bei der Datenerhebung Schreibfehler unterlaufen sind, die zu einer Kunden-Doublette in seinem Datenbestand geführt haben könnten. Der Fehler wurde aufgrund meiner Ermittlungen entdeckt und beseitigt. Den Verstoß des Autohauses gegen Art. 21 Abs. 3 DS-GVO habe ich ausdrücklich festgestellt und gerügt.

Trotz des großen Aufwands bei der Fehlersuche, meiner deutlichen Rüge und den erkennbaren Bemühungen des Unternehmens, seinen Datenbestand zu bereinigen und so Datenschutzverstöße zu vermeiden, erhielt der betroffene Kunde einige Monate später erneut E-Mail-Werbung des Autohauses. Nun stellte sich bei meinen Ermittlungen heraus, dass Daten zu seiner Person auch noch in der Datenbank eines Fahrzeugherstellers erfasst waren, die zuvor bei der Fehlersuche nicht tiefgreifend genug überprüft wurde. Der dortige Datensatz wurde zuvor nicht entdeckt und es war daher auch keine Werbesperre dazu eingetragen, was zur erneuten werblichen Verwendung der Daten zur Person des Beschwerdeführers führte, die eigentlich für Werbezwecke hätten gesperrt sein sollen.

Aufgrund dieses erneuten gleichgelagerten Verstoßes gegen Art. 21 Abs. 3 DS-GVO habe ich eine förmliche Verwarnung gegen das Autohaus nach Art. 58 Abs. 2 Buchst. b DS-GVO ausgesprochen, die auch bestandskräftig und damit unanfechtbar wurde.

Ein Jahr später erhielt der Betroffene gleichwohl erneut Briefwerbung dieses Autohauses, weshalb er sich empört über die Missachtung seiner datenschutzrechtlichen Ansprüche und enttäuscht über die Unwirksamkeit meiner aufsichtsbehördlichen Maßnahmen nochmals bei mir gegen das Autohaus wandte. Bei den anschließenden Untersuchungen musste ich feststellen, dass die dieser Werbepost zugrunde liegenden Daten zur Person des Betroffenen aus einer weiteren Datenbank des Autohauses stammten, in der er ohne Vorname und mit einer leicht abgewandelten Schreibweise seiner Postanschrift gespeichert war. Auch hier war es dem Autohaus zum wiederholten Mal trotz angeblich intensiver Suche nicht gelungen, einen Datensatz dem Betroffenen zuzuordnen und mit einer Werbesperre zu versehen. Gerade in verteilten und heterogenen Datenbanksystemen, wie sie in vielen Unternehmen üblich sind, muss aber besonders achtsam und sorgfältig gearbeitet werden, wenn garantiert werden soll, dass Werbewidersprüche auf Dauer umfassend und nachhaltig beachtet werden. Dass Datenbestände über mehrere Datenbanken und Niederlassungen verteilt sind und Schreibweisen von Namen und An-

schriften aufgrund mangelnder Sorgfalt bei der Datenerfassung in einzelnen Datensätzen voneinander abweichen, darf nicht zu Lasten der Rechte der betroffenen Kunden gehen.

Da das Autohaus zuvor bereits nach Art. 58 Abs. 2 Buchst. b DS-GVO verwarnt wurde, habe ich ein Bußgeldverfahren nach Art. 83 Abs. 5 Buchst. b DS-GVO wegen des mehrfach wiederholten Verstoßes gegen Art. 21 Abs. 3 DS-GVO gegen das Autohaus eingeleitet und mit der Verhängung einer Geldbuße abgeschlossen. Das Autohaus war bezüglich der Datenschutzverstoßes zwar einsichtig, hat aber wegen der Höhe der verhängten Geldbuße Einspruch gegen meinen Bescheid eingelegt. Diesem Einspruch habe ich nicht abgeholfen und das Verfahren an das zuständige Gericht abgegeben. Eine gerichtliche Entscheidung über die Geldbuße liegt zum Zeitpunkt der Berichterstellung noch nicht vor.

Zusammenfassend kann festgehalten werden, dass Verantwortliche ihre technischen und organisatorischen Maßnahmen zur Umsetzung von Werbewidersprüchen, wie die Eintragung von Werbesperren in Kundendatenbanken oder die Führung, Pflege und Anwendung von Widerspruchslisten (sog. „interne Robinsonlisten“ oder „Nixie-Dateien“), sehr sorgfältig planen und auch bei verteilten Datenbanken, bei Auftragsverarbeitern und in komplexen Datenverarbeitungsumgebungen wirksam anwenden müssen. Bei mangelnder Sorgfalt und daraus resultierenden Fehlern, die zu einer werblichen Verwendung personenbezogener Daten trotz vorliegenden Werbewiderspruchs führen, drohen ihnen Sanktionen der Aufsichtsbehörde, insbesondere wenn diese Fehler öfter auftreten oder sich gar wiederholen.

9.2
Recherche von personenbezogenen Daten im WWW zu Werbezwecken

Wer im WWW personenbezogene Daten recherchiert, um diese in Folge zu werblichen Zwecken zu verarbeiten, sollte sich der gesetzlichen Voraussetzungen bewusst sein.

Der Kontaktaufnahme mittels Werbe-E-Mails wurden durch den Gesetzgeber enge Grenzen gesetzt. Datenschutzrechtlich bedeutet dies zunächst, dass zugunsten des Versenders eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten vorhanden sein muss.

Der Versand von Werbe-E-Mails ist datenschutzrechtlich zulässig, wenn die betroffene Person hierzu eine ausdrückliche, informierte und freiwillige Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 DS-GVO erteilt hat.

Daneben kann die Datenverarbeitung zu Werbezwecken grundsätzlich auch auf eine Interessensabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden. In einer solchen überwiegen allerdings die Interessen der betroffenen Personen immer diejenigen des Verantwortlichen, wenn dessen Handeln nicht im Einklang mit der Rechtsordnung steht, insbesondere dem Recht gegen unlauteren Wettbewerb widerspricht. 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. Werbetreibende können, soweit keine Einwilligungen vorliegen, Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO nicht als datenschutzrechtliche Grundlage für E-Mail-Werbung in Anspruch nehmen, da ein wirtschaftliches Interesse an ungesetzlicher Werbung nie als berechtigtes Interesse anerkannt werden kann.

Eine ausdrückliche, informierte und freiwillige Einwilligung kann allerdings durch betroffene Personen nicht erteilt werden, wenn ihre personenbezogenen Daten ohne ihre Kenntnis im WWW auf unterschiedlichen Websites recherchiert worden sind.

Innerhalb des Berichtszeitraums versandte ein Marketingunternehmen eine werbliche E-Mail an eine Betroffene, die in keinerlei Beziehung zu dem Unternehmen gestanden hatte und sich folglich über die werbliche Kontaktaufnahme bei mir beschwerte. Im Rahmen des Verfahrens konnte ermittelt werden, dass das Unternehmen das WWW durchsucht hatte und auf unterschiedlichen Webseiten über 2.100 potenziell geeignete Kunden recherchierte, die personenbezogenen Daten der Betroffenen erhob, speicherte und sodann zu werblichen Zwecken per E-Mail verarbeitete.

Ein solches willkürliches und ungeplantes „Datensammeln“ ist allerdings nicht zulässig. Die Verarbeitung von personenbezogenen Daten darf nur rechtmäßig, zweckgebunden und sachlich richtig erfolgen. Außerdem ist sie ihrem Umfang nach auf Daten zu beschränken, die zur Zweckerfüllung notwendig sind.

Auf Grund dessen erfolgte eine Abhilfe-Anordnung nach Art. 58 Abs. 2 Buchst. f und g DS-GVO und dem verantwortlichen Unternehmen wurde untersagt, die E-Mail-Adressen der Betroffenen im Speziellen sowie alle weiteren E-Mail-Adressen zu Werbezwecken zu nutzen, die zu Zwecken der Werbung erhoben wurden und zu denen der Verantwortliche bisher keine Geschäftsbeziehung unterhielt, soweit ihm keine ausdrückliche Einwilligung der Betroffenen in die Verarbeitung zur E-Mail-Werbung vorliegt. Weiterhin wurde dem Verantwortlichen aufgetragen, alle E-Mail-Adressen, die dieser ausschließlich zu werblichen Zwecken erhoben hat und bei denen ihm keine

Einwilligungen der jeweiligen Adressaten in die Verarbeitung zur werblichen Nutzung vorliegen, zu löschen.

Diese Maßnahmen entfalteten ihre Wirkung. Das Unternehmen besserte nach und bestätigte, dass es alle recherchierten Datensätze gelöscht habe und folglich nicht weiter zu werblichen Zwecken verarbeiten würde. Nach Abschluss des Verwaltungsverfahrens wurde die Prüfung einer Geldbuße in die Wege geleitet.

9.3
Zur Freiwilligkeit der Werbeeinwilligung

„Ich will!“ bedeutet nicht „Ich muss wollen“. Das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO soll die Freiwilligkeit einer Einwilligung absichern, insbesondere auch bei Werbeeinwilligungen. Von Freiwilligkeit kann keine Rede sein, wenn eine Verweigerung der Werbeeinwilligung mit Nachteilen verbunden ist.

Verantwortliche dürfen personenbezogene Daten Betroffener nur dann verarbeiten, wenn ein Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. a bis f DS-GVO greift. Wird eine Einwilligung des Betroffenen nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO eingeholt, ist diese nur dann wirksam, wenn sie entsprechend Art. 4 Nr. 11 DS-GVO freiwillig erfolgt.

Dies wurde im Zusammenhang mit Werbung ebenfalls durch ein Gerichtsurteil des OLG Frankfurt am Main (vom 27. Juni 2019 – 6 U 6/19) bestätigt, in dem entschieden wurde, dass ein Freebie nur zulässig sei, wenn die Werbeeinwilligung des Nutzers freiwillig im Sinne der DS-GVO erteilt worden ist.

Im Berichtszeitraum kontaktierte mich ein Betroffener, der ein Ticket zu einer Veranstaltung online käuflich erwerben wollte. Im Rahmen des letzten Schrittes des Kaufprozesses wurde ihm ein nicht vorausgefülltes Optionskästchen angeboten, mit dem der Betroffene eine Einwilligung zur werblichen Kontaktaufnahme erteilen könnte. Als er ohne Auswahl dieses Optionsfelds und somit ohne Einwilligung in den Erhalt von personalisierten Marketinginformationen den Verkauf abschließen wollte, öffnete sich ein Informationsfeld mit dem Hinweis, dass ohne die Erteilung einer Einwilligung nur der Erwerb direkt vor Ort an der Kasse möglich sei. Das verantwortliche Unternehmen argumentierte vehement, dass der Veranstaltungsteilnehmer trotz dieser Zwangssituation absolut frei wäre in seiner Entscheidung, keine Einwilligung zu erteilen, und an der Kasse vor Ort ein Ticket ohne Erteilung einer Werbeeinwilligung erwerben kann. Weiterhin bewertete der Verantwortliche, das Ticket an der Kasse vor Ort zu erwerben, als zumutbare Alternative. Das

Kopplungsverbot des Art. 7 Abs. 4 DS-GVO greife nicht, da im konkreten Einzelfall eine werbefreie Alternative zum Kartenkauf angeboten werde.

Die Freiwilligkeit der Einwilligung fehlt jedoch, wenn die Voraussetzung für den Kauf eines Online-Tickets die Einwilligung in den Erhalt eines Newsletters ist. Entsprechend des Art. 7 Abs. 4 DS-GVO muss bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, dem Umstand Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrages von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrages nicht erforderlich ist. Weiterhin führt der Erwägungsgrund 43 Satz 2 der DS-GVO dazu aus, dass die Einwilligung nicht als freiwillig erteilt gilt, wenn die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

Die Einwilligung ist demnach nur dann freiwillig, wenn die betroffene Person, ohne dass Druck oder Zwang auf sie ausgeübt wird, um sie zu einer Einwilligung zu bewegen, ihre Daten für Zwecke zur Verfügung stellt, die für den Vertrag nicht erforderlich sind, etwa für Direktmarketing durch den Verantwortlichen oder Dritte. Erwägungsgrund 42 der DS-GVO verlangt eine echte Wahlfreiheit der betroffenen Person, die in der Lage sein soll, die Einwilligung zu verweigern oder zurückzunehmen, ohne dadurch Nachteile zu erleiden.

Im Rahmen des Aufsichtsverfahrens stellte sich heraus, dass mit dem Kauf eines Online-Tickets sowohl weitere digitale Services für die Kunden im Vorfeld der eigentlichen Veranstaltung einhergehen, als auch ein kostenloses Ticket für den öffentlichen Nahverkehr zur Verfügung gestellt wird, um umweltfreundlich zur Veranstaltung anreisen zu können.

Neben der Tatsache, dass eine Einwilligung zur Verarbeitung personenbezogener Daten zu werblichen Zwecken für den Erwerb eines Online-Tickets zum Besuch einer Veranstaltung eindeutig nicht erforderlich ist, stellt darüber hinaus auch der Ausschluss von digitalen Services im Vorfeld der Veranstaltung und der Wegfall der kostenlosen, umweltfreundlichen An- und Abreisemöglichkeit eine Benachteiligung der betroffenen Person dar, die auf die Erteilung einer Einwilligung in die werbliche Nutzung ihrer personenbezogenen Daten verzichtet.

Gegenüber dem Verantwortlichen reichte es aus, ihn darauf hinzuweisen, dass die Aufsichtsbehörde ihn nach Art. 58 Abs. 2 lit. d DS-GVO anweisen kann, seine Verarbeitungsvorgänge auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen. Er akzeptierte das und konzipierte den Prozess zur Abfrage einer Einwilligung in die werbliche Kontaktaufnahme beim Erwerb eines Online-Tickets neu. Hierdurch wurde DS-GVO-konform die Einwilligung in die werbliche Verar-

beitung der im Unternehmen gespeicherten personenbezogenen Daten von dem Erwerb eines Online-Tickets entkoppelt.

9.4
Technisch-organisatorische Maßnahmen bei Adresshändlern

Technische und organisatorische Maßnahmen sollen personenbezogene Daten, die von Unternehmen erhoben, verarbeitet und gespeichert werden, bestmöglich schützen. Die Schwierigkeit liegt oft im Detail, ob nämlich die gewählten Maßnahmen wirklich ausreichend sind, ein angemessenes Schutzniveau sicherzustellen. Gerade Unternehmen, die gewerblich mit personenbezogenen Daten handeln, müssen sich diesbezüglich an einem hohen Maßstab messen lassen.

Verantwortliche haben entsprechend der DS-GVO eine breite Palette an Aufgaben und Verpflichtungen, sobald sie personenbezogene Daten von Betroffenen erheben, erfassen, organisieren, verarbeiten oder offenlegen. Ein wesentlicher Bestandteil ist dabei der Schutz personenbezogener Daten sowie die Gewährleistung einer sicheren Verarbeitung. Dies geschieht insbesondere im Wege der Umsetzung geeigneter technischer und organisatorischer Maßnahmen, kurz TOM's.

Entsprechend Art. 32 DS-GVO sind TOM's unter Berücksichtigung des aktuellen Stands der Technik sowie der Art, des Umfangs, den Umständen und dem Zweck der Verarbeitung von personenbezogenen Daten einzurichten. Leider bleibt die DS-GVO eine Liste von konkreten verpflichtenden technischen und organisatorischen Maßnahmen schuldig. Ein Blick in die alte, bis 2018 geltende Fassung des BDSG bringt zu diesem Themenschwerpunkt in der Anlage zu § 9 Abs. 1 BDSG (alte Fassung) eine informative Konkretisierung und benennt folgende Bereiche: *„Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungsgebot".*

Wie essenziell eine Zugriffskontrolle als technische und organisatorische Maßnahme ist, zeigt der folgende Fall: Ein Betroffener erhielt eine postalische Werbesendung, die im Rahmen des Datenschutzhinweises auf einen hessischen Adresshändler als Verantwortlichen für die Erhebung und Verarbeitung der personenbezogenen Daten verwies. Der Betroffene wollte sodann sowohl sein Auskunftsrecht nach Art. 15 DS-GVO als auch sein Recht auf Werbewiderspruch nach Art. 21 Abs. 2 und 3 DS-GVO geltend machen und wandte sich postalisch an die im Datenschutzhinweis hinterlegte Adresse. Anstatt innerhalb der gesetzlichen Frist nach Art. 12 Abs. 3 DS-GVO eine Bestätigung seines Werbewiderspruchs und eine detaillierte Auskunft

durch den Verantwortlichen zu erhalten, kam sein postalisches Schreiben als unzustellbar zurück, woraufhin er sich mit der Bitte an mich wandte, ihn bei der Durchsetzung seiner datenschutzrechtlichen Betroffenenrechte zu unterstützen.

In Erfüllung dieser Bitte konnte ich ermitteln, dass der hessische Adresshändler im genannten Zeitraum seinen Unternehmenssitz innerhalb Hessens gewechselt hatte. Um innerhalb dieser Umbruchphase sicherzustellen, dass alle datenschutzrechtlichen Betroffenenanfragen das Unternehmen auch zur Kenntnis und weiteren Veranlassung erreichen, stellte das Unternehmen frühzeitig einen Nachsendeantrag bei der Deutschen Post.

Es stellte sich jedoch überraschend heraus, dass die Unternehmenspost im Rahmen des Nachsendeantrags an eine private Adresse eines Unternehmensangehörigen weitergeleitet wurde. Hierbei handelte es sich um ein Mehrfamilienhaus mit drei Parteien. Weiterhin hatte nicht allein der Unternehmensangehörige Zugriff auf den Briefkasten, sondern auch seine im gleichen Haushalt lebende Lebensgefährtin.

Der Datenschutz schließt Homeoffice-Tätigkeit nicht grundsätzlich aus. Verantwortliche müssen jedoch der im Vergleich zum betrieblichen Arbeitsplatz veränderten Gefährdungslage im Homeoffice Rechnung tragen und sicherstellen, dass das Schutzniveau angemessen ist. Aus diesem Grund muss in jedem Einzelfall unter Berücksichtigung der Art, der zu verarbeitenden Daten und ihres Verwendungszusammenhangs sorgfältig und differenziert geprüft werden, ob die getroffenen technischen und organisatorischen Maßnahmen des Verantwortlichen ausreichend sind, um ein angemessenes Schutzniveau sicherzustellen. Wenn es beim Homeoffice zur Verarbeitung von personenbezogenen Daten kommt, kann dies zu Risiken für die Persönlichkeitsrechte der Personen, deren Daten verarbeitet werden, führen. Die Gefahr eines Datenmissbrauchs oder einer unzulässigen Einflussnahme durch Dritte ist beim Homeoffice höher, da der Arbeitgeber nur eingeschränkte Kontroll- und Einflussmöglichkeiten hat.

Im Rahmen einer Homeoffice-Tätigkeit müssen, wenn diese nicht ausschließlich medienbruchfrei erfolgt, geeignete häusliche Räumlichkeiten und Arbeitsmittel zur sicheren Aufbewahrung und vertraulichen Behandlung von Unterlagen und Datenträgern mit personenbezogenen Daten vorhanden sein.

Es dürfen ausschließlich Unternehmenszugehörige oder von der Unternehmensleitung dazu ausdrücklich autorisierte Personen Zugang zu den im Zusammenhang mit der Arbeitstätigkeit anfallenden personenbezogenen Daten haben. Weder Familienangehörige oder Lebenspartner noch Mitbewohner oder sonstige Personen dürfen Zugriff auf die zu schützenden Daten erhalten.

Da nicht sichergestellt war, dass fremde Dritte keinen Zugriff auf personenbezogene Daten erhalten, stellte die Nachsendung von Unternehmenspost an einen vom Unternehmensangehörigen gemeinsam mit seiner Partnerin genutzten Privatbriefkasten einen Verstoß gegen die Pflichten aus Art. 5 Abs. 1 Buchst. f sowie Art. 32 Abs. 1 und 2 DS-GVO dar. Insbesondere den Unternehmenszweck des Verantwortlichen berücksichtigend, der u. a. im Vertrieb und der Verarbeitung von personenbezogenen Daten und dem Handel mit Adressen besteht und sich als besonders datenintensiv darstellt, musste zwingend eine Abhilfemaßnahme nach Art. 58 Abs. 2 Buchst. d DS-GVO mit sofortiger Vollziehung erfolgen.

Diese Maßnahme entfaltete ihre Wirkung. Das Unternehmen besserte umgehend nach und ließ sich fortan die Unternehmenspost an den neuen Unternehmenssitz nachsenden. So war sichergestellt, dass lediglich Unternehmensangehörige Zugriff auf personenbezogene Daten von Betroffenen erhalten können. Auf Grund der Gesamtumstände wurde nach Abschluss des Verwaltungsverfahrens ein Verfahren zur Verhängung einer Geldbuße nach Art. 83 Abs. 4 Buchst. a DS-GVO eingeleitet.

10. 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. Die Bedingungen für Videoüberwachungen werden am Beispiel des kommunalen Schutzes eines Weltkulturerbes (Kap. 10.1) und eines Generalkonsulats (Kap. 10.2) erörtert.

10.1
Videoüberwachung durch Kommunen

Bei einer Videoüberwachung durch Unternehmen (oder durch Personen mit Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit) kommt die Datenschutz-Grundverordnung zur Anwendung. Möchten Kommunen öffentlich zugängliche Bereiche filmen, kommt als Rechtsgrundlage das Hessische Datenschutz- und Informationsfreiheitsgesetz in Betracht. Beispielhaft an der geplanten Neueinrichtung der Videoüberwachungsanlage, betreffend das Weltkulturerbe Mathildenhöhe Darmstadt, werden die Voraussetzungen für eine Videoüberwachung durch Kommunen erläutert.

Schutz eines Kulturerbes

Das „Übereinkommen zum Schutz des Kultur-und Naturerbes der Welt“ (Welterbe-Übereinkommen) wurde 1972 von der Generalkonferenz der UNESCO verabschiedet. Dieses Abkommen beruht auf der Idee „… dass Teile des Kultur- oder Naturerbes von außergewöhnlicher Bedeutung sind und daher als Bestandteil des Welterbes der ganzen Menschheit erhalten werden müssen“. Seit 2021 ist die Mathildenhöhe Darmstadt UNESCO Welterbe.[78]

Das Welterbe Mathildenhöhe Darmstadt besteht aus mehreren Gebäuden und Objekten. Neben einem Ausstellungsgebäude umfasst das Ensemble den Hochzeitsturm, die Russische Kapelle, einen Gartenpavillon, ein Ateliergebäude, einen Platanenhain, den Bacchusbrunnen, das Lilienbecken und weitere Gebäude.

Die Stadt Darmstadt erfragte, wie eine Überwachung zum Schutz des Welterbes unter Datenschutzkriterien stattfinden könne. Die geplante Einrichtung einer neuen Videoüberwachungsanlage wurde damit begründet, das Welterbe

78 S. www.mathildenhoehe-darmstadt.de.

zu schützen und Vandalismus vorzubeugen. Es wurden folgende Vorkommnisse geschildert: Die Ausstellungshalle sei in der Vergangenheit immer wieder durch Farbschmierereien und andere Vandalismustaten beschädigt worden.[79] Es bleibe viel Müll durch Besucher liegen. Im Jahr 2021 sei der Sockel des Wahrzeichens beschmiert und die Toilettenanlage beschädigt worden.

Kameras zur Überwachung des Geländes waren an zentraler Stelle auf der Mathildenhöhe bereits vor Einführung der DS-GVO installiert. Die Geräte waren aus Datenschutzgründen jedoch abgeschaltet. Bis zur datenschutzkonformen Einrichtung eines neuen Kamerasystems wurde ein privater Sicherheitsdienst beauftragt, das Gelände zu sichern.

Rechtsgrundlagen für Videoüberwachungen

Jede Videoüberwachung stellt grundsätzlich einen erheblichen Eingriff in das Persönlichkeitsrecht der beobachteten Personen dar und kann eine schwere Persönlichkeitsverletzung sein. Eine Verarbeitung von personenbezogenen Daten (und Videoüberwachung ist eine solche Verarbeitung) durch öffentliche Stellen ist daher nach Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO nur rechtmäßig, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO ist kein eigenständiger Erlaubnistatbestand und nur in Verbindung mit einer weiteren Grundlage anwendbar. Der Verordnungsgeber hat in Art. 6 Abs. 3 dem nationalen Gesetzgeber die Möglichkeit gegeben, für diese Aufgabe im öffentlichen Interesse geeignete Erlaubnistatbestände für die Datenverarbeitung vorzusehen, und in Art. 6 Abs. 2 DS-GVO bestimmt, dass die Mitgliedstaaten spezifischere Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen können, um eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten.

Zunächst war also zu prüfen, ob die Videoüberwachung des Welterbes für die Aufgabenwahrnehmung erforderlich ist, die im öffentlichen Interesse liegt, damit die Öffnungsklauseln in Art. 6 Abs. 2 und 3 DS-GVO wirksam werden können.[80] Im öffentlichen Interesse liegt die Aufgabe, wenn sie zu Bereichen der Ordnungs-, Leistungs- und Lenkungsverwaltung zählt. Als Lenkungsverwaltung wird die Förderung und Steuerung von Bereichen des sozialen, wirtschaftlichen und kulturellen Lebens bezeichnet. Die Lenkungsverwaltung kann dabei gleichzeitig Leistungsverwaltung (z. B. Subvention)

79 Darmstädter Echo vom 9. November 2022.

80 S. z. B. Schulz in: Gola/Heckmann, DSGVO/BDSG, 3. Aufl. 2022, DS-GVO Art. 6 Rn. 51-54; Roßnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1, Rn. 67 ff., Art. 6 Abs. 2 Rn. 22 ff., Art. 6 Abs. 3 Rn. 19 ff.

wie auch Ordnungsverwaltung (Verbot von Straftaten) sein. Die Unterhaltung sowie der Schutz des Welterbes stellt eine im öffentlichen Interesse liegende Aufgabe dar.

Eine präzisere Bestimmung und damit weitere Grundlage zur Videoüberwachung durch öffentliche Stellen, der Gemeinden und Landkreise des Landes Hessen findet sich in § 4 HDSIG.

§ 4 Abs. 1 HDSIG

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,

2. zur Wahrnehmung des Hausrechts

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Unter öffentlich zugänglichen Räumen sind Bereiche zu verstehen, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und ihrem Zweck nach auch dazu bestimmt sind. Die Zweckbestimmung kann sich aus einer Widmung, z. B. für den öffentlichen Verkehr, oder aus dem erkennbaren Willen des Berechtigten ergeben. Ein solcher Raum kann innerhalb und außerhalb von Gebäuden liegen.

Gebäude und die gesamte Liegenschaft Mathildenhöhe sind als öffentlicher Raum im Sinne des Gesetzes einzuordnen. Es ist nämlich gerade erwünscht, dass der Schatz des Welterbes der Öffentlichkeit zugänglich gemacht wird.

Die Videoüberwachung des öffentlich zugänglichen Raumes muss erforderlich sein. Dies ist gegeben, wenn die Videoüberwachung die Aufgabenerfüllung der öffentlichen Stelle oder die Ausübung des Hausrechts wesentlich unterstützt.[81] Sie muss dagegen nicht „unerlässlich“ sein. Daraus folgt aber auch, dass die Erforderlichkeit deutlich mehr verlangt als nur eine beiläufige Nützlichkeit oder gar bloße Tauglichkeit. Zur Zweckerfüllung darf es also kein anderes gleich wirksames, aber milderes Mittel geben; die Geeignetheit wird vorausgesetzt. Daneben muss ein fehlendes überwiegendes schutzwürdiges Interesse betroffener Personen gegeben sein. Dies ist in der Praxis eher die Ausnahme als die Regel.[82]

---

81 S. z. B. Wilhelm, in: BeckOK DatenschutzR BDSG § 4 Rn. 24; s. zu § 6b Abs. 1 Satz 1 Nr. 1 BDSG aF Scholz: in Simitis, BDSG, 8. Aufl. 2014, § 6b Rn. 71.

82 S. Spieker gen. Döhmann, in: Roßnagel, HK-HDSIG, 2021, § 4 Rn. 16, 17.

Datenschutzgerechtes Ergebnis

Der Schutz von Kulturgütern und -objekten liegt im öffentlichen Interesse – insbesondere bei unwiederbringlichen Schätzen und Objekten. Bei einem Ortstermin auf der Mathildenhöhe Darmstadt, bei dem die Datenschutzbeauftragte sowie Beschäftigte aus dem Bereich Planung der Stadtverwaltung, Vertreter der Polizei und der Betriebsleiter des Eigenbetriebs Kulturinstitute der Wissenschaftsstadt Darmstadt beteiligt waren, wurde besprochen, wo und wie eine Videoüberwachungsanlage geeignet, erforderlich und angemessen wäre. Dabei hat meine Behörde eine beratende Funktion und nicht die Aufgabe, eine Videoüberwachungseinrichtung abzunehmen, freizugeben oder zu bewilligen.

Im Rahmen der Gefahrenabwehr dürfen die Ordnungsbehörden Videoüberwachungsmaßnahmen an Orten durchführen, an denen schon verschiedentlich Straftaten begangen wurden und die Gefahr besteht, dass weitere Straftaten begangen werden (rechtliche Grundlage wäre hier § 14 Abs. 3 und 4 HSOG). Ein Kriminalitätsschwerpunkt im Sinne des HSOG liegt hier jedoch nicht vor.

Im konkreten Fall wurde der Einsatz von mehr Personal durch einen Sicherheitsdienst, die Polizei oder die Ordnungsbehörde durch die Beteiligten bereits geprüft. Ein Sicherheitsdienst wurde beauftragt und die Ordnungsbehörden führten vermehrt Streifengänge durch.

Im Weiteren wird von der Kommune, aufbauend auf dem Grundsatz der Datenminimierung, ein Sicherheitskonzept erstellt, das neben der personellen Vor-Ort-Prüfung eine gute Ausleuchtung von schlecht einsehbaren Orten der Liegenschaft beinhaltet. Besonders schützenswerte Exponate sollen darüber hinaus gesondert gesichert werden. Bei der Videoüberwachung selbst wird geprüft werden, ob die Überwachung auf bestimmte Zeiträume beschränkt werden kann, z. B. in denen Einbrüche oder Sachbeschädigungen überwiegend geschehen oder kein Personal vor Ort ist. Sensible oder nicht benötigte Aufnahmebereiche (z. B. Toiletten) werden nicht von der Überwachung umfasst sein. Die Kameras sollen dabei so ausgerichtet sein, dass Personen außerhalb der fraglichen Fläche nicht den Eindruck haben müssen, ihre Bewegungen würden durch die Kameras erfasst. Dabei werden die schützenswerten Interessen des Einzelnen an einem ungestörten Aufenthalt auf der Mathildenhöhe berücksichtigt und ein Baustein des Konzeptes sein.

Nicht von der Norm des § 4 HDSIG erlaubt ist eine weiträumige Überwachung von Plätzen, wo sich Menschen länger zum Verweilen aufhalten, sowie an Zugängen oder auch Toilettenanlagen. Hierfür reicht es auch nicht aus, wenn

begründet wird, dass Parkbesucher Müll hinterlassen. Ohne Nachweis einer bestehenden konkreten Gefahr darf der Park nicht überwacht werden.[83]

10.2
Videoüberwachung vor dem iranischen Generalkonsulat

Mein Versuch, die Videoüberwachung durch das iranische Generalkonsulat in Frankfurt zu überprüfen, führte zu einer Klärung der Zulässigkeit der Videoüberwachung durch alle Fremden Missionen in Deutschland.

Im September 2022 kam in Teheran die Studentin Jina Mahsa Amini nach einer Kopftuchkontrolle im Polizeigewahrsam zu Tode. Diese Gewalttat führte im Iran zu landesweiten Protesten gegen die Kopftuchpflicht und gegen die Regierung, die durch staatliche Stellen und Revolutionsgarden unterdrückt wurden. Um dagegen auch in Deutschland zu protestieren, errichteten politisch Aktive auf der gegenüberliegenden Straßenseite des iranischen Generalkonsulats in Frankfurt eine ständige Mahnwache. Ich erhielt im Berichtszeitraum Hinweise von Mitgliedern des Landtags, vom Hessischen Rundfunk und von der Stadt Frankfurt aufgrund der dort eingegangenen Beschwerden, dass die Mahnwache durch Videokameras des iranischen Generalkonsulats überwacht werde. Aus den Hinweisen ging hervor, dass das iranische Generalkonsulat Videokameras am Gebäude installiert habe, die nicht nur das Gelände des Konsulats, sondern auch den gesamten Straßenraum vor dem Gebäude aufnähmen. Teilnehmer der Mahnwache befürchteten, dass sie durch die Videoüberwachung identifiziert würden und ihre Freunde und Verwandten im Iran Repressalien unterworfen werden könnten.

Die Prüfung der Situation vor Ort zumindest durch Außenansicht ergab, dass die meisten Überwachungskameras auf das eigene Konsulatsgelände gerichtet waren. Es waren jedoch zwei Kameras im Gebäudeinnern hinter der vollverglasten Gebäudefront erkennbar, die für eine Videoüberwachung des öffentlichen Bereichs genutzt werden konnten. Für eine festinstallierte Dome-Kamera konnte nicht festgestellt werden, wohin das Kameraauge ausgerichtet ist und ob Schwenk- und Zoom-Funktionen vorhanden sind, die eine Überwachung des Außenbereichs ermöglichten. Für eine mobile Standkamera war von ihrem Standplatz und ihrer Ausrichtung her davon auszugehen, dass sie nur den öffentlichen Raum im Fokus haben konnte. Insgesamt ergab die Prüfung der Lage vor Ort den Eindruck, dass Kameras

83 S. auch VGH Bayern vom 30. Mai 2023 zur Videoüberwachung eines Parks in Bayern, Abrufbar unter https://www.vgh.bayern.de/mam/gerichte/bayvgh/presse/5_bv_20.2104.pdf.

des Generalkonsulats den Raum vor seinem Gebäude, die Straße, die Zufahrt zum gegenüberliegenden Parkplatz sowie den Parkplatz selbst erfassen und damit auch die Mahnwache.

In der Vergangenheit war es bei internationalen Missionen in Hessen immer erfolgreich, mit ihnen direkt Kontakt aufzunehmen und die Datenschutzfragen einvernehmlich zu klären. Daher bat ich das iranische Generalkonsulat um Informationen zu der Verwendung der eingesetzten Kameras. Das Generalkonsulat reagierte auf diese Bitte jedoch nicht, sondern beschwerte sich über das iranische Außenministerium, das Auswärtige Amt und die Hessische Staatskanzlei darüber, dass ich nicht den gebotenen diplomatischen Weg beschritten hatte. Nachdem ich die Rechtslage und mein Vorgehen der Staatskanzlei und dem Auswärtigen Amt erläutert und auf die Dringlichkeit der Nachfrage hingewiesen hatte, versandte das Auswärtige Amt an alle diplomatischen und konsularischen Missionen, Internationalen Organisationen und anderen Vertretungen in Deutschland (Fremden Missionen) zur Videoüberwachung der jeweiligen Liegenschaften eine „Rundnote“.

In dieser Rundnote bat das Auswärtige Amt die Fremden Missionen bei eigenen Schutzmaßnahmen durch Videoüberwachung die rechtlichen Grenzen zu beachten.

Grundsätzlich ist nur die Videoüberwachung der Liegenschaft selbst sowie des unmittelbaren Außenbereichs (Umfriedung der Liegenschaft von außen) zulässig. Gemäß Art. 3 DS-GVO gelten deren Vorgaben räumlich auch dann, wenn eine Fremde Mission in Deutschland Personen im Umfeld der Liegenschaft beobachtet.

Art. 6 der DS-GVO setzt einer Videoüberwachung sehr enge Grenzen. Sie kann im Einzelfall nach Art. 6 Abs. 1 UAbs. 1 Buchst. e sowie Abs. 3 DS-GVO und §§ 3 und 4 BDSG zulässig sein, sofern sie zur Wahrnehmung der Aufgaben der Fremden Mission erforderlich ist und keine Anhaltspunkte dafür bestehen, dass überwiegende Interessen betroffener Personen entgegenstehen. Im Rahmen der Überwachung eines Anwesens dürfen in der Regel keine öffentlich zugänglichen Straßenzüge oder Gehwege überwacht werden.

Um die Einschränkung der Grundrechte von Passanten und Anwohnern möglichst gering zu halten, darf die Fremde Mission nur den Bereich unmittelbar um das Gebäude überwachen, jedoch nicht die Straße und den gegenüberliegenden Bürgersteig. Sie muss Bereiche durch Verpixelung unkenntlich machen, die entbehrlich sind, sowie insbesondere Eingänge und Fenster von anderen Anwesen. Außerdem müssen die erhobenen Daten unverzüglich gelöscht werden, sobald sie für den Zweck, die Sicherheit der Fremden Mission sicherzustellen, nicht mehr benötigt werden (in der Regel

binnen 72 Stunden). Die Videoüberwachung ist außerdem adäquat, in der Regel durch Hinweisschilder, kenntlich zu machen.

11. Wirtschaft

Der große Bereich der Wirtschaft, der Banken, der Auskunfteien, des Verkehrswesens, der Selbstständigen und der Sozialwirtschaft führt zu vielfältigen Fragen des Datenschutzes. Auch für den Berichtszeitraum sind Bewertungen zu sehr unterschiedlichen Datenschutzthemen zu berichten. Im Vordergrund stehen Fragen des Datenschutzes bei Auskunfteien, nämlich Empfehlungen zum Scoringverfahren (Kap. 11.1), zu zwei Urteilen des EuGH – einmal zum Bonitätsscoring (Kap. 11.2) und einmal zur Datenverarbeitung rund um die Restschuldbefreiung (Kap. 11.3) – und schließlich zu den Verhaltensregeln von Auskunfteien (Kap. 11.4). In diesem Kapitel geht es aber auch um die Verwendung von Eigentümerdaten aus dem Liegenschaftskataster (Kap. 11.5), die Erstellung von Fotos in der Wohnung von Käufern durch Zusteller von Paketen (Kap. 11.6), den Versand von Zugangsdaten an veraltete Mobilfunknummern (Kap. 11.7) und die Freiwilligkeit der biometrischen Identifizierung in Fitness-Studios (Kap. 11.8).

11.1
Empfehlungen zum Scoringverfahren

Die Regierungskoalition verabredete in ihrem Koalitionsvertrag das Ziel, für mehr Transparenz und allgemein für eine Verbesserung des Verbraucher- und Datenschutzes beim Kreditscoring zu sorgen. Hierzu hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) mit ihrer Stellungnahme vom 11. Mai 2023, an der ich mitgewirkt habe, der Bundesregierung diverse Vorschläge zur Verbesserung des Datenschutzes bei Scoringverfahren unterbreitet.

In Deutschland besteht in Bezug auf Daten, Algorithmen, Geschäftsentscheidungsprozesse und deren Zusammenspiel ein hoher Aufklärungs- und Erklärungsbedarf, da hierzu große Unsicherheit in der Bevölkerung besteht. Um dem entgegenzuwirken, hat die DSK gegenüber der Bundesregierung zu einem Teilbereich, dem Verfahren zum Kreditscoring, umfassend Stellung genommen.

Als Scoring wird die Zuordnung eines Zahlenwertes (Wahrscheinlichkeitswert) zu einer Person zum Zweck der Verhaltensprognose oder Verhaltenssteuerung bezeichnet. Die Bestimmung dieses Zahlenwertes erfolgt in der Regel auf der Grundlage einer breiten Datenbasis durch ein algorithmisches Verfahren.

Ein Score zur Bonität eines Kunden, der einen Kreditantrag stellt, bildet für das Kreditinstitut eine Grundlage für eine Entscheidung für eine Kreditvergabe. Die Berechnung dieses Scores zur Wahrscheinlichkeit einer Erfüllung des

Kreditvertrags erfolgt auf der Grundlage eines mathematisch-statistischen Verfahrens.

Die DSK hat ihrer Stellungnahme folgende Empfehlungen ausgesprochen:[84]

Verständlicher Score durch mehr Transparenz

Betroffenen Personen fehlen oft verständliche Informationen über Details, die Bedeutung und Gewichtung einzelner Merkmale des Scoringverfahrens. Diese sollten daher – über die bereits bestehenden Informationspflichten hinaus – proaktiv Kenntnis über den Einsatz von Scoringverfahren zu ihrer Person erhalten, auch wenn die abschlägige Entscheidung nicht unmittelbar auf einem Scorewert beruht (Erweiterung der Unterrichtungspflicht des § 30 Abs. 2 BDSG).

Bei einer nachteiligen Entscheidung für die betroffene Person durch den Scorewert empfiehlt die DSK eine Verpflichtung des Verantwortlichen, die Berechnung und den verwendeten Scorewert der betroffenen Person mitzuteilen. Ferner sollten betroffene Personen in leicht nachvollziehbarer Weise (beispielhafte Darstellungen und Visualisierung (Erklärvideos)) das Verfahren, die Bedeutung und die Beeinflussung durch einzelne Merkmale des Scores verständlich gemacht werden. Verbessern ließen sich außerdem die zu erteilenden Informationen und Auskünfte an Betroffene hinsichtlich des Umfangs und der Detailtiefe sowohl von den Stellen, die Scorewerte ermitteln, als auch von den verwendenden Stellen. Die DSK nennt hier die für die Berechnung genutzten Daten der Betroffenen, die verarbeiteten Scorewerte und ihre Empfänger, die Scoremerkmale (zum Beispiel „laufende Kreditverträge“, „Zahl der Kreditkarten“, „Alter“) und die Gewichtung von Merkmalen, etwa durch Auflistung nach Relevanz.

Transparenter sollte auch die Aussagekraft des konkreten Scorewerts (Einordnung in ein Risikoschema in Bezug auf die betroffene Person) und dessen Prognosegenauigkeit gemacht werden, insbesondere dann, wenn nur wenige score-relevante Informationen zu einer Person vorliegen. Dies betrifft insbesondere die Merkmale „Anschriftenwechsel“ und „Wohnumfeldbewertungen“ (sog. Geoscoring).

Ferner empfiehlt die DSK, dass Scoringverfahren zukünftig zertifiziert und die Zertifizierung den betroffenen Personen mitgeteilt werden sollte. Dies setzt – anders als bisher – voraus, dass die Wissenschaftlichkeit der Berechnung und die Prognosegenauigkeit von unabhängigen Stellen geprüft werden,

84 https://www.datenschutzkonferenz-online.de/media/st/DSK-Handlungsempfehlungen_Verbesserung_des_Datenschutzes_bei_Scoringverfahren.pdf.

da das dafür erforderliche Know-how in den meisten Datenschutzbehörden nicht vorhanden ist.

Weiter wäre in diesem Zusammenhang wichtig, dass die gewerbsmäßig berechnenden Stellen für die Scorewerte verpflichtet werden, die übermittelten Werte mindestens ein Jahr lang zu speichern und nicht – wie bislang – nach der Übermittlung unverzüglich zu löschen, da nur bei der Speicherung der Daten eine Auskunftspflicht gegenüber den Betroffenen besteht.

Eine andere Möglichkeit für mehr Transparenz ist die Verwendung von sogenannten Daten-Cockpits und Score-Simulatoren. Daten-Cockpits bieten den Betroffenen die Möglichkeit, ihre Daten nicht nur einzusehen, sondern auch Betroffenenrechte, zum Beispiel durch Beschwerdemechanismen, geltend zu machen. Score-Simulatoren können Betroffenen erste Informationen geben, welche Merkmale welche Wirkungen bei der Berechnung des Scores entfalten.

Qualität und Angemessenheit der Scores

Die DSK spricht sich auch für den Verzicht oder das Verbot einzelner Kriterien bei der Score-Berechnung aus: Häufig bei der Berechnung verwendete Informationen von geringer Signifikanz (z. B. Bewertung von Namen, Geoscoring, Anschriftenwechsel) sind kritisch, weil damit die lediglich statistische Annahme von der real zu bewertenden Person diametral abweichen kann. In diesem Zusammenhang wäre eine gesetzliche Negativliste sinnvoll, die festlegt, welche Daten nicht in einen Score einfließen dürfen (z. B. Name, Geschlecht, Daten von Plattformen der sozialen Medien oder dem Internet).

Einen weiteren Ansatzpunkt sieht die DSK in der Implementierung von Verfahren zur Sicherstellung richtiger und aktueller Daten für das Scoring, um so die Scoregüte zu gewährleisten. Bei der Erstprüfung der Daten sollte derjenigen, der den Score berechnet, eine Bewertung der Zuverlässigkeit der Quellen vornehmen. Ferner sollten sie Betroffenen Instrumente (insbesondere unkomplizierte Beschwerdeverfahren) zur Verfügung stellen, um unrichtige und nicht mehr aktuelle Daten berichtigen zu können.

Damit diese empfohlenen Maßnahmen auch umgesetzt werden, hält die DSK verbindliche gesetzliche Regelungen für sinnvoll, da nur so ein Schutz aller Verbraucherinnen und Verbraucher bei allen Scorewerterstellern erreicht werden könne.

11.2
EuGH-Urteil zum Bonitäts-Scoring der Auskunfteien

Am 7. Dezember 2023 hat der EuGH in der Rechtssache C-634/21[85] am Beispiel der SCHUFA über die Frage, ob die Erstellung eines Bonitäts-Scores durch eine Auskunftei und dessen Verwendung durch ein Kreditinstitut eine grundsätzlich verbotene automatisierte Entscheidung nach Art. 22 Abs. 1 DS-GVO darstellt, eine Entscheidung getroffen (s. Kap. 3.1 und 1.1).

Für den EuGH ist Art. 22 Abs. 1 DS-GVO unter drei kumulativen Voraussetzungen anwendbar. Es muss erstens eine „Entscheidung" vorliegen, zweitens muss diese Entscheidung „ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling" beruhen und drittens muss sie „gegenüber (der betroffenen Person) rechtliche Wirkung entfalten" oder sie „in ähnlicher Weise erheblich" beeinträchtigen (Rn. 43).

Der Begriff „Entscheidung" ist nach dem EuGH weit auszulegen. Bereits aus dem Wortlaut des Art. 22 DS-GVO ergibt sich, dass dieser Begriff sich nicht nur auf Handlungen bezieht, die rechtliche Wirkung gegenüber der betroffenen Person entfalten, sondern auch auf Handlungen, die diese Person in ähnlicher Weise erheblich beeinträchtigen (Rn. 44). Die Entscheidung kann aus einer Kette von mehreren Maßnahmen bestehen, nicht nur aus der diese Kette abschließenden Handlung. Entscheidend ist, ob auf die untersuchte Maßnahme die beiden anderen Voraussetzungen zutreffen.

Die zweite Voraussetzung ist, dass die Entscheidung ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruht. Die Datensammlung der Auskunftei und die Erstellung des Wahrscheinlichkeitswerts erfüllen die Definition des „Profiling" in Art. 4 Nr. 4 DSGVO und damit auch die zweite Voraussetzung (Rn. 47).

Hinsichtlich der dritten Voraussetzung ist für den EuGH entscheidend, ob das Handeln des Dritten, dem der Wahrscheinlichkeitswert übermittelt wird, „maßgeblich" von diesem Wert geleitet wird. Sofern der von einer Wirtschaftsauskunftei ermittelte und einer Bank mitgeteilte Wahrscheinlichkeitswert eine maßgebliche Rolle bei der Gewährung eines Kredits spielt, ist die Ermittlung dieses Werts als solche als Entscheidung einzustufen, die im Sinne von Art. 22 Abs. 1 DS-GVO gegenüber einer Person „rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt" (Rn. 50).

Der EuGH stellt zusätzlich zu der Interpretation des Art. 22 Abs. 1 DS-GVO zwei systematische Überlegungen an, um sein Ergebnis zu rechtfertigen. Zum einen problematisiert er, dass Regelungen des Art. 22 DS-GVO leerlaufen

85 EuGH Urteil vom 7.12.2023, C-634/21 – ECLI:EU:C:2023:957, NJW 2024, 413.

können, wenn nur die letzte Handlung in einer Entscheidungskette berücksichtigt würde, Entscheidungen in der Praxis aber in mehreren Schritten und arbeitsteilig getroffen werden. Er verweist dabei auf Abs. 2 (Voraussetzung für Aufhebung des Verbots), Abs. 3 (Garantien wie das Recht auf Erwirkung des Eingreifens einer Person, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung) und Abs. 4 (keine besonderen Kategorien) (Rn. 53–55). Zum anderen verweist er auf Art. 13, 14 und 15 DS-GVO, nach denen „aussagekräftige Informationen über die involvierte Logik" zu geben sind, wenn eine Entscheidung nach Art. 22 Abs. 1 DS-GVO vorliegt. Nur wenn „Entscheidung" so weit verstanden wird, wie der EuGH dies tut, greifen diese Regelungen. Ansonsten würde die Auskunftei keine Entscheidung treffen und das Kreditinstitut keine automatisierte Verarbeitung durchführen. Keiner von beiden müsste über die „involvierte Logik" informieren. Daher bestünde „die Gefahr einer Umgehung von Art. 22 DS-GVO und folglich eine Rechtsschutzlücke" (Rn. 61). „In diesem Fall würde nämlich die Ermittlung eines Wahrscheinlichkeitswerts nicht den besonderen Anforderungen von Art. 22 Abs. 2 bis 4 DS-GVO unterliegen, obwohl dieses Verfahren auf einer automatisierten Verarbeitung beruht und Wirkungen entfaltet, welche die betroffene Person erheblich beeinträchtigen, da das Handeln des Dritten (Bank), dem dieser Wahrscheinlichkeitswert übermittelt wird, von diesem maßgeblich geleitet ist." (Rn. 62).

11.3 EuGH-Urteil zur Datenverarbeitung von Daten zur Restschuldbefreiung

Im Urteil des EuGH in den Rechtssachen C 26/22 und C-64/22[86] ging es um die Frage, ob Auskunfteien Daten zu einer Restschuldbefreiung für drei Jahre speichern dürfen, die sie aus dem Insolvenzregister übernommen haben (s. auch Kap. 3.1 und 1.1).

Maßstab für den EuGH war Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO. Diesen Erlaubnistatbestand prüft er in drei Stufen. In der ersten Stufe bejaht er die berechtigten Interessen der Auskunftei und der Kreditwirtschaft. Hierfür nahm er Bezug auf EU-Regelungen zu Verbraucherschutz und Immobilienkrediten und auf das „reibungslose Funktionieren des gesamten Kreditsystems" (Rn. 83–86). Für die zweite Stufe verweist der EuGH darauf, dass die Datenverarbeitung auf das unbedingt Notwendige zur Verwirklichung des berechtigten

86 EuGH Urteil vom 7.12.2023, C 26/22 und C-64/22 – ECLI:EU:C:2023:958, NJW 2024, 417.

Interesses zu beschränken ist (Rn. 87). Die Prüfung der Erforderlichkeit verbindet er mit der dritten Stufe, der Abwägung der gegensätzlichen Interessen.

Zugunsten der Auskunfteien ist zu berücksichtigen, dass die objektive und zuverlässige Bewertung der Kreditwürdigkeit es der Auskunftei ermöglicht, „Informationsunterschiede auszugleichen und damit Betrugsrisiken und andere Unsicherheiten zu verringern“ (Rn. 93). Aber auch das Insolvenzregister zielt auf „eine bessere Information der betroffenen Gläubiger und Gerichte“ ab (Rn. 96), was das Interesse an einer zusätzlichen Speicherung reduziert.

Für die Bewertung der Auswirkungen der Speicherung der Daten ist zu berücksichtigen, dass die „Verarbeitung von Daten über eine Restschuldbefreiung, wie etwa die Speicherung, Analyse und Weitergabe dieser Daten an einen Dritten“, „einen schweren Eingriff in die Grundrechte der betroffenen Person“ darstellt (Rn. 94). Solche Daten dienen als negativer Faktor bei der Beurteilung der Kreditwürdigkeit der betroffenen Person und stellen daher sensible Informationen über ihr Privatleben dar. Die „Verarbeitung kann den Interessen der betroffenen Person beträchtlich schaden und die Ausübung ihrer Freiheiten erheblich erschweren, insbesondere wenn es darum geht, Grundbedürfnisse zu decken“. Die negativen Folgen für die betroffene Person sind „umso größer und die Anforderungen an die Rechtmäßigkeit der Speicherung dieser Informationen umso höher, je länger die Daten durch Wirtschaftsauskunfteien gespeichert werden“ (Rn. 95).

Bei der Gewichtung der entgegengesetzten Interessen nimmt der EuGH Bezug auf die Regelung in § 3 InsBekV, die für das öffentliche Register eine Speicherdauer von nur sechs Monaten vorsieht. Der deutsche Gesetzgeber geht dabei „davon aus, dass nach Ablauf einer Frist von sechs Monaten die Rechte und Interessen der betroffenen Person diejenigen der Öffentlichkeit, über diese Information zu verfügen, überwiegen“ (Rn. 97). Für den EuGH ist entscheidend, dass die Restschuldbefreiung es dem Begünstigten ermöglicht, sich erneut am Wirtschaftsleben zu beteiligen. Die Verwirklichung dieses Ziels wäre jedoch gefährdet, wenn Auskunfteien zur Beurteilung der wirtschaftlichen Situation einer Person Daten über eine Restschuldbefreiung für einen Bonitätsscore verwenden könnten, nachdem sie aus dem öffentlichen Insolvenzregister gelöscht worden sind (Rn. 98). Der EuGH stellt daher fest, dass die Interessen des Kreditsektors, über Informationen hinsichtlich einer Restschuldbefreiung zu verfügen, keine Verarbeitung dieser Daten nach Ablauf der Frist für ihre Speicherung im öffentlichen Insolvenzregister rechtfertigen können. Eine Speicherung dieser Daten durch eine Auskunftei kann nach der Löschung dieser Daten aus einem öffentlichen Insolvenzregister nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden (Rn. 99).

Für die parallele Speicherung der Daten zur Restschuldbefreiung während ihrer Veröffentlichung im Insolvenzregister trifft der EuGH keine so klare Feststellung. Einerseits sind „die Auswirkungen einer parallel erfolgenden Speicherung zwar als weniger schwerwiegend an(zu)sehen als nach Ablauf der sechs Monate“. Andererseits stellt diese Speicherung einen Eingriff in die in den Art. 7 und 8 der Charta verankerten Rechte dar. Sie verstärkt den Eingriff in das Recht der Person auf Achtung des Privatlebens (Rn. 100). Daher hat das vorlegende Verwaltungsgericht Wiesbaden zu prüfen, ob die Vorratsspeicherung dieser Daten durch die Auskunftei auf das zur Verwirklichung des berechtigten Interesses unbedingt Erforderliche beschränkt ist, obwohl die fraglichen Daten im öffentlichen Register abgerufen werden können und ohne dass ein Wirtschaftsunternehmen in einem konkreten Fall um Auskunft ersucht hat (Rn. 91).

11.4
Verhaltensregeln der Auskunfteien

Die größeren Auskunfteien in Deutschland sind in dem Verband „Die Wirtschaftsauskunfteien“ zusammengeschlossen. Dieser Verband gab sich zum 25. Mai 2018 Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien gemäß Art. 40 DS-GVO. Diese Verhaltensregeln beschränken sich auf Prüf- und Löschfristen und enthalten keine Regelungen zur materiellen Berechtigung der Speicherung von personenbezogenen Daten.

Die Verhaltensregeln wurden nach Abstimmung unter allen deutschen Aufsichtsbehörden von der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen gemäß Art. 40 Abs. 5 DS-GVO genehmigt. Da der Verband seinen Sitz im Jahr 2023 nach Wiesbaden verlagert hat, bin nun ich die zuständige Datenschutzaufsichtsbehörde.

Die Verhaltensregeln sind bis zum 24. Mai 2024 befristet. Nach ihrem Teil IV verlängern sich die Verhaltensregeln um jeweils weitere sechs Jahre, sofern die zuständige Datenschutzaufsichtsbehörde keine Beanstandungen erhebt. Aufgrund der beiden zuvor dargestellten EuGH-Urteile, der EDSA-Leitlinie 1/2019 über Verhaltensregeln und Überwachungsstellen vom 4. Juni 2019, des DSK-Beschlusses zur Verarbeitung von Positivdaten aus Verträgen über Mobilfunkdiensten und Dauerhandelskonten durch Auskunfteien vom 22. Juni 2021, der DSK-Vorschläge für Handlungsempfehlungen an die Bundesregierung zur Verbesserung des Datenschutzes bei Scoringverfahren vom 11. Mai 2023 (s. Kap. 11.1) und der DSK-Entschließung zu Kernelementen der Überwachungsaufgaben von Überwachungsstellen für Verhaltensregeln nach Art. 40 DS-GVO vom 23. November 2023, habe ich Beanstandungen

geltend gemacht. Der Verband hat daraufhin erklärt, die Verhaltensregeln überarbeiten zu wollen und mir im Jahr 2024 zur Genehmigung vorzulegen.

11.5
Eigentümerdaten aus dem Liegenschaftskataster

„Eigentümerdaten aus dem Liegenschaftskataster" ist immer wieder ein Thema der Datenschutzaufsicht. Nach der letzten Änderung des Hessischen Vermessungs- und Geoinformationsgesetzes ergeben sich folgende Schwerpunkte in der Aufsichtspraxis.

Bei Beschwerden und Anfragen handelt es sich meist um Fälle, bei denen Immobilienmaklern oder Kaufinteressenten die Eigentümer von Grundstücken anschreiben und diese bei mir anfragen, woher die kontaktaufnehmende Partei die Daten erhalten hat und ob die Katasterbehörde die Daten rechtmäßig bekanntgeben darf.

Eine Verarbeitung personenbezogener Daten und damit auch eine Übermittlung oder Offenlegung ist gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO zulässig, wenn eine rechtliche Verpflichtung dies erfordert. Gemäß § 16 Abs. 1 des Hessischen Vermessungs- und Geoinformationsgesetzes (HVGG) kann jede Person oder Stelle das Liegenschaftskataster, das eine bei den Ämtern für Bodenmanagement geführte allgemein zugängliche Quelle darstellt, einsehen und Auskünfte oder Angaben daraus erhalten.

Allerdings wird dieses Recht im Hinblick auf Einsichtnahme, Auskunft und Ausgabe von personenbezogenen Daten (Name des Eigentümers oder der Eigentümerin, ggf. das Geburtsdatum und die Anschrift) durch § 16 Abs. 2 HVGG eingeschränkt.

§ 16 HVGG

(1) Geobasisdaten und zugehörige Metadaten sind vorbehaltlich der Abs. 2 und 5 öffentlich zugänglich. Der Zugang wird durch die Gewährung von Einsicht in die Datenbestände sowie die Erteilung von Auskünften oder die Bereitstellung von Ausgaben daraus eröffnet.

(2) Der Zugang zu den Namen, Geburtsdaten und Anschriften der Eigentümerinnen, Eigentümer und deren Bevollmächtigten steht nur den Personen oder Stellen zu, die ein berechtigtes Interesse an der Kenntnis dieser Daten haben. Das berechtigte Interesse ist darzulegen.

(…)

§ 16 Abs. 1 HVGG stellt demnach eine bereichsspezifische Rechtsgrundlage dar, welche die Verarbeitung von Eigentümerdaten legitimiert. Hierzu muss die anfragende Person jedoch ein berechtigtes Interesse an den genannten

personenbezogenen Daten nachweisen können. Unter einem berechtigten Interesse versteht man jedes sachbezogene, persönliche, wissenschaftliche, statistische, historische, rechtliche und auch wirtschaftliche Interesse, das über ein allgemeines, unspezifiziertes Informationsinteresse oder die „reine Neugierde“ hinausgeht. Ein wirtschaftliches Interesse an der Kenntnis der Eigentümerdaten ist schon dann anzuerkennen, wenn jemand ein Kauf- oder Pachtinteresse an dem Grundstück geltend macht. Immobilienmakler haben dabei für sich alleine kein berechtigtes Interesse an der Kenntnis der personenbezogenen Daten der im Liegenschaftskataster geführten Eigentümer. Der bloße Hinweis auf ihre berufliche Tätigkeit begründet noch kein berechtigtes Interesse im Sinne von § 16 Abs. 2 HVGG. Ein wirtschaftliches Interesse an der Kenntnis der Eigentümerdaten ist jedoch dann anzuerkennen, wenn der Makler von einem bestimmten Interessenten beauftragt worden ist, Kontakt wegen eines Kaufinteresses an einer Immobilie oder in einer Immobilie herzustellen. Auch können Privatpersonen, die beispielsweise Interesse am Erwerb einer bestimmten Immobilie haben, ein berechtigtes Interesse haben.

Die anfragenden Personen verarbeiten die Daten in der Regel auf Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO weiter. Dabei ist in § 18 Abs. 2 HVGG zudem spezialgesetzlich geregelt, dass die Namen, Geburtsdaten und Anschriften der Eigentümerinnen, Eigentümer und deren Bevollmächtigten nur für den Zweck genutzt werden dürfen, der das berechtigte Interesse am Zugang zu diesen Daten begründet und zu dessen Erfüllung die betreffenden Daten übermittelt wurden. Eine Weiterverwendung für andere Zwecke ist unzulässig. Die nur vereinzelt vorkommenden Zuwiderhandlungen können im Einzelfall aufgeklärt und geahndet werden.

Aus datenschutzrechtlicher Sicht ist demnach die Übermittlung der Daten durch die Ämter für Bodenmanagement bei Darlegung eines berechtigten Interesses sowie die Weiterverarbeitung der Daten im Rahmen des angegebenen berechtigten Interesses nicht zu beanstanden.

Verantwortliche sind jedoch verpflichtet, die von der Verarbeitung betroffenen Personen über die Verarbeitung ihrer Daten zu informieren. In den Fällen, in denen die Daten aus dem Liegenschaftskataster stammen, haben die anfragenden und weiterverarbeitenden Verantwortlichen die Daten nicht direkt bei den Betroffenen erhoben. Sie unterliegen daher der Informationspflicht nach Art. 14 DS-GVO. Meist wird diese Pflicht nicht oder nur unzureichend erfüllt, so dass hier ein Hauptgrund für die Feststellung von Verstößen liegt.

Nach Änderung des HVGG sind inzwischen Makler von der Möglichkeit, sich einen Direktabruf nach § 17 HVGG einrichten zu lassen, ausgeschlossen. Ein Missbrauch eines Direktabrufs für andere Zwecke (z. B. reine Kaltakquise) ist so seitdem schwieriger möglich und besser nachträglich überprüfbar.

Darüber hinaus wird gem. § 16 Abs. 3 Satz 1 HVGG über den Zugang zu Eigentümerdaten durch Personen mit einem berechtigten Interesse zum Zweck der Datenschutzkontrolle ein Protokoll geführt. Dadurch kann die Datenschutzaufsichtsbehörde erfolgte Abrufe überprüfen und in Einzelfällen die Rechtmäßigkeit einer Auskunft prüfen und Verstöße ahnden.

11.6
Fotos in der Wohnung durch Zusteller

Die Anfertigung von Fotos der verpackten Ware in der Privatwohnung im Rahmen der Zustellung von Waren ist allenfalls über die Einwilligung datenschutzrechtlich zulässig. In diesem Fall sind die Anforderungen im Hinblick auf die Rechenschaftspflicht des Verantwortlichen zu dokumentieren.

Anweisungen des Verantwortlichen

Hintergrund der Beschwerde gegen ein Möbelhaus war eine Bestellung des Beschwerdeführers über den Online-Shop des Möbelhauses, die durch den vom Möbelhaus beauftragten Zusteller geliefert und in das Haus des Beschwerdeführers getragen wurde. Anschließend erstellte der Mitarbeiter des Zustellers im Haus des Beschwerdeführers ungefragt Fotos von der abgestellten verpackten Warenlieferung. Auf den Fotos waren Details der Wohnung des Beschwerdeführers zu erkennen. Weder im Vorfeld noch beim Liefervorgang wurde der Beschwerdeführer um sein Einverständnis zur Anfertigung und Verwendung der Fotos gebeten.

Auf Nachfrage erklärte das Möbelhaus als verantwortliche Stelle, dass es dem Zusteller mit dem Lieferauftrag auch den Vor- und Nachnamen sowie die Adresse des Kunden mitteilt, um diese Daten zur Lieferung zu verwenden. Nach der entsprechenden Arbeitsanweisung des Verantwortlichen für den Zulieferer sollte er Fotos von den angelieferten, noch verpackten Produkten nur dann anfertigen, wenn der Kunde die Bestätigung des Erhalts der Produkte mittels Abgabe einer Unterschrift verweigert oder wenn Beschädigungen der Produkte oder an Eigentum des Empfängers (als Folge der Anlieferung) erkennbar sind. Im Beschwerdefall lag aber keine der beiden Fallgruppen vor. Nach Aussage des Möbelhauses habe der Mitarbeiter des Zustellers die Fotos fälschlicherweise angefertigt.

Auf den Fotos dürfe gemäß der Arbeitsanweisung nur die ausgelieferte Ware, nicht der Kunde zu sehen sein. Nur im Fall der Beschädigung von Eigentum des Empfängers habe der Zulieferer vom Empfänger vor der Anfertigung der Fotos dessen Zustimmung einzuholen. Soweit gemäß der Arbeitsanweisung Fotos angefertigt würden, würden die Fotos dem digitalen Lieferschein zu-

gefügt, mit diesem abgespeichert und gemäß den gesetzlichen Aufbewahrungspflichten für zehn Jahre gespeichert und dann gelöscht.

Nach Auffassung des Verantwortlichen wurden mit der Anfertigung und Speicherung der Fotos im Rahmen des Lieferprozesses keine personenbezogenen Daten im Sinne der DS-GVO verarbeitet: Weder werde der Beschwerdeführer auf den Fotos abgebildet, noch sei er anhand der Fotos – unter Berücksichtigung weiterer Merkmale – identifizierbar. Die Fotos zeigten lediglich die verpackten Produkte in einem nicht näher definierbaren Raum. Zentrales Motiv der Fotos seien die verpackten Produkte, nicht die Räumlichkeiten, in denen sie sich befänden. Es sei nicht gesichert, dass es sich bei den auf den Fotos ausschnittsweise sichtbaren Räumen um Eigentum, Besitz oder von dem Beschwerdeführer tatsächlich allein bewohnte Räumlichkeiten oder nicht vielmehr um die Wohnung seiner Familie oder Hausgemeinschaft oder eines Dritten handele. Da die Produktfotos nach der Auffassung des Verantwortlichen keine personenbezogenen Daten darstellen, habe es keine entsprechenden Informationen des Kunden im Vorfeld gegeben und die Anfertigung, Übermittlung und Speicherung der Fotos habe auch keinen Eingang in das Verfahrensverzeichnis der verantwortlichen Stelle gefunden.

Zulässigkeit der Fotoaufnahmen

Für eine Anwendbarkeit der DS-GVO genügt jedoch eine Identifizierbarkeit der betroffenen Person gemäß Art. 4 Nr. 1 DSGVO. Das von einer Kamera aufgezeichnete Bild einer Person fällt unter den Begriff „personenbezogene Daten“, sofern es die Identifikation der betroffenen Person mittels Zuordnung zu einer Kennung – wie einem Namen – ermöglicht.[87] Dem Zusteller werden von der verantwortlichen Stelle der Vor- und Nachname und die Adresse des Kunden übermittelt. Im Falle der Anfertigung von Fotos ist der Kunde durch das Vorliegen dieser eindeutigen Kennung sowohl für den Zusteller als auch die verantwortliche Stelle identifizierbar. Die in Rede stehenden Fotos sind folglich im Rahmen des geschilderten Verarbeitungsprozesses personenbezogene Daten nach Art. 4 Nr. 1 DSGVO.

Die nach Art. 6 Abs. 1 DS-GVO erforderliche Rechtsgrundlage für die Erhebung, Übermittlung und Speicherung der Fotos fehlt jedoch.

Eine Einwilligung des Kunden wurde nicht eingeholt, so dass der Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO nicht in Betracht kommt.

Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO findet ebenfalls keine Anwendung, da die Verarbeitungen zwar im Zusammenhang mit einem Kaufvertrag über

87 S. z. B. BeckOK DatenschutzR/Schild DS-GVO Art. 4 Rn. 14 m. w. N.

die bestellten Möbel erfolgen, die Anfertigung von Fotos jedoch nicht für die Erfüllung des Kaufvertrags erforderlich ist.[88] Erforderlich für solche typischen Versandhandelsgeschäfte ist im Hinblick auf die Zustellung die Verarbeitung der Daten zum konkreten Kaufvorgang sowie zu Namen und Adresse des Käufers, um diesem die Ware übergeben oder liefern zu können. Händler oder Paketdienstleister haften zwar bei Verlust oder Beschädigung, wenn das Paket kontaktlos geliefert und im Hausflur abgelegt wird; wie der Verantwortliche in diesem Falle jedoch selbst ausführte, ist anhand der Fotos nicht gesichert, dass es sich bei den fotografierten Räumlichkeiten überhaupt um solche des Käufers und Beschwerdeführers handelt. Einen Beweiswert zur Freizeichnung einer etwaigen Haftung hinsichtlich einer tatsächlich vorgenommenen Lieferung und Übergabe an den Kunden kommt den Fotos entsprechend nicht zu: Fotos als Zustellbestätigung sind nicht unbedingt erforderlich, da ja auch im Falle der Weigerung der Abgabe einer Unterschrift (was wohl auch eher der Pandemie-Situation geschuldet war und somit im Weiteren keine Bedeutung mehr hätte) eine Bestätigung des Fahrers der Zustellung genügen würde. Auch schützen die Fotos nicht vor diebischen Fahrern, da sie lediglich beweisen, dass die Lieferung kurz am auf den Fotos abgebildeten Ort lag. Auch eine Beschädigung des Produkts oder am Eigentum des Empfängers (so die vom Verantwortlichen genannte weitere Fallgruppe) kann durch Fotos der eingepackten Ware nicht nachgewiesen werden und somit nicht für die korrekte Abwicklung des Kaufvertrags erforderlich sein.

Auch das berechtigte Interesse des Verantwortlichen ist nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO als weitere mögliche Rechtsgrundlage für die Verarbeitungen abzulehnen: Der Verantwortliche hat schon nicht ausreichend dargelegt, inwiefern ein berechtigtes Interesse an der Anfertigung der Fotos besteht und aus welchen Gründen die konkrete Datenverarbeitung in Form der Fotos zur Wahrung dieser Interessen auch tatsächlich erforderlich ist. Darüber hinaus ist im Hinblick auf die Schutzwürdigkeit der Betroffeneninteressen im Rahmen der vorzunehmenden Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO unbedingt zu berücksichtigen, dass hier mit der Anfertigung von Fotos in der Privatwohnung massiv in Grundrechte und Grundfreiheiten (Art. 13 Grundgesetz (GG), Art. 7 Charta der Grundrechte der Europäischen Union (GRCh), Art. 7 GRCh und Art. 8 Europäische Menschenrechtskonvention (EMRK)) der betroffenen Person eingegriffen wird. Auf den Fotos sind Details des Raumes in der Privatwohnung erkennbar und dieser wird eindeutig dem Betroffenen zugeordnet. Der Einwand des Verantwortlichen, hier sei nicht der höchstpersönliche Lebensbereich der

88 Das Kriterium der Erforderlichkeit ist grundsätzlich eng auszulegen – s. z. B. Kühling/Buchner/Buchner/Petri DS-GVO Art. 6 Rn. 38.

Person tangiert, ist nicht nachvollziehbar. Ein Überwiegen der Interessen des Verantwortlichen ist von diesem weder dargelegt worden, noch sind dafür Gründe im Hinblick auf die Schwere des Eingriffs für den Betroffenen zu erkennen.

Letztlich ist auch die Speicherdauer von solchen Fotos dem vom Verantwortlichen zu definierenden Zweck (mit engem Bezug zur Zustellung) anzupassen. Hier die allgemeine Frist für die Aufbewahrung des Lieferscheins von zehn Jahren anzusetzen, erscheint in jedem Fall nicht angemessen.

Nach entsprechenden Hinweisen an den Verantwortlichen sagte dieser zu, unverzüglich auf die Anfertigung von Fotos im Rahmen des Liefervorgangs zu verzichten und seine Arbeitsanweisung an die Zusteller entsprechend zu ändern.

Zusammenfassend ist festzuhalten, dass in derartigen Fällen die Anfertigung von Fotos in der Wohnung des Betroffenen allenfalls über den Weg der Einwilligung als Rechtsgrundlage denkbar ist. Will die verantwortliche Stelle diesen Weg gehen, so sind die Betroffenen im Vorfeld gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO für den bestimmten Fall und unmissverständlich zu informieren und müssten eine entsprechende eindeutige Erklärung oder Handlung vor Anfertigung der Fotos abgeben. Dieser Vorgang ist vom Verantwortlichen im Hinblick auf seine Rechenschaftspflicht gemäß Art. 5 Abs. 2 DS-GVO auch zu dokumentieren und auch in sein Verfahrensverzeichnis nach Art. 30 Abs. 1 DS-GVO aufzunehmen.

11.7
Versand von Zugangsdaten an veraltete Mobilfunknummer

Der Versand von Daten für den Online-Zugang (Online-Kennung) an Rufnummern aus einer früheren Geschäftsbeziehung ist datenschutzrechtlich unzulässig, sofern diese nicht erneut verifiziert wurde.

Der Beschwerdeführer und das Kreditinstitut unterhielten eine Geschäftsbeziehung, die bereits vor einigen Jahren beendet worden war. Die Bank archivierte die Kundendaten und speicherte diese zur Erfüllung der gesetzlichen Aufbewahrungsfristen. Dieses Vorgehen ist nach Art. 6 Abs. 1 Buchst. c DS-GVO nicht zu beanstanden.

In diesem Zusammenhang wurden auch die Kontaktdaten, wie die Mobilfunknummer des Beschwerdeführers, fortwährend gespeichert. Die Speicherung dieser Daten ist datenschutzrechtlich nicht zu beanstanden, da durch eine Archivierung des Kundendatensatzes und gleichzeitiger Sperrung für

die operativen Systeme dem Schutzbedürfnis des Betroffenen ausreichend Rechnung getragen wird.

Im Berichtsjahr hat der Beschwerdeführer dann ein neues Konto bei dem Kreditinstitut eröffnet, das den gesperrten, aber noch gespeicherten Datensatz zum Kunden reaktivierte. Hierbei wurden auch die Kontaktdaten aus der vorangegangenen Geschäftsbeziehung im operativen System reaktiviert.

Der Betroffene gab allerdings im Kontoeröffnungsantrag eine andere Rufnummer an, da er die Mobilfunknummer aus der vorherigen Geschäftsbeziehung gewechselt hatte. Das Kreditinstitut speicherte nunmehr zwei Rufnummern zum Betroffenen, wovon eine nicht mehr aktuell war. Der Kunde selbst wusste nichts von der fortwährenden Speicherung der „alten“ Rufnummer.

Im Rahmen der Kontoeröffnung versandte das Kreditinstitut standardmäßig die Online-Kennung an die zum jeweiligen Kunden hinterlegte Rufnummer. Sofern mehrere Rufnummern gespeichert wurden, erfolgte der Versand an sämtliche gespeicherten Mobilfunknummern per SMS.

Datenschutzrechtlich war dieses Vorgehen zu beanstanden. Nach Art. 5 Abs. 1 Buchst. f DS-GVO müssen personenbezogene Daten so verarbeitet werden, dass die Verarbeitung der Daten sicher gestaltet ist und unberechtigte Dritte diese nicht zur Kenntnis nehmen können:

Art. 5 DS-GVO

(1) Personenbezogene Daten müssen

(…)

f) 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“); (…)

Nach diesem Grundsatz sind entsprechende technische und organisatorische Maßnahmen zu implementieren, die ausreichenden Vertraulichkeitsschutz gewährleisten. Hierzu gehört auch, die Aktualität von Kontaktdaten zu prüfen, bevor diese verwendet werden.

Daher habe ich das Kreditinstitut dazu aufgefordert, grundsätzlich die Aktualität der Rufnummern vor Verwendung zu verifizieren. Das Verfahren wurde daraufhin entsprechend angepasst.

11.8
Biometrische Identifizierung

Bei der Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 DS-GVO ist Vorsicht geboten. Vertragsstrafen schließen eine „ausdrückliche Freiwilligkeit" im Sinne des Art. 9 Abs. 2 Buchst. a DS-GVO zwingend aus.

Mich erreichte eine Beschwerde, die sich gegen eine Fitnessstudiokette mit Sitz in Hessen richtete. Die Einlasskontrolle in den einzelnen Filialen wurde mit RFID-Armbändern mit einem personalisierten RFID (Radio-Frequency-Identification)-Chip realisiert, die den Mitgliedern zu Vertragsbeginn ausgehändigt wurden. Bei einem RFID-System handelt es sich um ein Verfahren zur automatischen Identifizierung von Objekten über Funk. Obschon RFID-Systeme in unterschiedlichsten Varianten existieren, ist jedes RFID-System im Kern durch die folgenden Eigenschaften definiert: Das System ermöglicht eine eindeutige Kennzeichnung von Objekten durch spezifische Daten, die im Chip elektronisch gespeichert sind. Diese können dann zur Identifikation des Objekts über einen Funkfrequenzkanal ausgelesen werden. Das gekennzeichnete Objekt sendet seine Daten nur dann, wenn ein dafür vorgesehenes Lesegerät diesen Vorgang abruft.[89] Neben einem Bild des jeweiligen Mitglieds wurden im konkreten Fall Abdrücke von mehreren Fingern mittels eines elektronischen Lesegeräts angefertigt und hinterlegt. Das Armband wird beim Einlass gegen ein fest installiertes Lesegerät gehalten. Der Benutzer muss im Anschluss einen seiner Finger auf einen unter dem Lesegerät befindlichen Fingerprintsensor legen, wo dieser gescannt wird. Eine Widerspruchsmöglichkeit war dem Beschwerdeführer nicht bekannt.

Nachdem ich die verantwortliche Stelle zur Stellungnahme aufgefordert hatte, wurde mir mitgeteilt, dass durch die Daten auf dem RFID-Armband die Möglichkeit der schnellen Zuordnung des jeweiligen Mitglieds (mit Armband) zur Zutrittskontrolle garantiert sei. Dies geschehe, indem die Daten auf dem Armband das jeweilige Mitglied mit der Mitgliedersoftware verbinde und somit eine sichere und sofortige Zuordnung möglich sei. Das Armband wird alleiniges Eigentum des Kunden. Hinsichtlich der Anfertigung eines Mitgliederfotos bestehe eine Widerspruchsmöglichkeit. Hiernach könne ein dem Mitglied zuordenbarer Gegenstand fotografiert werden, nach dem das Mitglied dann beim „Check-In" gefragt wird.

89 S. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/RFID/rfid_node.html.

Das Template des Fingerabdrucks, das für die Zuordnung des Mitgliedsarmbandes nötig ist, sei nur auf dem vom Mitglied erworbenen Mitgliedsarmband gespeichert, so dass keine Verbindung zwischen der Clubverwaltungssoftware und dem einzelnen Fingerabdruck hergestellt werden könne. Hierzu würden sichere Verschlüsselungstechnologien zum Einsatz kommen. Dies erfolge anhand von Vektoren in bestimmten Sektoren im Speicher des internen Chips des Datenträgers. Diese Bereiche seien speziell über „Crypt Keys“ vor externen Zugriffen gesichert.

Sofern ein (potenzielles) Mitglied des Fitnessstudios der Verarbeitung von Fingerabdrücken widersprochen hatte, erhielt es vom Fitnessstudio ein separates Dokument, das dann vom Mitglied unterzeichnet werden musste. Der Inhalt des Dokuments lautete wie folgt:

> *„Hiermit bestätige ich, dass auf meinem Mitgliedsarmband, auf meinen ausdrücklichen persönlichen Wunsch hin, mein Fingerabdrucksfoto zur Identifikation NICHT gespeichert wird. Mir ist bewusst, dass das Armband damit nicht nur durch mich, sondern auch durch andere, denen ich die Karte bewusst oder unbewusst oder durch Verlust oder gar Diebstahl überlasse, zum Eintritt in den Club missbraucht werden kann. Mit meiner Unterschrift akzeptiere ich die folgende Regelung der […]: ‚Die Nutzung der Karte und damit das Training in unserem Studio ist nur Ihnen oder dem vertraglichen Nutzer höchstpersönlich gestattet. Bei jedem Verstoß gegen diese Pflicht verlangt […] von Ihnen einen pauschalierten Schadensersatz von € 250,-. Sofern sie nachweisen können, dass durch den Missbrauch der Karte kein oder nur ein geringerer Schaden entstanden ist, schulden Sie nur den geringeren nachgewiesenen Betrag.‘“*

Als Rechtsgrundlagen für die Datenverarbeitung wurden vom Verantwortlichen folgende Normen genannt:

– Kontrolle der Nutzung der vertraglich zugesicherten Leistungen und dessen Nachweis der Leistungserbringung zur Erfüllung eines Vertrags aus Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO,
– Kontrolle des Zutritts nur durch berechtigte, vertraglich gebundene Mitglieder & Wahrung des Hausrechts und Schutz der Mitglieder nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO sowie
– Prävention § 265a StGB – Erschleichen von Leistungen.

Nach Prüfung der Stellungnahme forderte ich den Verantwortlichen aus folgenden Gründen auf, die Erfassung und Verarbeitung der Fingerabdrücke umgehend einzustellen.

Eine Verarbeitung des Fingerabdrucks findet unzweifelhaft statt. Beim sogenannten „Enrollment“ wird der Fingerabdruck von dem verwendeten Gerät gelesen, auch wenn jenes Gerät nicht netzwerktechnisch angebunden sein mag und ein unbefugter Zugriff dadurch weniger wahrscheinlich sein dürfte, als etwa bei einer Speicherung in einer Datenbank des Herstellers. Danach wird eine numerische Repräsentation auf dem Chip gespeichert. Beide Schritte sind Verarbeitungen von Daten des Fingerabdrucks.

Bei Fingerabdrücken handelt es sich um biometrische Daten gem. Art. 4 Nr. 14 DS-GVO. Diese unterliegen nach Art. 9 Abs. 1 DS-GVO einem besonderen Schutz im Sinne eines generellen Verarbeitungsverbots. Art. 9 Abs. 2 DS-GVO normiert eine Reihe von Erlaubnistatbeständen, die das Verarbeiten biometrischer Daten unter gewissen engen Voraussetzungen zulassen. In diesem Fall kommt nur eine Verarbeitung aufgrund einer „ausdrücklichen Einwilligung“ der betroffenen Person im Sinne des Art. 9 Abs. 2 Buchst. a DS-GVO in Betracht. Diese Einwilligung muss gemäß Art. 4 Nr. 11 DS-GVO „freiwillig“ erfolgen. Nach Art. 7 Abs. 4 DS-GVO scheitert die Freiwilligkeit der Einwilligung daran, wenn die Erfüllung eines Vertrags von einer Einwilligung in eine Datenverarbeitung abhängig gemacht wird, die nicht für die Vertragserfüllung erforderlich ist. Eine Einwilligung ist demnach nicht freiwillig, wenn der Betroffene faktisch keine andere Wahl hat, als der Datenverarbeitung zuzustimmen, um in den Genuss einer Dienstleistung oder einer anderen vertraglichen Leistung zu kommen.[90] Aufgrund dieses Koppelungsverbots steht der „pauschalisierte Schadensersatz“ in Höhe von 250 Euro der freiwilligen Einwilligung des Art. 9 Abs. 2 Buchst. a DS-GVO insofern entgegen, als dass davon auszugehen ist, dass ein Großteil der Kunden unter Androhung einer möglichen Vertragsstrafe zur Vermeidung derselben der Verarbeitung zustimmt. Mithin scheidet Freiwilligkeit aus.

Da kein weiterer Erlaubnistatbestand des Art. 9 Abs. 2 DS-GVO einschlägig ist, mangelt es an einer Rechtsgrundlage. Überdies lässt sich die Vermeidung von Missbrauch sowie die Kontrolle des Zutritts mit milderen Mitteln erreichen.

In der Folge wurde die Androhung der Vertragsstrafe bei Missbrauch aus der Einwilligung entfernt. Der Verantwortliche bietet die Nutzung des Fingerabdruckscanners auf freiwilliger Basis an, so dass dieser jederzeit widersprochen werden kann. Zusätzlich wurde ein Prozess eingeführt, nach dem die

90 S. z. B. Stemmer in: BeckOK Datenschutzrecht, Wolff/Brink/v. Ungern-Sternberg, 45. Edition, Rn. 42.

Mitarbeiter am Empfang jeden Kunden, der per Fingerabdruck in das Studio gelangt, ansprechen und prüfen, ob sie der Speicherung der Fingerabdrücke weiterhin zustimmen. Zusätzlich wurde ein Hinweisschild angebracht, das auf die Widerspruchsmöglichkeit hinweist.

12. Gesundheitsversorgung

Gesundheitsdaten sind besonders schützenswert, weil sie intensiv das Persönlichkeitsrecht betreffen und ein hohes Diskriminierungspotenzial aufweisen. Für sie ist mit besonderer Sorgfalt die informationelle Selbstbestimmung zu wahren. Gesundheitsdaten sind aber auch von besonderer Bedeutung, um für die Gesundheit von Menschen vorzusorgen, sie zu erhalten oder wiederherzustellen. Es geht also bei Gesundheitsdaten immer um einen Ausgleich zwischen dem Ermöglichen hilfreicher Datenverarbeitung und dem Schutz vor ungewollter oder unzulässiger Datenverarbeitung. Um diesen Ausgleich ging es auch bei der Stellungnahme der Datenschutzbeauftragten zum Gesundheitsdatennutzungsgesetz (GDNG) (Kap. 12.1). Ihn kann man auch erreichen, wenn man präventiv Klinik-Neubauten begeht und bereits weit vor der Aufnahme von Datenverarbeitungen auf eine datenschutzgerechte Gestaltung der Kliniken achtet (Kap. 12.2). Auch in der Alltagspraxis von Apotheken (Kap. 12.3) und Arztpraxen (Kap. 12.4) muss Datenschutz durchgesetzt werden.

12.1 Stellungnahme zum Gesundheitsdatennutzungsgesetz

Im Juli 2023 hat das Bundesgesundheitsministerium (BMG) einen Gesetzentwurf für ein Gesundheitsdatennutzungsgesetz (GDNG) veröffentlicht. Den GDNG-Gesetzentwurf habe ich gemeinsam mit den unabhängigen Datenschutzbehörden des Bundes und der Länder konstruktiv begleitet und auf Korrekturbedarf hingewiesen. Die mit dem Gesetzentwurf beabsichtige umfangreichere Nutzung von Gesundheitsdaten durch mehr Akteure muss den verfassungsrechtlichen Anforderungen entsprechen und das Recht auf informationelle Selbstbestimmung, insbesondere die Betroffenenrechte, wahren. Das Gesetz wurde am 14. Dezember 2023 vom Bundestag beschlossen und trat zum 26. März 2024 in Kraft.

Der Gesetzentwurf zum GDNG ist Bestandteil der Digitalisierungsstrategie für das deutsche Gesundheitswesen des BMG. Mit dem GDNG soll eine bessere Weiternutzung von Gesundheitsdaten über den Versorgungskontext hinaus ermöglicht werden, um dadurch die Potenziale der Daten des Gesundheitssystems zu nutzen. Für die Versorgung, öffentliche Gesundheit, Forschung und Innovation sollen hochqualitative und repräsentative Daten bereitgestellt werden.

Eine verbesserte Nutzung von Gesundheitsdaten zum Wohle der Allgemeinheit ist zu begrüßen und das Vorhaben daher grundsätzlich zu unterstützen.

Die gesetzlichen Neuregelungen müssen aber das besondere Schutzniveau der hier betroffenen Gesundheitsdaten berücksichtigen.

Als Co-Vorsitz der Taskforce Forschungsdaten habe ich mich daher federführend an der Stellungnahme der DSK zum GDNG beteiligt.[91] In der Stellungnahme sind auch die positiven Aspekte des GDNG, wie die Einführung eines strafbewehrten Forschungsgeheimnisses, dargestellt.

Erheblicher Korrekturbedarf am GDNG besteht aber z. B. hinsichtlich der Neuregelung datengestützter Auswertungen durch Kranken- und Pflegekassen in § 25b SGB V-E. Diese Auswertungen der Versicherten sollen zum individuellen Gesundheitsschutz, zur Verbesserung der Versorgung und zur Verbesserung der Patientensicherheit durchgeführt werden. Die Versicherten sollen individuell angesprochen werden, z. B. bei der Erkennung von Krebsrisiken. Eine Einwilligung der Versicherten ist hierbei aber nicht vorgesehen, sondern sie können dieser Datenverarbeitung nur widersprechen. Diese Neuregelungen bergen aufgrund der Möglichkeit einer umfassenden Profilbildung das Risiko von „gläsernen Versicherten“ mit umfassenden Beeinflussungs- und Diskriminierungsrisiken. Die DSK-Stellungnahme fordert daher die ersatzlose Streichung dieser Regelung. Im verabschiedeten Gesetz wurde diese Vorschrift jedoch beibehalten und mit einer strengen Zweckbindung versehen.

Außerdem soll mit dem GDNG auch eine Widerspruchsregelung für die Übermittlung pseudonymisierter Gesundheitsdaten aus der elektronischen Patientenakte an das Forschungsdatenzentrum des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM) eingeführt werden (§ 363 Abs. 5 SGB V-E). Bisher war hierzu eine Datenfreigabe der Versicherten vorgesehen.

Eine solche undifferenzierte Widerspruchslösung zu den vielfältigen im Gesetz vorgesehenen Nutzungszwecken nähme aber nicht angemessen auf den Schutzbedarf der aus der Gesundheitsversorgung stammenden Daten aus der elektronischen Patientenakte Rücksicht. Möchte der Gesetzgeber eine Widerspruchslösung anstatt einer Einwilligung nutzen, so muss er granulare Widerspruchsmöglichkeiten vorsehen. Der Bundestag hat die Regelung in der Gesetzesfassung jedoch im Wesentlichen beibehalten.

Die am 14. August 2023 veröffentliche Stellungnahme der DSK wurde von der Bundesregierung im Rahmen des Regierungsentwurfs zum GDNG vom 30. August 2023 berücksichtigt und hat einige datenschutzrechtliche Verbesserungen herbeigeführt. Es verbleiben aber Kritikpunkte am GDNG, insbesondere zu den umfangreichen Auswertungsmöglichkeiten der Krankenkassen.

---

91 https://www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf

In Art. 5 des GDNG-Referentenentwurfs war außerdem ein Zuständigkeitswechsel der Datenschutzaufsicht im Bereich der Sozialdaten und der klinischen Forschung zum Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) vorgesehen. Dieser Zuständigkeitsverlust der Landesdatenschutzaufsichtsbehörden begegnete erheblichen verfassungsrechtlichen Bedenken und hätte zu vielen Unklarheiten und Abgrenzungsproblemen in der Aufsichtstätigkeit geführt. Daher habe ich mich auch hier federführend an einer Stellungnahme der Landesdatenschutzaufsichtsbehörden zu diesem im GDNG geplanten Zuständigkeitswechsel beteiligt.[92]

Diese Stellungnahme war erfolgreich, da die im Referentenentwurf noch vorgesehene Neuregelung über die Zuständigkeitsverlagerung im Regierungsentwurf vom 30. August 2023 gestrichen wurde.

Durch die frühzeitige Positionierung der Datenschutzaufsichtsbehörden ist es gelungen, rechtzeitig Einfluss auf dieses wichtige Gesetzesvorhaben zu nehmen und die Betroffenenrechte zu stärken.

12.2
Begehung von Klinik-Neubauten

Im Berichtszeitraum habe ich die Begehung von Klinik-Neubauten als einen Schwerpunkt im Gesundheitswesen gewählt. Hierdurch konnte ich wertvolle Einblicke in den Krankenhausbereich erhalten und auf die Berücksichtigung des Datenschutzes, in diesem besonders sensiblen Bereich, hinwirken.

Im Rahmen des Schwerpunkts „Klinik-Neubauten“ fand am 29. März 2023 meine Begehung des Neubaus der Helios Dr. Horst Schmidt Kliniken in Wiesbaden (HSK Wiesbaden) statt. Daran schloss sich am 15. Juni 2023 meine Begehung des Neubaus des Varisano Klinikums Frankfurt Höchst an. Bei diesen Begehungen konnte ich einen Eindruck von den räumlichen und praktischen Gegebenheiten in den Kliniken vor Ort erlangen.

Der Neubau der HSK Wiesbaden war bei der Begehung noch nicht fertiggestellt, der Bezug war für Januar 2024 vorgesehen. Bei der Begehung dieses noch nicht in Betrieb genommenen Neubaus wurde daher durch mich in den Blick genommen, inwieweit bei der Planung und Umsetzung des Gebäudes den Belangen des Datenschutzes Rechnung getragen wurde.

Im Kontext der Begehung der HSK Wiesbaden wurde deutlich, dass bei Vorhaben dieser Größenordnung eine engmaschige Begleitung des Neu-

92 https://datenschutzkonferenz-online.de/media/st/23_08_10_Datenschutzaufsicht-Laender-zu-Art_5_GDNG-E.pdf.

bauprojekts durch einen Datenschutzbeauftragten sowie den operativen Datenschutz notwendig ist. Diese sollte möglichst frühzeitig und bis zur Inbetriebnahme erfolgen.

Der Umzug in den Neubau des Klinikums Höchst fand bereits im Februar 2023 statt. Mir konnten daher verschiedene Stationen im Krankenhausbetrieb vorgestellt werden. Bei einigen Themen wurde hierbei ein Verbesserungsbedarf identifiziert und mit dem Datenschutzbeauftragten des Klinikums erörtert. Die Umsetzung dieses Verbesserungsbedarfs war zum Ende des Berichtszeitraums bereits weitestgehend abgeschlossen.

Aus datenschutzrechtlicher Perspektive sind bei Klinik-Neubauten, ausgehend von den Erkenntnissen der Begehungen, insbesondere die folgenden Themen als wiederkehrende Herausforderungen zu identifizieren:

Vollständige Räumung der Patientenunterlagen im Altbau

Aus datenschutzrechtlicher Sicht ist bei dem Umzug eines Klinikbetriebs in ein neues Gebäude insbesondere darauf zu achten, dass in den alten Gebäuden keine personenbezogenen Patientendaten zurückbleiben, auf die ggf. unberechtigte Dritte Zugriff nehmen könnten. In der besonderen Ausnahmesituation eines Umzugs und der damit verbundenen Verlegung von Patientinnen und Patienten kann es dazu kommen, dass Dokumente vergessen werden. Nach dem Umzug sollte deshalb durch eine Begehung aller Stockwerke kontrolliert werden, dass keine Unterlagen mit personenbezogenen Daten zurückgelassen wurden.

Diskretion bei der Datenverarbeitung

Moderne Pflegestützpunkte und Empfangsbereiche der jeweiligen Stationen sind häufig patientenfreundlich und damit baulich offen gestaltet. Dies bedeutet, dass vereinzelt Einblicke in Arbeitsbereiche möglich sind. Im Zusammenhang mit solchen Arbeitsbereichen gibt es einige datenschutzrelevante Punkte, die von den Verantwortlichen zu beachten sind. Diese sind primär auf die Sicherstellung der Vertraulichkeit der Verarbeitung gemäß Art. 5 Abs. 1 Buchst. f i. V. m. Art. 32 Abs. 1 Buchst. b DS-GVO gerichtet.

So ist bei der Verwendung von Bildschirmen, auf denen personenbezogene Daten angezeigt werden können, darauf zu achten, dass diese nur für befugte Personen einsehbar sind. Dies kann in der Regel durch eine spezielle Ausrichtung der Bildschirme und die Verwendung von Sichtschutzfolien erreicht werden. Auch das regelmäßige automatische Sperren des Bildschirms nach kürzeren Zeiten der Inaktivität ist ein probates Mittel. Das Klinikum Höchst

hat auf meinen entsprechenden Hinweis zur Diskretion Sichtschutzfolien an den Bildschirmen der Pflegestützpunkte angebracht.

Ein Spezialfall möglicher unbefugter Zugriffe ergibt sich darüber hinaus auch dann, wenn mobile IT-Systeme zur Verarbeitung von personenbezogenen Daten verwendet werden. So kann es im Interesse des Klinikbetriebs liegen, bewegliche Computersysteme auf den Stationen einzusetzen, mit denen etwa Medikationspläne während der Visite verschiedener Patientenzimmer abgerufen werden können. Werden solche Systeme genutzt, muss auch für sie sichergestellt werden, dass außerhalb der Nutzung durch befugtes Klinikpersonal kein Zugriff auf die darauf gespeicherten personenbezogenen Daten möglich ist, etwa wenn ein solches System in einem öffentlich zugänglichen Bereich abgestellt wird. Das Klinikum Höchst hat hierzu weitere technische und organisatorische Maßnahmen, wie die durchgängige Beaufsichtigung mobiler Computersysteme in öffentlich zugänglichen Räumen und die Verschlüsselung von Medikationsplänen, getroffen.

Mehrere unterschiedliche Verantwortliche

In Kliniken arbeiten oft unterschiedliche datenschutzrechtliche Verantwortliche unter einem Dach zusammen. So sind für die Rettungsdienststellen, die Notarzt-, Rettungs- und Transportdienste ausführen, häufig die jeweiligen Hilfsorganisationen (z. B. Deutsches Rotes Kreuz, Johanniter-Unfall-Hilfe) datenschutzrechtlich Verantwortliche. Der Ärztliche Bereitschaftsdienst (ÄBD) wird in hessischen Kliniken von der Kassenärztlichen Vereinigung Hessen betrieben. Zudem nutzen ggfs. auch andere Leistungserbringer aus dem Gesundheitsbereich Räumlichkeiten des Klinikgebäudes (z. B. Medizinische Versorgungszentren).

Da es sich hierbei um unterschiedliche Verantwortliche handelt, bedarf jeder gegenseitige Zugriff auf personenbezogene Daten einer datenschutzrechtlichen Rechtsgrundlage und ist auf das notwendige Maß zu beschränken. Die Verantwortlichen müssen jeweils die Umsetzung der Datenschutzgrundsätze aus Art. 5 DS-GVO gewährleisten. Die jeweiligen Verantwortlichen sollten ausschließlich zum übrigen Klinikbetrieb abgrenzbare Räumlichkeiten nutzen. Außerdem sind auch die IT-Systeme und -Dienste der unterschiedlichen Verantwortlichen zu trennen.

Sind Beschäftigte in einer Klinik für mehrere Verantwortliche tätig, so muss das jeweilige Rechte- und Rollenkonzept dies unter Berücksichtigung des Grundsatzes der Erforderlichkeit und der Risiken für die Vertraulichkeit und die Integrität der Verarbeitung personenbezogener Daten aus der unbefugten Nutzung von Mitarbeiterzugängen abbilden.

Rohrpost

Viele Kliniken, wie etwa die HSK Wiesbaden und das Klinikum Höchst, nutzen auch noch in der heutigen Zeit aus Gründen der Zweckmäßigkeit und der Effektivität ein Rohrpostsystem. Hiermit können Blutproben und histologische Proben oder Nachrichten in Papierform in kürzester Zeit zwischen einzelnen Stationen versendet werden. Dieses System wird zur internen Übermittlung von Gesundheitsdaten, als besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO, genutzt.

Auch wenn es sich dabei um ein analoges System handelt, sind grundsätzlich die Anforderungen des Datenschutzes an die Verarbeitung personenbezogener Daten zu beachten. So können sich aus dieser Übermittlungsform Risiken für die Rechte und Freiheiten der betroffenen Personen ergeben, die mit denen beim Einsatz eines Fax vergleichbar sind (s. hierzu auch 50. Tätigkeitsbericht 2021, Kap. 18.5).

So ist es etwa denkbar, dass beim Versand ein falscher interner Empfänger angewählt wird oder sich bei der Empfangsstelle vorübergehend keine befugte Person befindet, welche die Nachricht entgegennehmen kann, so dass diese dort einige Zeit unbeaufsichtigt zugänglich sein könnte. Im Vergleich zu üblichen Anwendungsfällen eines Fax ist jedoch auch risikominimierend zu berücksichtigen, dass eine Nutzung des Rohrpostsystems ausschließlich klinikintern möglich ist und es dem Verantwortlichen somit unproblematisch möglich sein sollte, geeignete technische und organisatorische Maßnahmen zur Abmilderung dieser Risiken zu ergreifen.

Videoüberwachung

In Kliniken werden gelegentlich auch Videokameras eingesetzt, insbesondere zur Patientensicherheit. Die Videoüberwachung in einer Klinik führt aber aufgrund der hier betroffenen Gesundheitsdaten und des sensiblen Kontextes regelmäßig zu hohen Risiken für die Persönlichkeitsrechte der Patientinnen und Patienten. Daher ist vor dem Beginn der Videoüberwachung eine Datenschutzfolgenabschätzung nach Art. 35 DS-GVO notwendig.

Vor der Einrichtung einer Videoüberwachung ist zu prüfen, welche Notwendigkeit und welche berechtigten Interessen für die Videoüberwachung bestehen. Videokameras sind so auszurichten, dass nur die zwingend notwendigen Bereiche erfasst werden.

Die Patientinnen und Patienten sind mit Informationstafeln und Hinweisschildern transparent über die Videoüberwachung zu informieren.

Der Einsatz von Videoüberwachung in einer Klinik ist außerdem regelmäßig zu evaluieren, insbesondere im Hinblick auf die Erforderlichkeit. Im Klinikum

Höchst war z. T. eine Videoüberwachung für bestimmte Bettenwarten mit Patienten vorgesehen. Die entsprechenden Stellen waren dann aber im Praxisbetrieb nicht als solche genutzt worden. Eine Videoüberwachung zum Zwecke der Patientensicherheit war damit im Echtbetrieb nicht mehr erforderlich und konnte entgegen der ursprünglichen Planung entfallen. Das Klinikum Höchst hat die entsprechenden Videokameras deaktiviert und die Informationstafeln überarbeitet.

Datenschutzkonforme Entsorgung von Dokumenten

In Klinik-Neubauten erfolgt die Verarbeitung der Patientendaten häufig volldigitalisiert. Dennoch kann nicht zuverlässig ausgeschlossen werden, dass in bestimmten Bereichen und Einzelfällen schriftliche Dokumente mit personenbezogenen Daten genutzt werden. Für diese Dokumente sind verschließbare Datenschutztonnen vorzusehen, damit entsorgte Dokumente nicht mehr aus dem Müll „gefischt“ werden können.

In der Zentralen Notaufnahme des Klinikums Höchst wurde bei der Begehung der Alarmausdruck eines Notruf-Einsatzes vorgefunden. Hierbei handelte es sich um ein externes Dokument eines Rettungsdienstes, auf dem der Ort des Rettungseinsatzes und die Diagnose erkennbar waren. Das Dokument werde vom Klinikum datenschutzkonform entsorgt. Ich habe das Klinikum in diesem Kontext gebeten, noch einmal zu prüfen, ob ausreichende Prozesse zum Umgang mit externen Dokumenten implementiert sind (z. B. im Rahmen einer Verfahrensanweisung).

Auf einer Station des Klinikums Höchst war zudem für die Entsorgung des „Datenschutz“-Papiermülls ein normaler Mülleimer vorgesehen. Der Einsatz solch normaler Mülleimer sei nach Auskunft des Klinikums der Übergangzeit nach dem Umzug geschuldet, denn im gesamten Klinikum sollten verschließbare Datenschutz-Container installiert werden. Ich habe darauf hingewirkt, dass dies unverzüglich umgesetzt wird. Das Klinikum Höchst hat mir nach der Begehung eine Verfahrensanweisung zur Entsorgung von Datenschutzabfall und Abfall mit vertraulichen Informationen vorgelegt und das Aufstellen von 45 Sicherheitstonnen eines Entsorgers für den Datenschutzabfall bestätigt.

IT-Sicherheit

Bei großen Kliniken handelt es sich regelmäßig auch um eine KRITIS-Infrastruktur nach § 2 Abs. 10 BSIG. Betreiber Kritischer Infrastruktur haben nach § 8a BSIG besondere Anforderungen an organisatorische und technische Maßnahmen zu beachten. Für Krankenhäuser gibt es einen branchenspezifischen Sicherheitsstandard (B3S), der gegenüber dem BSI als Nachweis

der KRITIS-Anforderungen genutzt werden kann. Einige Vorkehrungen aus diesem Sicherheitsstandard können sich mit datenschutzrechtlichen Vorgaben überschneiden, insbesondere mit Blick auf die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO.

Wenngleich die KRITIS-Eigenschaft einer Stelle oder auch die Umsetzung daraus resultierender Anforderungen aus datenschutzrechtlicher Sicht nicht als Nachweis der Erfüllung der Anforderungen des Datenschutzes akzeptiert werden können, ist festzustellen, dass die entsprechenden Umsetzungs- und Nachweispflichten gegenüber dem BSI es dem Verantwortlichen im Allgemeinen auch erleichtern sollten, seinen datenschutzrechtlichen Pflichten nachzukommen.

Fazit

Insgesamt haben die Neubauten der HSK Wiesbaden und des Klinikums Höchst aus datenschutzrechtlicher Sicht einen guten Eindruck vermittelt. Bei den Begehungen war erkennbar, dass der Datenschutz schon bei der baulichen Gestaltung an vielen Stellen mitgedacht wurde. In den beiden Begehungsterminen konnte ich Fragen seitens der Kliniken im Rahmen einer niederschwelligen Beratung beantworten und Hinweise geben. Durch diesen präventiven Ansatz können Datenschutzverletzungen im Zusammenhang mit den Neubauten und Umzügen des Klinikbetriebs effektiv verhindert werden. Im Rahmen meines gesetzlichen Beratungsauftrags empfehle ich daher grundsätzlich, eine Beratung durch meine Behörde in Anspruch zu nehmen. Dies zum Beispiel dann, wenn spezifische Fragen zu klären oder Aspekte zu betrachten sind, die nach einer Konsultation der organisationsinternen Ressourcen – insbesondere des betrieblichen Datenschutzbeauftragten – noch offen sind.

12.3
Datenschutz in der Apotheke

Auch in Apotheken dürfen für legitime Zwecke erhobene Daten nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine angemessene Sicherheit der personenbezogenen Daten muss auch gewährleistet sein, wenn Daten gelöscht oder vernichtet werden sollen.

Post vom Apotheker

Eine Beschwerdeführerin schilderte folgenden Sachverhalt: In ihrem Briefkasten habe sie einen an sie adressierten Brief gefunden. Aus dem Inhalt konnte sie schließen, dass es sich bei dem Absender um den ortsansässigen

Apotheker handelte, bei dem sie einige Tage zuvor ein Rezept eingelöst hatte. Mit dem Brief versuchte der Apotheker, ihr privat näher zu kommen und Kontakt zu knüpfen. Die Kontaktaufnahme hatte allerdings nicht den gewünschten Erfolg und führte stattdessen zu ihrer Beschwerde bei mir. Sie habe zu keinem Zeitpunkt dem Apotheker ihre Adressdaten gegeben oder ihm erlaubt, ihre Daten für private Zwecke zu nutzen. Der Apotheker habe wohl die Adressdaten genutzt, die auf Rezepten neben dem verordneten Medikament mit aufgedruckt sind.

Nach Art. 5 Abs. 1 Buchst. b DS-GVO müssen personenbezogene Daten „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden".

Die Rezeptdaten dürfen zur Einlösung des Rezeptes verwendet werden. Adressdaten können z. B. für die Lieferung eines Medikamentes erforderlich sein. Eine Nutzung der Daten zu einer privaten Kontaktaufnahme ist jedoch keine Verarbeitung, die mit dem ursprünglichen Zweck der Datenerhebung vereinbar ist. Der Brief des Apothekers diente nicht zur Abwicklung der Kundenbeziehung, daher kommt die Rechtsgrundlage zur Erfüllung einer vertraglichen Beziehung gem. Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO, nicht in Betracht. Auch ein überwiegendes Interesse des Apothekers gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO liegt nicht vor, die Rezeptdaten für den Privatkontakt zu nutzen.

Eine Nutzung wäre allenfalls dann zulässig gewesen, wenn er die betroffene Person explizit gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 Abs. 1 DS-GVO gefragt und diese eingewilligt hätte, was jedoch nicht der Fall war.

Damit war eine Verwendung der Adressdaten außerhalb der Rezepteinlösung ohne die Einwilligung der Betroffenen unzulässig und stellte damit einen Verstoß gegen Art. 5 Abs. 1 Buchst. b, 6 Abs. 1 UAbs. 1 Buchst. a und 7 Abs. 1 DS-GVO dar.

Da der Apotheker sich einsichtig zeigte und versicherte, dass dies ein Einzelfall war, habe ich von einem Verfahren zur Verhängung einer Geldbuße abgesehen und den Apotheker gemäß Art. 58 Abs. 2 Buchst. b DS-GVO verwarnt. Zudem habe ich darauf aufmerksam gemacht, dass zukünftige vergleichbare Verstöße nach Art. 83 Abs. 5 DS-GVO mit einer Geldbuße geahndet werden können.

Umgang einer Apotheke mit zu vernichtenden Dokumenten

In einer Beschwerde wurde mir geschildert, dass eine Apotheke eine Datenmülltonne, über die Dokumente mit Gesundheitsdaten entsorgt werden, in

einem ohne Weiteres zugänglichen Innenhof einer Wohnanlage aufgestellt habe. Dieser Aufstellungsort sei besonders ungeeignet, da die Apotheke Drogenabhängige substituiere. Drogenabhängige seien bereits mehrfach im Innenhof angetroffen worden. Darüber hinaus werden Dokumente mit sensiblen Gesundheitsdaten auch über die im Hof stehenden Altpapiercontainer der Wohnanlage entsorgt.

Die Schilderungen veranlassten mich, kurzfristig unangekündigt die Apotheke aufzusuchen, um den Sachverhalt vor Ort aufzuklären und ggf. Abhilfe zu schaffen.

Die in der Eingabe erwähnte Datenmülltonne und die Altpapiercontainer befanden sich zum Zeitpunkt meiner Begehung tatsächlich im Innenhof einer Wohnanlage. Der Innenhof wurde von den Bewohnern und Besuchern der Wohnanlage und der Apotheke genutzt und war nur über eine Tür mit Schließanlage zugänglich. Bei meinem unangekündigten Besuch fand ich in den den Bewohnern und Besuchern zugänglichen Altpapiercontainern Schreddergut der Apotheke, allgemeinen Müll der Bewohner und allgemeine Post.

Unterlagen mit personenbezogenen Daten, die sich Kunden der Apotheke zuordnen ließen, habe ich zu diesem Zeitpunkt nicht gefunden. Eine zusätzliche von der Apotheke genutzte Datenmülltonne befand sich neben den Altpapiercontainern. Sie war mit einem Vorhängeschloss versehen und zur Hälfte gefüllt.

Durch die Aufstellung im Innenhof war die Datenmülltonne allerdings Tag und Nacht allen Bewohnern und Besuchern der Anlage zugänglich ist. Sie ließe sich hier leicht wegrollen und entwenden. Mit geringer krimineller Energie wäre es auch möglich, das Vorhängeschloss zu öffnen oder über den Einwurfschlitz an einzelne Dokumente zu gelangen. Ein ausreichender Diebstahlschutz war nicht gegeben.

Ich habe daher gefordert, dass die Datenmülltone entweder im Außenbereich gesondert zu sichern ist (abschließbarer Verschlag) oder durchgängig in den Räumlichkeiten der Apotheke zu verwahren ist. Auf diese Weise kann sichergestellt werden, dass Unbefugte keine Möglichkeit haben, sich Zugang zu dem Inhalt der Tonne zu verschaffen. Es sollte im Übrigen noch einmal schriftlich für die Mitarbeiter festgelegt werden, für welche Art von Datenmüll die übrigen Mülltonnen genutzt werden dürfen. Die Apotheke sagte vor Ort zu, eine entsprechende Lösung umzusetzen.

Die „Löschung und Vernichtung“ von personenbezogenen Daten fällt gemäß Art. 4 Nr. 2 DS-GVO unter den Verarbeitungsbegriff der DS-GVO. Nach Art. 5 DS-GVO müssen personenbezogene Daten entsprechend den in Abs. 1 Buchst. a bis f enthaltenen Grundsätzen verarbeitet werden. Dabei muss die

Verarbeitung in einer Weise erfolgen, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

Neben der Möglichkeit, zu vernichtende Unterlagen direkt zu schreddern, besteht die Möglichkeit, durch einen zertifizierten Entsorgungsbetrieb eine verschlossene Papiertonne aufstellen zu lassen, bei der die fachgerechte Entsorgung des Inhalts vertraglich und organisatorisch sichergestellt ist. Dabei ist allerdings auch zu beachten, dass die Datenmülltonne so aufgestellt wird, dass diese angemessen sicher verwahrt wird, damit nicht Unbefugte Zugang erlangen können.

Die Apotheke hat meine Forderungen umgehend umgesetzt. Für die sichere Datenvernichtung gib es dokumentierte Prozessbeschreibungen und Arbeitsanweisungen. Der Prozess und die damit verbundenen Arbeitsanweisungen sind, nach Angabe der Apotheke, ebenfalls Gegenstand der Schulungen bei Aufnahme der Arbeitstätigkeit und ggf. von Folgeschulungen. Die Einhaltung werde laufend überwacht, z. B. durch Stichprobenkontrollen der Altpapiercontainer und der Datenmülltonne. Die Inhalte der Datenmülltonne werden regelmäßig von einem auf Aktenvernichtung spezialisierten Dienstleister entsorgt. Die von der Apotheke getroffenen Maßnahmen habe ich als ausreichend erachtet und von weiteren aufsichtsrechtlichen Maßnahmen abgesehen.

12.4
Datenschutz in Arztpraxen

In mehreren Fällen gab es im Berichtsjahr Anlass, Verfahren zur Verhängung von Geldbußen gegen hessische Arztpraxen einzuleiten. Durch einen sorgfältigeren Umgang mit den Patientendaten wären diese Fälle zu verhindern gewesen.

Google-Rezensionen

Mehrfach gingen bei mir Beschwerden ein, in denen Arztpraxen auf negative Google-Rezensionen geantwortet und dabei Patientendaten preisgegeben haben.

Im ersten Fall habe ich den Hinweis eines Bürgers erhalten, dass eine Zahnarztpraxis auf eine anonyme Rezension zu ihrer Praxis auf „google.com“ den Patienten mit Nachnamen angesprochen und somit Patienten- und Behandlungsdaten offenbart hatte. Tatsächlich äußerte sich der Patient negativ über die Organisation der Praxis und über die zu hohen Kosten für seine Behandlung unter einem Pseudonym. Dabei beschrieb er auch ein

Detail seiner Erkrankung. Die Praxis antwortete darauf und sprach den Patienten mit seinem Nachnamen an. Dadurch konnten die von dem Patienten genannten Behandlungsdetails diesem zugeordnet werden.

Schon bei der Tatsache, bei einem bestimmten Arzt in Behandlung gewesen zu sein, handelt es sich um ein Gesundheitsdatum im Sinne von Art. 4 Nr. 15 DS-GVO.

Art. 4 Nr. 15 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

15. „Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Durch die Nennung des Namens des Patienten auf der Internetseite „www.google.com" wurde diese Tatsache durch die Arztpraxis offengelegt. Zudem wurden die Angaben des Patienten bezüglich seiner Behandlung auf diese Weise mit seinem Namen verknüpft und mithin de-anonymisiert.

Ich habe daher einen Verstoß gegen Art. 9 Abs. 1 DS-GVO festgestellt und ein Verfahren zur Verhängung einer Geldbuße eingeleitet.

Art. 9 Abs. 1 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.

In einem weiteren Fall hat die Beschwerdeführerin angegeben, dass sie eine Arztpraxis anonym auf „Google" rezensiert und die Arztpraxis darauf unter Nennung ihres Namens geantwortet habe. Dem widersprach die Praxis. Sie gab an, die Beschwerdeführerin habe ihre Kritik unter ihrem Klarnamen veröffentlicht. Erst als die Praxis sich darauf äußerte und die Beschwerdeführerin mit ihrem Namen ansprach, habe diese ihren Namen aus ihrer ursprünglichen Rezension gelöscht und sich an meine Behörde gewandt.

Aus der veröffentlichten Rezension und dem Kommentar der Praxis darauf ließ sich nicht ersehen, ob hier zunächst der volle Name der Beschwerde-

führerin angegeben wurde. Einen Nachweis für ihre Behauptungen haben weder die Beschwerdeführerin noch die Praxis erbracht.

Auch wenn man zu Gunsten der Praxis davon ausgeht, dass die Beschwerdeführerin erst im Zuge der Beschwerde den Klarnamen gelöscht hat, ist aus meiner Sicht die Veröffentlichung des vollen Namens der Beschwerdeführerin durch die Praxis ab dem Zeitpunkt der Löschung durch die Beschwerdeführerin rechtswidrig. Letztlich war ab diesem Zeitpunkt der Name nicht mehr offensichtlich öffentlich gemacht, im Sinne des Art. 9 Abs. 2 Buchst. e DS-GVO.

Art. 9 Abs. 2 Buchst. e DS-GVO

(2) Absatz 1 gilt nicht in folgenden Fällen:

(…)

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

Die Praxis hat auf meinen Hinweis hin ihre Antwort auf die Rezension abgeändert. Im Hinblick auf die Offenlegung des Namens der Beschwerdeführerin durch die Praxis auf „google.com“ für den Zeitraum ab der Löschung ihres Namens durch die Beschwerdeführerin habe ich einen Verstoß gegen Art. 9 Abs. 1 DS-GVO festgestellt. Auch hier wurde ein Verfahren zur Verhängung einer Geldbuße eingeleitet.

In weiteren Fällen habe ich die Antworten von Ärztinnen und Ärzten für datenschutzkonform erachtet. Hier wurde lediglich auf die bereits durch die Beschwerdeführer freiwillig veröffentlichten Daten Bezug genommen (Art. 9 Abs. 2 Buchst. e DS-GVO). Die Verarbeitung erfolgte auf der Grundlage von Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO. Hiernach ist die Verarbeitung personenbezogener Daten 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.

Alte Überweisungsträger neu bedruckt

In einem Fall hat eine Ärztin Atteste auf der Rückseite von alten Überweisungsträgern anderer Patienten ausgestellt. Die alten Patientendaten wurden dabei mit Kugelschreiber durchgestrichen, konnten jedoch leicht entziffert werden. Dem Fall lag der Hinweis eines Arbeitgebers zugrunde. Eine seiner Mitarbeiterinnen hatte ihm eine von der Ärztin ausgestellte Arbeitsunfähigkeitsbescheinigung vorgelegt. Auf der Rückseite der Arbeitsunfähigkeitsbescheinigung befand sich eine alte Überweisung einer anderen Patientin aus

dem Jahr 2019. Der Überweisungsschein enthielt Angaben zum Namen, Adresse, Versicherung und Versichertennummer, dem ausstellenden Arzt sowie zur Diagnose/Verdachtsdiagnose und dem entsprechenden Auftrag. Die Angaben zum Namen, zur Adresse und zum Geburtsdatum wurden auf dem Überweisungsschein mit Kugelschreiber durchgestrichen, waren jedoch ohne weiteres lesbar.

Bei meiner Anhörung zum Sachverhalt zeigte sich die Ärztin einsichtig und sagte zu, künftig nur noch neutrales Papier zu verwenden. Allerdings erreichte mich nur wenige Wochen später ein erneuter Hinweis desselben Arbeitgebers. Seine Mitarbeiterin hatte eine weitere Arbeitsunfähigkeitsbescheinigung vorgelegt, auf deren Rückseite sich ein Überweisungsschein einer anderen Patientin aus dem Jahr 2019 befand. Auch hier waren die Angaben zum Namen, zur Adresse und zum Geburtsdatum sowie zur Versicherten-Nummer der Patientin mit Kugelschreiber durchgestrichen, konnten jedoch leicht entziffert werden.

Erneut habe ich die Ärztin auf den Verstoß hingewiesen. Darauf erwiderte diese, dass die Papierherstellung mit einem enormen Wasserverbrauch verbunden sei; aus diesem Grunde benutze sie so oft wie möglich bereits bedrucktes Papier.

Einen Monat später übermittelte derselbe Arbeitgeber zum dritten Mal eine Krankmeldung seiner Mitarbeiterin durch die Ärztin, die auf einem alten Überweisungsschein aus dem Jahr 2018 gedruckt wurde. Die nur dürftig mit Kugelschreiber durchgestrichenen Angaben konnten wieder leicht gelesen werden.

Hier habe ich einen Verstoß gegen Art. 5 Abs. 1 Buchst. f DS-GVO in Verbindung mit Art. 32 DS-GVO festgestellt. Gemäß Art. 5 Abs. 1 Buchst. f DS-GVO müssen personenbezogene Daten 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“). Nach Art. 32 DS-GVO hat der Verantwortliche 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 geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Je sensibler die personenbezogenen Daten sind, desto größer ist auch der Schutzbedarf, der bei der Auswahl der zu treffenden Maßnahmen zugrun-

dezulegen ist. Die Überweisungsscheine enthielten Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO. Diese sind gemäß Art. 9 Abs. 1 DS-GVO besondere Kategorien personenbezogener Daten und mithin besonders schützenswert. Hier reicht ein einfaches Durchstreichen der Angaben mit dem Kugelschreiber nicht aus. Die durchgestrichenen Daten aus den drei vorliegenden Überweisungsscheinen konnten leicht entziffert werden. Darüber hinaus enthielten die Überweisungsscheine weitere zahlreiche Angaben, die die Identifikation der betroffenen Personen ermöglichen (z. B. Geschlecht, Zeitpunkt der Überweisung, behandelnder Arzt, Diagnosen und Befunde).

Darüber hinaus habe ich einen dreifachen Verstoß gegen Art. 9 Abs. 1 DS-GVO festgestellt. Bei Angaben zu Diagnosen/Verdachtsdiagnosen, Befunden/Medikation sowie bei der Tatsache, bei einem bestimmten Arzt in Behandlung zu sein oder an einen überwiesen zu werden, handelt es sich um Gesundheitsdaten. Diese sind gemäß Art. 9 Abs. 1 DS-GVO besondere Kategorien personenbezogener Daten und dürfen nur unter den Voraussetzungen des Art. 9 Abs. 2 DS-GVO verarbeitet werden. Die Ärztin hat diese Gesundheitsdaten ohne Rechtsgrund zunächst gegenüber der Patientin offengelegt, die sie krankgeschrieben hatte. Da diese gezwungen war, die Arbeitsunfähigkeitsbescheinigungen ihrem Arbeitgeber vorzulegen, wurden die Daten auch diesem gegenüber offengelegt. Im Hinblick auf die festgestellten Verstöße habe ich ein Verfahren zur Verhängung einer Geldbuße eingeleitet.

Faxfehlversand

In zwei Fällen haben Arztpraxen jeweils mehrfach Patientendaten versehentlich an unbefugte private Stellen gefaxt. Auch nach Hinweis durch diese Stellen an die Praxen wurden die Fehlsendungen nicht eingestellt. Eine Meldung nach Art. 33 DS-GVO ist in beiden Fällen nicht erfolgt.

Der Hinweisgeber gab an, mehrfach fälschlicherweise Faxe einer Darmstädter Arztpraxis empfangen zu haben. Die irrtümlich zugesendeten Unterlagen enthielten Namen, Adressen, Geburtsdaten und medizinische Diagnosen von Patientinnen und Patienten. Alle Faxe waren an eine Arztpraxis in Offenbach adressiert gewesen. Zum Nachweis legte der Hinweisgeber drei Laborbefunde und fünf Arztbriefe vor, die im Februar 2022 an ihn gefaxt wurden. Auch erklärte er, dass er mehrfach telefonisch und zuletzt per E-Mail die Arztpraxis aufgefordert hatte, die Irrläufer abzustellen. Er hatte die Praxis auch auf ihre Pflicht aus Art. 33 Abs. 1 DS-GVO hingewiesen, die Verletzungen des Schutzes personenbezogener Daten an die zuständige Aufsichtsbehörde zu melden.

Nach Angaben der Arztpraxis habe diese daraufhin versucht, den Sachverhalt mit der Empfängerpraxis in Offenbach zu klären und zunächst den Versand

auf Briefpost umgestellt. Nach ca. vier Wochen sei ein Testlauf gemacht worden. Die Arztpraxis habe aus der Empfängerpraxis die Rückmeldung bekommen, dass alles wieder in Ordnung sei. Ab April 2022 wurden daher wieder Arztberichte gefaxt.

Anfang April 2022 ging bei dem Hinweisgeber erneut ein Fax mit entsprechendem Inhalt ein. Angesichts der wiederholten Vorfälle wandte sich der Hinweisgeber an mich. Nach dieser Eingabe und der bereits erfolgten Anhörung der Arztpraxis durch mich ging beim Hinweisgeber Mitte April ein weiterer Arztbrief der Arztpraxis per Fax ein.

Bei meiner Prüfung ließ sich anhand der Schilderungen der Arztpraxis nicht beurteilen, aus welchem Grund die gefaxten Patientendaten beim falschen Empfänger angekommen waren. Grundsätzlich denkbar sind etwa eine Fehleingabe der Zielnummer beim Versand, aber auch eine technische Ursache (Fehlleitung bei korrekter Zieleingabe).

Die Arztpraxis sicherte mir zu, dass sie nun den Kommunikationsdienst KIM (Kommunikation im Medizinwesen) über die Telematikinfrastruktur nutze. Die Empfängerpraxen, die noch nicht auf KIM umgestellt hätten, würden die Unterlagen über den Postweg erhalten.

Die Laborbefunde und Arztbriefe wurden ohne Rechtsgrundlage an den Hinweisgeber übermittelt. Insgesamt wurden Laborbefunde und Arztbriefe von zehn betroffenen Personen offengelegt. Zudem hat die Praxis durch die Faxnutzung gegen Art. 5 Abs. 1 Buchst. f in Verbindung mit Art. 32 DS-GVO verstoßen. Grundsätzlich weist der Faxversand vergleichbare Risiken auf, wie diese etwa auch beim unverschlüsselten Versand von E-Mail-Nachrichten gegeben sind. Die Nachrichten werden ungeschützt übertragen. Auch ist das Risiko gegeben, dass personenbezogene Daten wegen einer nicht korrekten Eingabe der Zielfaxnummer Dritten unbefugt offenbart werden können. Personenbezogene Daten, die einen besonderen Schutzbedarf aufweisen, sollen daher grundsätzlich nicht per Fax übertragen werden, wenn keine zusätzlichen Schutzmaßnahmen bei den Versendern und Empfängern implementiert sind. In diesem Fall haben sich die Risiken der Nutzung eines unsicheren Kommunikationsmittels verwirklicht, auch wenn sich im Nachhinein nicht feststellen lässt, aus welchem Grund die gefaxten Briefe beim falschen Empfänger angekommen sind.

Auch liegt ein Verstoß gegen Art. 33 Abs. 1 DS-GVO vor, da eine Meldung der Vorfälle durch die Arztpraxis nicht erfolgt ist.

Art. 33 Abs. 1 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.

Angesichts der hier übermittelten Arztbriefe an eine fachfremde private Stelle, die nicht der Schweigepflicht unterliegt, war hier von einem Risiko für die Rechte und Freiheiten natürlicher Personen auszugehen.

Im Hinblick auf die umfangreichen Verstöße habe ich ein Verfahren zur Verhängung einer Geldbuße eingeleitet.

Entsorgung von Patientendaten im öffentlichen Müllcontainer

Dem Fall lag ein Hinweis eines Anwohners aus Kassel zugrunde. Dieser meldete mir, dass eine Arztpraxis mit zwei Praxisinhabern in seiner Nachbarschaft wiederholt nicht ausreichend geschredderte Patientenunterlagen in der öffentlichen Papiertonne entsorge. Auch würden teilweise komplette Seiten entsorgt werden. Ich bin dem Hinweis nachgegangen und habe zunächst einen Verstoß gegen Art. 5 Abs. 1 Buchst. f in Verbindung mit Art. 32 Abs. 1 und 2 DS-GVO festgestellt.

Als verantwortliche Stelle unterliegt eine Arztpraxis (auch nach Abschluss der Behandlung) den Pflichten aus Art. 5 Abs. 1 Buchst. f DS-GVO und hat daher durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit personenbezogener Daten zu gewährleisten. Hierzu gehört auch, dass unbefugte Personen keinen Zugang zu den Daten haben dürfen. Welche Maßnahmen zum Schutz der Daten ergriffen werden müssen, hängt insbesondere von dem Risiko eines unberechtigten Zugriffs, der Art der Verarbeitung sowie der Bedeutung der Daten für die Rechte und Interessen der betroffenen Person ab. So sind bei der Beurteilung des angemessenen Schutzniveaus gemäß Art. 32 Abs. 1 und 2 DS-GVO insbesondere die Risiken durch unbefugte Offenlegung von und unbefugten Zugang zu personenbezogenen Daten zu berücksichtigen.

Da es sich bei Patientenunterlagen um Gesundheitsdaten handelt, ist es unzulässig, diese ohne besondere Vorkehrungen in einem öffentlich zugänglichen Container zu entsorgen. Auf meinen Hinweis hin hat die Arztpraxis ein externes Unternehmen für die fachgerechte Entsorgung von Patientenunter-

lagen beauftragt. Die Polizei Kassel hat zudem auf meine Bitte den Container wiederholt kontrolliert, um eventuelle weitere Verstöße festzustellen und zu unterbinden. Letztlich wurde auch hier ein Verfahren zur Verhängung einer Geldbuße gegen die beiden Ärzte eingeleitet.

13. 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. Dieser Ausgleich ist auch das Ziel der Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) und ihrer Taskforce Forschungsdaten (Kap. 13.1). Ihm diente auch die Beratung von Forschungsprojekten am Universitätsklinikum Frankfurt a. M. (Kap. 13.2), die Zusammenarbeit mit der Initiative Gesundheitsindustrie Hessen (Kap. 13.3) sowie die Stellungnahme zur Änderung des Hessischen Landesstatistikgesetzes (Kap. 13.4).

13.1
Erfolgreiche Arbeit der Taskforce Forschungsdaten der DSK

Die Taskforce Forschungsdaten der DSK hat auch im Berichtsjahr die DSK durch intensive Arbeit an unterschiedlichen Themen erfolgreich unterstützt. Da ich neben dem BfDI den Co-Vorsitz innehabe und am 20. September 2023 bereits die 10. Sitzung stattfand, soll im Folgenden sowohl ein kurzer Rückblick als auch ein Ausblick auf die weiteren Projekte der Taskforce erfolgen.

Die Taskforce Forschungsdaten

Die Taskforce Forschungsdaten wurde im Rahmen der 102. DSK im November 2021 gegründet (17 Zustimmungen). Hierzu gab es die folgende Verlautbarung der DSK:

> „1. Die DSK richtet als einheitlichen Ansprechpartner für die Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF) sowie für alle länderübergreifenden Datenschutzfragen der Verbundforschung im Übrigen eine ‚Task Force Forschungsdaten' ein.
>
> 2. Die Task Force wird wegen bisheriger Schwerpunkte gemeinsam vom HBDI als Vorsitzendem des AK Wissenschaft und Forschung und dem BfDI geleitet.
>
> 3. In der Task Force sollten neben dem AK Wissenschaft und Forschung die Arbeitskreise Gesundheit und Soziales, Internationaler

Datenverkehr sowie Technik vertreten sein; sie steht der Beteiligung weiterer Mitglieder bzw. Arbeitskreise der DSK offen."

Die Auftaktsitzung der Taskforce fand am 31. Januar 2022 statt. Seitdem tagte sie alle zwei Monate. Bis November 2023 fanden insgesamt elf reguläre Sitzungen statt.

Veröffentlichte Stellungnahmen

Die Taskforce Forschungsdaten hat die folgenden DSK-Veröffentlichungen maßgeblich vorbereitet und entworfen:

– DSK Entschließung (November 2022): „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung"[93]
– DSK Stellungnahme zum EHDS (März 2023): „Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Daten- schutzniveau der Datenschutz-Grundverordnung nicht aushöhlen"[94]
– DSK Stellungnahme zum Gesundheitsdatennutzungsgesetz – GDNG (August 2023)[95]
– DSK Entschließung zur gesetzlichen Regulierung medizinischer Register (November 2023)[96]
– DSK Entschließung zur Harmonisierung der Forschungsregelungen in Landeskrankenhausgesetzen (November 2023)[97]

Beratungen und behandelte Themen

Im Jahr 2022 hat die Taskforce die Forschungsinitiative RACOON intensiv beraten und hierfür einige Sondersitzungen durchgeführt. Die Abstimmung der beteiligten Aufsichtsbehörden war – auch wegen der unterschiedlichen

93 https://www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf.
94 https://datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf.
95 https://datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf.
96 https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf.
97 https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf.

landesrechtlichen Regelungen – sehr zeitintensiv (s. 51. Tätigkeitsbericht, Kap. 16.4).

Einen weiteren Dialog führte die Taskforce mit der TMF e. V./MII zum neuen Modul „Drittstaatentransfer“ der MII-Mustertexte der Medizininformatik-Initiative (MII). Im Februar 2023 fand hierzu ein Workshop mit der TMF in Berlin statt. Die TMF hat der Taskforce zudem im März 2023 das Forschungsdatenportal Gesundheit (FDPG) der MII vorgestellt. In der Taskforce fand des Weiteren ein Austausch zum MII-Anschluss der Universitätskliniken über die Datenintegrationszentren (DIZ) statt.

Zu erwähnen ist auch, dass ein regelmäßiger Austausch der Taskforce mit der AG BIO-IT, Big Data und E-Health des BIO Deutschland e. V. stattfindet. Die Taskforce Forschungsdaten hat wiederholt an Sitzungen der AG teilgenommen und dort zu Themen wie dem EHDS und dem GDNG referiert.

Aktuelle Projekte

Die folgenden Projekte sind momentan Gegenstand der Sitzungen der Taskforce Forschungsdaten:

– Die Taskforce Arbeitsgruppe „Transfertools“ erarbeitet derzeit eine Übersicht möglicher Übermittlungsgrundlagen nach Kapitel V DS-GVO für den weiteren Austausch mit der TMF/ MII im Anschluss an den gemeinsamen Workshop.
– Die Taskforce Arbeitsgruppe Genomdaten bereitet eine Entschließung zur Sekundärnutzung von Genomdaten, gemäß einem aktuellen Auftrag der DSK, vor.
– Fortsetzung des Dialogs mit dem Bundesministerium für Wirtschaft (BMWK) und Fachverbänden wie dem BDI e. V.; hierzu wurde ein Best Practice Papier zum multizentrischen Forschungsprojekt RACOON von der Taskforce finalisiert. Außerdem fand eine gemeinsame Sitzung von Taskforce und BDI und weiteren Vertretern von Interessenverbänden im Januar 2024 statt.

Ausblick

Die Taskforce Forschungsdaten wird auch im Jahr 2024 die DSK effektiv unterstützen, um zeitnah auf neue datenschutzrechtliche Fragestellungen und neue Gesetzesvorhaben aus dem Forschungsbereich reagieren und Datenschutzstrategien für die wissenschaftliche Forschung entwickeln zu können.

13.2
Forschungsprojekte am Universitätsklinikum Frankfurt a. M.

Im Berichtszeitraum habe ich einen intensiven Austausch mit dem Universitätsklinikum Frankfurt a. M. geführt und dabei verschiedene Forschungsprojekte kennengelernt. Von besonderem Interesse war für mich in diesem Zusammenhang auch die Einbindung des Universitätsklinikums Frankfurt a. M. in die Medizininformatik-Initiative (MII).

Um Einblicke in aktuelle Forschungsprojekte zu erhalten, hat mir das Universitätsklinikum Frankfurt a. M. (UKF) in mehreren Besprechungen verschiedene Forschungsprojekte vorgestellt. Hierzu fanden im Berichtszeitraum drei Besprechungen mit dem Institut für Medizininformatik (IMI) des UKF statt. Bei diesen Besprechungen wurden mir unterschiedliche Forschungsprojekte am IMI präsentiert (z. B. OSSE, Privacy Umbrella, SATURN) und datenschutzrechtliche Fragestellungen erörtert.

Mit dem System OSSE (Open-Source Registersystem für Seltene Erkrankungen) kann nach dem Baukastenprinzip ein individuelles Patientenregister für Seltene Erkrankungen erstellt werden. Das IMI stellt hierzu die Open-Source Software bereit und unterstützt die Betreiber der Register auch mit Muster-Dokumenten, insbesondere Patienteneinwilligungen und Datenschutzkonzepten. Das System OSSE nutzt die „Mainzelliste“ als Pseudonymisierungsdienst.[98]

Außerdem hat mir das IMI auch die Anbindung an die Medizininformatik-Initiative (MII) dargestellt und hierfür das Datenintegrationszentrum (DIZ) und die Nutzung des Broad Consent vorgestellt. In der MII arbeiten alle Universitätskliniken daran, dass Versorgung und Forschung in Deutschland näher zusammenrücken. Das UKF ist Teil des MII-Konsortiums „MIRACUM“.

Das DIZ in Frankfurt a. M. soll insbesondere im Rahmen der MII Routinedaten aus der Patientenversorgung digital vernetzen und für die medizinische Forschung verfügbar machen. Über das MII Forschungsdatenportal für Gesundheit (FDPG) können Forschende Zugang zu den Patientendaten für medizinische Forschungszwecke beantragen und Machbarkeitsanfragen stellen. Die Räumlichkeiten des DIZ wurden den Mitarbeitern meiner Behörde vorgestellt und die Datenflüsse beschrieben.

Bei zwei Forschungsprojekten mit Beteiligung des DIZ sei bereits das Verfahren der verteilten Auswertung erfolgreich angewandt worden. Die personenbezogenen Patientendaten mussten hierbei nicht das DIZ verlassen, sondern das DIZ erhielt von den Forschenden deren Skripte und lieferte ihnen nur die Ergebnisse zurück.

98 https://www.toolpool-gesundheitsforschung.de/produkte/mainzelliste.

Ich begrüße ausdrücklich den Einsatz solcher innovativen Forschungsmethoden, durch die kein Zugriff von externen Forschenden auf personenbezogene Daten nötig ist. Die Persönlichkeitsrechte der Bürgerinnen und Bürger müssen auch in der Forschung bestmöglich geschützt werden. Daher ist es nötig, dass solche Forschungsmethoden weiter in der Praxis erprobt werden.

Die Vertreter des UKF berichteten mir außerdem vom Einsatz der Broad Consent-Einwilligungsformulare am UKF. Hierzu wurden die Abläufe bei der Einholung des Broad Consent beschrieben. Das Broad Consent-Einwilligungsformular werde in der ersten Implementierungsphase bei ambulanten Aufnahmen durch die behandelnden Ärztinnen und Ärzte überreicht, diese stünden den Patientinnen und Patienten für Rückfragen zur Verfügung.

Eine wichtige Rolle für die Arbeit des DIZ wird auch die Treuhandstelle spielen, die sich noch im Aufbau befindet. Zu diesem Thema habe ich dem MII beratend datenschutzrechtliche Hilfestellung gegeben.

Gerade im Bereich der medizinischen Forschung ist es wichtig, einen Dialog mit den Forschenden zu führen, da diese die praktischen Gegebenheiten und Bedingungen am besten kennen. Der Austausch mit dem Universitätsklinikum Frankfurt a. M. hat dies erneut bestätigt. Die Informationen und Argumente aus der Praxis tragen dazu bei, fundierte datenschutzrechtliche Bewertungen treffen zu können.

Auch in Zukunft werde ich daher den Austausch mit den Forschenden fortsetzen.

13.3
Positionspapier Gesundheitsdaten der Initiative Gesundheitsindustrie Hessen

Eine Stärkung von Gesundheitsversorgung und Forschung im Einklang mit dem Datenschutz war in Hessen z. B. im Rahmen der Initiative Gesundheitsindustrie Hessen (IGH AG) möglich.

Ausgangslage

Im Rahmen der IGH AG sind im Berichtszeitraum viele Stakeholder aus Hessen aus den Bereichen Gesundheit, Wissenschaft und Forschung zusammengekommen. Das Vorbild für das Projekt ist die Roadmap Gesundheitsdatennutzung Baden-Württemberg, die es sich zum Ziel gesetzt hat, den Forschungs- und Versorgungsstandort Baden-Württemberg zu stärken und zukunftsfähig zu gestalten.[99] Auch im hessischen Projekt steht im Mittelpunkt

99 https://www.forum-gesundheitsstandort-bw.de/download_file/force/21093/84221.

die datenschutzgerechte, erleichterte Nutzbarkeit von Gesundheitsdaten für die Forschung auf Landesebene.

Herausforderungen und Ergebnisse

Eine erste Herausforderung für das Projekt war es, zunächst einen Überblick über die bestehende Gesetzgebung auf Länderebene, Bundesebene und europäischer Ebene zu geben. Ich habe hier meine Expertise einfließen lassen. Zudem konnte ich auf einige Leuchtturm-Projekte aus Hessen verweisen, die zeigen, dass die Forschung und Entwicklung im Gesundheitssektor sehr gut im Einklang mit dem Datenschutz möglich ist. Von Seiten der forschenden Unternehmen wurde letztlich Input gegeben, an welchen Stellen man sich eine Erleichterung der Datennutzung und einen verbesserten Zugang zu Daten wünscht.

Das durch die Kooperation erarbeitete finale Papier wurde am 13. Dezember 2023 veröffentlicht[100] und der Presse vorgestellt.[101] Im Ergebnis kann festgehalten werden, dass die meisten Forschungsprojekte aus dem Gesundheitsbereich ohne eine Absenkung von Datenschutzstandards umsetzbar sind. Wenn Hindernisse bestehen, kann diesen meist auf legislativer Ebene begegnet werden.

Ausblick

Für die großen Themen Digitalisierung, Telemedizin und KI kann das Positionspapier der IGH AG auch auf Landesebene sicher nur ein erster Schritt sein. Ich werde hier weiterhin die Gesundheitsunternehmen aus Hessen unterstützen und nach Lösungen suchen, die sowohl praxistauglich als auch datenschutzfreundlich sind.

100 https://digitales.hessen.de/sites/digitales.hessen.de/files/2023-12/gesundheitsdatenpapier_dezember_2023_barrierefrei.pdf.

101 https://www.gesundheitsindustrie-hessen.de/meldungen/digitalministerin-kristina-sinemus-stellt-gesundheitsdaten-papier-vor/.

14. 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, eine Abteilung für technisch-organisatorischen Datenschutz mit qualifizierten Mitarbeiterinnen und Mitarbeitern zu haben. Diese Abteilung habe ich entsprechend den aktuellen Herausforderungen und Aufgaben neu strukturiert (Kap. 14.1). Sie ist in ein Referat für die Beratung in Fragen des technisch-organisatorischen Datenschutzes (Kap. 14.2), in ein Referat für technische Datenschutzprüfungen (Kap. 14.3) und in ein Referat für die Begleitung von Datenschutzverletzungen (Kap. 14.4) gegliedert. Als Beispiel für Beratungen dienen die Kriterien für souveräne Cloud-Systeme (Kap. 14.5). Datenschutzverletzungen sind mir als Aufsichtsbehörde zu melden (Kap. 14.6). Ein gravierendes Beispiel für eine Datenschutzverletzung war ein gelungener Ransomware-Angriff auf eine hessische Kommune mit weitreichenden Schadensfolgen (Kap. 14.7). Eine wichtige Ursache für Datenschutzverletzungen kann die Nutzung von unsicheren privaten Apps oder Endgeräten zu dienstlichen Zwecken sein (Kap. 14.8).

14.1 Schwerpunktsetzung im technischen und organisatorischen Datenschutz

Die Aufgaben im technischen und organisatorischen Datenschutz haben sich verändert. Diesen veränderten Aufgaben habe ich auch die Struktur meiner Abteilung für technischen und organisatorischen Datenschutz angepasst.

Seit dem Wirksamwerden der DS-GVO am 25. Mai 2018 haben sich die Aufgaben im Bereich des technischen und organisatorischen Datenschutzes deutlich verändert. Wesentliche Tätigkeitsschwerpunkte sind inzwischen

– Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO,
– Beschwerden betroffener Personen gemäß Art. 77 DS-GVO und technische Datenschutzprüfungen sowie
– die Beratung öffentlicher Stellen in Hessen gemäß § 13 Abs. 2 Nr. 3 HDSIG.

In der Abteilung für technischen und organisatorischen Datenschutz vollzog sich parallel ein fließender „Generationenwechsel“. Im Ergebnis nahmen alle bis auf einen Mitarbeitenden der Abteilung ihre Tätigkeit in meiner Behörde in den Jahren nach dem Wirksamwerden der DS-GVO auf. Durch einen schrittweisen Übergang war es mir möglich, freiwerdende Stellen sukzessive

mit Mitarbeitenden zu besetzen, deren Expertisen den neuen Anforderungen des harmonisierten europäischen Datenschutzrechts entsprechen.

Die Organisationsstruktur innerhalb der Abteilung für technischen und organisatorischen Datenschutz blieb jedoch zunächst unverändert. In dieser arbeiteten die drei Referate der Abteilung jeweils eng mit den ihnen zugeordneten Spiegelreferaten aus den juristischen Abteilungen zusammen und waren hierbei jeweils für alle obigen Tätigkeitsfelder zuständig. Dies führte u. a. zu einem erhöhten Abstimmungsbedarf zwischen den Referaten, um eine einheitliche Fallbehandlung sicherzustellen. Auch führte die Verteilung der Ressourcen auf die drei Tätigkeitsschwerpunkte innerhalb der Referate nicht selten zu Zielkonflikten.

Im Berichtszeitraum erfolgte daher innerhalb der Abteilung eine Restrukturierung hinsichtlich der Zuständigkeiten der einzelnen Referate und der Zuordnung der Mitarbeitenden zu diesen. Im Ergebnis ist jedes der Referate der Abteilung mittlerweile jeweils für einen der genannten Tätigkeitsschwerpunkte zuständig. Durch eine teilweise Neuzuordnung der Mitarbeitenden zu den einzelnen Referaten war es mir darüber hinaus möglich, die individuellen Kenntnisse und Fähigkeiten der Mitarbeitenden bestmöglich einzusetzen.

In den Kap. 14.2, 14.3 und 14.4 werden die Tätigkeitsschwerpunkte der drei Referate in der Abteilung für technischen und organisatorischen Datenschutz und deren Umsetzung näher vorgestellt.

14.2
Beratung zum technisch-organisatorischen Datenschutz

Gemäß § 13 Abs. 2 Nr. 3 HDSIG gehört es zu meinen Aufgaben, öffentliche Stellen in Hessen in Fragen des Datenschutzes zu beraten. Nach der im Berichtszeitraum erfolgten Schwerpunktsetzung innerhalb der Abteilung 3 meiner Behörde ist mittlerweile ein Referat mit der Erfüllung dieser Aufgabe im Bereich des technischen und organisatorischen Datenschutzes betraut. Es verfolgt den nachfolgend beschriebenen Beratungsansatz.

Hintergrund

Das Thema Datenschutz findet häufig dann gesteigerte (mediale) Aufmerksamkeit, wenn es zu besonderen Vorfällen oder Ereignissen gekommen ist. Beispiele hierfür sind umfangreiche Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit Cyberangriffen oder öffentlich gewordene Verstöße gegen die DS-GVO, bei denen eine Datenschutzaufsichtsbehörde Gebrauch von ihren Befugnissen gemacht und eine hohe Geldbuße verhängt hat. Zwei wesentliche Aspekte haben solche Fälle gemeinsam. Zum einen

handelt es sich um konkrete Einzelfälle, die auf Seiten der Aufsichtsbehörde nicht selten mit einer umfassenden Sachverhaltsaufklärung und einem aufwändigen Verwaltungsfahren verbunden sind. Zum anderen wird die zuständige Aufsichtsbehörde reaktiv tätig, d. h. erst nachdem es bereits zu Verletzungen von Rechten und Freiheiten betroffener Personen gekommen ist.

Damit es erst gar nicht zu Verletzungen und Schadensfällen kommt, wird meine Behörde auch proaktiv tätig. So beraten Mitarbeitende meiner Behörde öffentliche Stellen in meinem Zuständigkeitsbereich in Fragen der datenschutzrechtskonformen Ausgestaltung der Verarbeitung personenbezogener Daten und der Gewährleistung der hierzu nötigen Rahmenbedingungen. Diese Tätigkeit findet zwar in der überwiegenden Mehrzahl der Fälle wenig mediale Aufmerksamkeit, sie leistet aber einen wichtigen Beitrag zur nachhaltigen Verankerung des Datenschutzes in der öffentlichen Verwaltung und zur Verhinderung von Schadensfällen.

Gegenstand der Beratung

Gemäß § 13 Abs. 2 Nr. 3 HDSIG gehört es zu meinen Aufgaben

§ 13 Abs. 2 Nr. 3 HDSIG

(2)

(…)

3. den Landtag, die im Landtag vertretenen Fraktionen, die Landesregierung, die Kommunen und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten, (…)

Einen besonderen Schwerpunkt der Beratung öffentlicher Stellen gemäß § 2 Nr. 1 HDSIG zu Fragen des technischen und organisatorischen Datenschutzes bilden Anfragen im Zusammenhang mit IT-Projekten. In solchen Projekten wird das Fundament für die spätere Verarbeitung personenbezogener Daten in IT-Verfahren gelegt. Da die späteren IT-Verfahren auf den Projektergebnissen aufbauen, muss die Umsetzung datenschutzrechtlicher Anforderungen als integraler Bestandteil frühzeitig, durchgängig und umfassend in IT-Projekten berücksichtigt werden, damit eine spätere datenschutzrechtskonforme Verarbeitung überhaupt erfolgen kann. Zur Ergreifung entsprechender technischer und organisatorischer Maßnahmen (TOM) hat der Gesetzgeber Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO insbesondere in Art. 24 Abs. 1 DS-GVO verpflichtet. Besonders hervorzuheben sind in diesem Zusammenhang TOM zur Umsetzung der Grundsätze des Datenschutzes gemäß Art. 5

Abs. 1 DS-GVO im Sinne des Datenschutzes durch Systemgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 Abs. 1 und 2 DS-GVO sowie TOM gemäß Art. 32 Abs. 1 DS-GVO zur Gewährleistung der Sicherheit der Verarbeitung. Die Auswahl und den wirksamen Einsatz geeigneter TOM, müssen Verantwortliche gemäß Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO nachweisen. Bereits in meinem 50. Tätigkeitsbericht zum Datenschutz hatte ich mich in Kap. 3.2 näher zur Bedeutung der Integration des Datenschutzes in IT-Projekte geäußert.

Als Teil des erfolgreichen Abschlusses eines IT-Projektes werden die Projektergebnisse bereitgestellt und in Betrieb genommen. In der Folge wird mit der eigentlichen Verarbeitung personenbezogener Daten in IT-Verfahren begonnen. In dieser Phase entfalten die als Teil des Projekts umgesetzten TOM erstmalig ihre Wirkung. Zusätzlich werden i. d. R. weitere betriebs- und umgebungsspezifische TOM ergriffen. Spätestens in dieser Phase erfolgt darüber hinaus eine Integration mit dem übergeordneten Datenschutzmanagement des Verantwortlichen. Dies umfasst u. a. die Einbindung in übergeordnete Prozesse, um

– die Rechte der von der Verarbeitung ihrer Daten betroffenen Personen gemäß Kapitel III DS-GVO zu gewährleisten,
– Maßnahmen zur DS-GVO-konformen Verarbeitung gemäß Art. 24 Abs. 1 DS-GVO zu überprüfen und zu aktualisieren,
– die Wirksamkeit der TOM zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 Buchst. d DS-GVO regelmäßig zu überprüfen, zu bewerten und zu evaluieren sowie
– Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 und Art. 34 DS-GVO zu erkennen und zu behandeln.

Greifen Verantwortliche zur Verarbeitung personenbezogener Daten auf Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO zurück, erfolgt darüber hinaus eine Integration in deren Datenschutzmanagementprozesse.[102]

Auch in technischen und organisatorischen Fragen des übergeordneten Datenschutzmanagements und zu dessen Ausgestaltung werde ich beratend tätig. Dies ist nicht auf einzelne IT-Projekte beschränkt. Vielmehr ermutige ich Verantwortliche und Auftragsverarbeiter im öffentlichen Bereich ausdrücklich, gerade bei der Ausgestaltung des übergeordneten Datenschutzmanagements auf Expertise aus meiner Behörde zurückzugreifen. Gerade hier dürfte sich eine besonders weitreichende und nachhaltige Wirkung entfalten. Gleiches

102 S. am Beispiel von Datenschutzverletzungen bei Auftragsverarbeitern 51. Tätigkeitsbericht Kap. 17.3.

gilt auch für Festlegung grundlegender Vorgaben für das Projektvorgehen und die Berücksichtigung des Datenschutzes hierin, sowie für Prozesse zur kontinuierlichen Überprüfung und Verbesserung.

Schließlich bringe ich mich in unterschiedliche Gremien ein. Ein Fokus liegt hierbei insbesondere auf einer unterstützenden Beratung, im Rahmen der Festlegung von grundlegenden Vorgaben für Digitalisierungsvorhaben in Hessen.

Beratungsansatz

Ich biete öffentlichen Stellen in Hessen Beratung in Fragen des technischen und organisatorischen Datenschutzes an. Die Annahme dieses Angebots stellt jedoch keine Verpflichtung für Verantwortliche und Auftragsverarbeiter dar. Ich verfolge einen umfassenden und zugleich flexiblen Beratungsansatz. Bezogen auf Projekte bedeutet dies, dass Projektteams sich in allen Projektphasen an mich wenden und eine Beratung anfragen können. Hierbei gilt allgemein, dass je früher ich einbezogen werde, die Aussicht auf eine erfolgreiche Beratung tendenziell umso höher ist. Umgekehrt gibt es hinsichtlich der Einbeziehung von mir aber kein „zu spät".

Die in Anspruch genommenen Beratungsleistungen können sich auf unterschiedliche Fragestellungen und Themenfelder beziehen und in Art und Umfang stark variieren. Die Ausgestaltung ist vom konkreten Beratungsbedarf abhängig. So können die Beratungsleistungen von einem einmaligen Termin zur Klärung spezifischer datenschutzrechtlicher Fragestellungen bis hin zu einer mehrjährigen Begleitung in einem Großprojekt reichen.

Gerade in Projekten mit langer Laufzeit richtet sich meine Beratung am Projektgeschehen und dem von Seiten des Projekts kommunizierten Beratungsbedarf in den einzelnen Projektphasen aus. Grundsätzlich muss in Projekten von Anfang an und durchgängig in allen Projektphasen eine angemessene Berücksichtigung und Umsetzung der datenschutzrechtlichen Vorgaben erfolgen, sofern auf Basis der Ergebnisse des jeweiligen Projekts personenbezogene Daten verarbeitet werden sollen.

So müssen z. B. bereits im Rahmen der initialen Projektplanung Ressourcen zur Umsetzung datenschutzrechtlicher Vorgaben vorgesehen und deren Einsatz zur Umsetzung von Arbeitspaketen mit Datenschutzbezug geplant werden. Eine zu späte, fehlerhafte oder gar unterlassene Berücksichtigung führt hier fast zwangsläufig mindestens zu Budgetüberschreitungen und Verzögerungen im zeitlichen Ablauf. Auch ist die explizite Einbeziehung und Konkretisierung datenschutzrechtlicher Anforderungen als Teil einer übergeordneten Anforderungsanalyse unverzichtbar. Dies gilt insbesondere auch

als Grundlage für die Auswahl von Produkten, Plattformen oder Diensten, um sicherzustellen, dass eine ausgewählte Lösung überhaupt datenschutzrechtskonform einsetzbar ist.

Im Rahmen der Beratung in Projekten kann es somit bedarfsorientiert zu Phasen intensiven Austauschs kommen, etwa zu Beginn eines Projekts. Diesen folgen häufig Phasen loser Beratung. Auch Unterbrechungen oder ein Ende der Beratung vor dem tatsächlichen Projektende sind keine Seltenheit. Umgekehrt muss das Projektende nicht zwingend auch ein Ende meiner Beratung bedeuten. Gerade eine nachgelagerte Reflexion des Projektverlaufs bietet häufig wertvolle Anhaltspunkte für Verbesserungen für zukünftige Projekte. Gerade hierin sehe ich ein besonderes Potenzial, da die Erkenntnisse aus der Beratung durch meine Behörde so nachhaltig Wirkung entfalten können.

Voraussetzungen

Als Grundlage für eine erfolgreiche Beratung durch mich müssen beratene Verantwortliche und Auftragsverarbeiter zunächst selbst die nötigen Voraussetzungen schaffen. Die wesentlichen Voraussetzungen werden im Folgenden kurz dargestellt.

Zunächst ist hervorzuheben, dass der Beratungscharakter stets gewahrt bleiben muss. Dies bedeutet unter anderem, dass von mir als Aufsichtsbehörde im Rahmen einer Beratung keine operativen oder steuernden Aufgaben übernommen werden können. Die Umsetzung datenschutzrechtlicher Anforderungen und die Steuerung eines IT-Projekts müssen vollständig aus diesem heraus und mit dessen Ressourcen erfolgen. Gleiches gilt für nicht selten gewünschte Abnahmen von Dokumenten, Meilensteinen und anderen Projektergebnissen, in besonderem Maße für Entscheidungen. Meine Beratung darf hier nicht mit einer datenschutzrechtlichen Prüfung oder gar Freigabe verwechselt werden. Auch führe ich keine datenschutzrechtlichen Auditierungen oder gar Zertifizierungen nach Art. 42 DS-GVO durch. Daher ist es unerlässlich, dass auf Seiten von Beratenen in ausreichendem Maße datenschutzrechtliche Expertise eingeplant und bereitgestellt wird. Meine Einbeziehung ersetzt dies nicht. Auch sollte der oder die behördliche Datenschutzbeauftragte im Rahmen einer Beratung gemäß Art. 38 Abs. 1 DS-GVO eingebunden werden.

Ein wichtiger Teil meiner Beratung dient häufig der Klärung konkreter datenschutzrechtlicher Fragestellungen. Zu deren Beantwortung ist eine entsprechende Vorbereitung auf Seiten des jeweiligen Beratenen erforderlich. So müssen die einzelnen Fragestellungen jeweils angemessen aufbereitet und in einen Kontext gesetzt werden. Generell sollten nur diejenigen datenschutzrechtlichen Fragestellungen als Bestandteil der Beratung berücksichtigt

werden, bei denen der Beratene im Rahmen der eigenen Befassung zu keinem oder einem unbefriedigenden Ergebnis gekommen ist. Demgegenüber sollte allgemeine datenschutzrechtliche Grundlagen und Fragestellungen sowie der Aufbau von Expertise beim Beratenen im Rahmen von Schulungen und Fortbildungsmaßnahmen bereits vor der eigentlichen Beratung adressiert werden. Auch hierbei kann ich unterstützend tätig werden.

Abschließend darf nicht unerwähnt bleiben, dass dem zuständigen Referat für Beratungsleistungen kapazitäre Grenzen gesetzt sind. Dies hat zur Folge, dass nicht immer alle von einem Projekt gewünschten Beratungsleistungen in vollem Umfang erbracht werden können. In diesem Fall müssen eine gemeinsame Priorisierung und Selektion von Beratungsleistungen erfolgen.

14.3
Technische Datenschutzprüfungen durch Datenschutzaufsichtsbehörden

Zur Durchführung von technischen Datenschutzprüfungen setze ich ein selbst betriebenes IT-Labor ein (s. hierzu 51. Tätigkeitsbericht Kap. 17.1). Um mit diesem effektiv und effizient prüfen zu können, sind nicht allein Anforderungen des IT-Betriebs, z. B. die Systemarchitektur betreffend, zu berücksichtigen; sondern auch gesetzliche Vorgaben des Datenschutzes und weitere Anforderungen, die mich, genau wie jeden anderen hessischen Verantwortlichen, betreffen. Im Rahmen der Restrukturierung meiner Abteilung für technischen und organisatorischen Datenschutz war dies ein Thema, das durch das nun zuständige Referat schwerpunktmäßig bearbeitet wurde.

Hintergrund und Rechtsgrundlage

Zu meinen gesetzlichen Aufgaben gehört es gemäß Art. 57 Abs. 1 Buchst. 1a DS-GVO und § 13 Abs. 2 Nr. 1 HDSIG die Anwendung der Datenschutzgesetze zu überwachen und durchzusetzen. Hierzu verfüge ich über entsprechende gesetzliche Befugnisse, zu denen gemäß Art. 58 Abs. 1 Buchst. b DS-GVO insbesondere die Befugnis zur Durchführung von Datenschutzüberprüfungen gehört.

Der technologische Fortschritt bringt immer neue technische Mittel der Verarbeitung personenbezogener Daten hervor, mit denen ich mich nicht nur aufgrund entsprechender Eingaben, sondern schon im Rahmen meiner Aufgabe zur Überwachung ebendieser Entwicklung stets auseinandersetze. Um angesichts dieser stetigen technischen Weiterentwicklung in der Lage zu sein, das Grundrecht auf informationelle Selbstbestimmung der hessischen Bürgerinnen und Bürger angemessen zu schützen, muss ich in der Lage

sein, technisch geprägte Verarbeitungen ihrer personenbezogenen Daten nachvollziehen und überprüfen zu können. Neben der Prüfung auf Grundlage von Dokumenten – z. B. durch schriftliche Befragungen – und der Prüfung von IT-Systemen und -Diensten an ihrem jeweiligen Einsatzort bietet sich hierzu regelmäßig auch eine technische Datenschutzprüfung mit Mitteln meiner Dienststelle an. Diese habe ich organisatorisch in einem Referat zusammengefasst, welches das hierfür verwendete IT-Labor schwerpunktmäßig betreut.

Voraussetzungen

Grundsätzlich kann ich technische Datenschutzprüfungen aus jedem Anlass heraus selbst initiieren. Von dieser Möglichkeit kann ich etwa dann Gebrauch machen, wenn ich für einen Prüfungsgegenstand mit breiter Relevanz für hessische Stellen eine besondere Sensibilisierung erzielen möchte oder wenn aufgrund externer Hinweise auf mögliche Datenschutzverstöße ein Anlass für eine Überprüfung entsteht. Häufig sind es insbesondere Beschwerden gemäß Art. 77 DS-GVO, die mir Anlass für eine zielgerichtete Überprüfung geben. Aufgrund des häufig beobachteten Zusammenhangs von Beschwerden und technischen Datenschutzprüfungen habe ich im Berichtszeitraum beschlossen, eines meiner drei Referate für technischen und organisatorischen Datenschutz mit der Zuständigkeit für diesen Themenkomplex zu betrauen. Die im Folgenden skizzierten Aspekte waren bei dieser Schwerpunktbildung für mich von zentraler Bedeutung und werden schrittweise von mir umgesetzt und angepasst.

Personal

Zur Planung und Durchführung von technischen Datenschutzprüfungen benötige ich entsprechend qualifizierte Bedienstete. Erforderlich sind zunächst Bedienstete, die in der Lage sind, die gestellten Anforderungen auf Ebene der IT-Systeme und -Dienste durch deren Auswahl, Installation, Konfiguration, Betrieb, Bedienung, Wartung und Anpassung umzusetzen. Hierfür sind Kompetenzen aus dem Bereich der Systemadministration erforderlich, die die nötigen Arbeitsschritte hin zu einem gebrauchsfähigen System beinhalten. Darüber hinaus sind auch Bedienstete erforderlich, die etwa bei der Bearbeitung von Eingaben oder aufgrund anderer Anlässe die teilweise abstrakten oder ermessensoffenen rechtlichen Anforderungen des Datenschutzes in konkrete, erfüllbare und überprüfbare technische Kriterien übersetzen. Nach der Durchführung von Datenschutzprüfungen müssen diese, die dabei gewonnenen Feststellungen dann auch hinsichtlich der Erfüllung solcher Anforderungen beurteilen können. Dies erfordert sowohl ein Verständnis für

dazu geeignete Systeme und deren Einsatzmöglichkeiten als auch für die Anforderungen des technischen Datenschutzes an sich.

Technische Ausstattung, IT-Labor

Um einen möglichst störungsfreien und sicheren Betrieb des eigentlichen Behördennetzes – z. B. der digitalen Aktenführung – nicht zu gefährden, habe ich mich dazu entschlossen, technische Datenschutzprüfungen in einem von diesem abgetrennten IT-Verbund durchzuführen. Das zu diesem Zweck gebildete IT-Labor verfügt über physische IT-Systeme, die in einem eigenen Netzwerk zusammengeschlossen sind. Zu diesen IT-Systemen gehören zum einen Server- und Client-Systeme und Netzwerkgeräte für eine allgemeine Infrastruktur, wie etwa für den Zugang zum IT-Labor an sich, eine Benutzerverwaltung oder auch ein Dienst für eine Wissensverwaltung. Zum anderen gehören auch solche IT-Systeme dazu, die spezifisch für einzelne Prüfungen genutzt werden können, wie etwa bestimmte mobile Endgeräte.

Im Sinne einer effizienten Prüfungsdurchführung setze ich verstärkt auf Automatisierung und Virtualisierung bei der Bereitstellung, Konfiguration und Bedienung von Prüfungsumgebungen. Wann immer dies praktikabel ist, können meine Bediensteten mithilfe eines Automatisierungs-Toolkits virtuelle IT-Systeme mit den jeweils benötigten Funktionalitäten erzeugen, konfigurieren und bereitstellen, was insbesondere die Durchführung von wiederholbaren und häufig benötigten Prüfungsszenarien erleichtert. Häufige Anwendungsfälle hierfür sind etwa die Prüfungen von Webseiten oder von mobilen Apps.

Prozesse, Dokumentationen, Beweismittel

Da das Ergebnis einer technischen Datenschutzprüfung nicht nur für die unmittelbar an der Prüfung beteiligten, in der Regel technisch versierten Personen relevant ist, muss auch für andere Adressaten eindeutig nachvollziehbar sein, wie es zustande gekommen ist. Hierzu gehören die juristischen Bediensteten meiner jeweils mitzuständigen Fachreferate, Gerichte, die ggf. im Rahmen einer Klage gegen eine meiner Entscheidungen solche Prüfungsergebnisse als Beweismittel bewerten können müssen, und nicht zuletzt auch die geprüften Stellen selbst, denen ich das Prüfungsergebnis insbesondere dann nachvollziehbar darlegen muss, wenn ich eine aufsichtsbehördliche Maßnahme gegen sie daran anknüpfe.

Um dies zu erreichen, setze ich auf eine ausführliche Dokumentation der Prüfungen. Hierbei unterscheide ich zwischen Überlegungen, die bereits im Vorfeld der eigentlichen Prüfungsdurchführung zu Ende zu führen sind,

wie etwa die Klärung der Frage, welche IT-Systeme und -Dienste eines Verantwortlichen ich mit welchen Mitteln des IT-Labors auf welche Art und Weise überprüfen möchte, und der Dokumentation der eigentlichen Prüfungsdurchführung, bei der vor allem die dabei gemachten Feststellungen festgehalten werden und im Nachgang durch die zuständigen Sachbearbeiter aus technischer Sicht des Datenschutzes bewertet werden.

Durch die Verwendung geeigneter Vorlagen für solche Dokumente, welche die relevanten Erwägungen des Datenschutzes an der Schnittstelle von Recht und Technik enthalten und die im Idealfall auch als „Schritt-für-Schritt-Anleitung" für die Prüfungsdurchführung dienen können, wird nachvollziehbar, wie die Ergebnisse einer technischen Datenschutzprüfung zustande gekommen sind.

Eine besondere Rolle kommt solchen Ergebnissen von technischen Datenschutzprüfungen zu, die entscheidungsrelevant für einen belastenden Verwaltungsakt – z. B. eine Verwarnung oder eine Geldbuße gegen einen Beschwerdegegner – werden können und daher mitunter auch als Beweismittel einer gerichtlichen Überprüfung standhalten können müssen. Der Umgang mit diesen muss also den Anforderungen des Verwaltungsrechts und im Rahmen von Verfahren zu Geldbußen mitunter auch denen des Strafprozessrechts genügen. Bei technischen Datenschutzprüfungen können kritische Aspekte z. B. die Nachvollziehbarkeit der Erhebung digitaler Beweismittel sowie deren unverändertes Bestehen seit dem Zeitpunkt der Erhebung sein. Daher lege ich besonderes Augenmerk darauf, dass der Gang eines Beweismittels von dessen Auswahl über seine Erhebung bis hin zur Ablage nachvollziehbar gestaltet ist. Hierfür bieten sich neben dokumentierten Prozessen auch technische Mittel an, etwa das Anfertigen von Bildschirmaufnahmen oder das Sichern von Integritätsinformationen in Form von Datei-Hashes.

Datenschutz bei technischen Prüfungen

Im Rahmen von technischen Datenschutzprüfungen verarbeitet meine Behörde mitunter selbst personenbezogene Daten in der Rolle eines datenschutzrechtlich Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO. Bei bestimmten Prüfungen können auch durchaus große Mengen personenbezogener Daten betroffen sein oder solche, deren Verarbeitung ein hohes Risiko für Rechte und Freiheiten der betroffenen Personen mit sich bringt. Zu denken wäre hier etwa an die unbefugte Veröffentlichung solcher personenbezogenen Daten im sogenannten „Darknet" durch Angreifergruppen, die diese Daten zuvor im Rahmen eines Ransomware-Angriffs bei einem Unternehmen oder einer öffentlichen Stelle unbefugt kopiert haben. Handelt es sich bei der angegriffenen Stelle um eine Stelle mit Sitz in Hessen, kann es erforderlich

sein, dass ich selbst in solche Veröffentlichungen Einsicht nehme, etwa um Angaben des Verantwortlichen zu dem Vorfall zu überprüfen.

Daher habe ich Vorkehrungen dafür getroffen, dass die Verarbeitung solcher personenbezogenen Daten in meiner Behörde in gesetzeskonformer Weise erfolgen kann. Hierfür habe ich meine behördliche Datenschutzbeauftragte frühzeitig in die Ausgestaltung der Prozesse und Dokumentationen im Rahmen des IT-Labors eingebunden.

IT-Sicherheit

Die im IT-Labor z. B. im Rahmen von Untersuchungen verarbeiteten personenbezogenen Daten, wie auch mögliche Auswirkungen auf die Handlungsfähigkeit und übrigen Belange der Behörde insgesamt, machen es auch im IT-Labor erforderlich, entsprechend Art. 5 Abs. 1 Buchst. f in Verbindung mit Art. 32 DS-GVO ein angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten zu gewährleisten. Dazu ist es erforderlich, ein aus Sicht der Informationssicherheit angemessenes Sicherheitsniveau für den Betrieb des IT-Labors zu erreichen und aufrechtzuerhalten. Zu diesem Zweck orientiere ich mich bei der Umsetzung und Einhaltung der notwendigen Anforderungen an der anerkannten und standardisierten Vorgehensweise der IT-Grundschutz-Methodik des BSI. Ein wichtiger Aspekt der Umsetzung für mein IT-Labor ist dabei dessen technische Abtrennung von den IT-Systemen und -Diensten der übrigen Dienststelle insbesondere auf Netzwerkebene sowie die differenzierte Betrachtung des Schutzbedarfs einzelner Komponenten des IT-Labors in Abhängigkeit von deren Einsatzzweck. Da die daraus resultierenden sicherheitsrelevanten Maßnahmen der Informationssicherheit für den Schutz personenbezogener Daten im IT-Labor notwendig, aber nicht ausreichend sein können, ergänze ich sie durch geeignete technische und organisatorische Maßnahmen des Datenschutzes.

14.4
Aus Fehlern lernen – Begleitung von Datenschutzverletzungen

Die Meldepflicht von Datenschutzverletzungen nach Art. 33 Abs. 1 DS-GVO führt dazu, dass viele unterschiedliche verantwortliche Stellen in Hessen Kontakt mit mir aufnehmen müssen. Bei der aufsichtsrechtlichen Begleitung von Datenschutzvorfällen spielen neben dem Sicherstellen, dass ein Vorfall beendet ist, drei Aspekte eine Rolle: Orientierung anbieten, Optimierungsprozesse unterstützen und Rechte der Betroffenen sicherstellen.

Aufsichtsbehördliche Begleitung von gemeldeten Datenschutzverletzungen

Immer wieder kommt es zu Angriffen auf die Informationstechnik (IT) von Organisationen sowohl im nicht öffentlichen wie auch öffentlichen Bereich, bei denen vertrauliche Daten eingesehen, kompromittiert oder gelöscht werden. Insbesondere Ransomware-Angriffe, bei denen oft große Mengen personenbezogener Daten aus den IT-Systemen der betroffenen Organisationen verschlüsselt und häufig auch durch die Angreifer exfiltriert werden, nehmen zu. Diese Art von Vorfällen führt in der Regel zu Verletzungen des Schutzes personenbezogener Daten, da sie mindestens ein Risiko für die Rechte und Freiheiten betroffener Personen darstellen. Daher sind diese Angriffe durch den Verantwortlichen gemäß Art. 33 Abs. 1 DS-GVO unverzüglich der zuständigen Aufsichtsbehörde zu melden (s. näher 51. Tätigkeitsbericht Kap. 17.3).

Meine Herangehensweise und mein grundsätzliches Vorgehen bei der Begleitung von Datenschutzverletzungen sind geprägt von den drei Aspekten: Orientierung zu bieten, Optimierungsprozesse zu unterstützen sowie Rechte der Betroffenen sicherzustellen. Eingehende Meldungen nach Art. 33 DS-GVO werden erfasst, eingeordnet und dem zuständigen Schwerpunktreferat für die Sicherheit in der Verarbeitung (s. Kap. 14.1) zugeordnet.

Datenschutzrechtliche Grundlagen für die aktive Begleitung

Der Ausgangspunkt für eine Begleitung von Datenschutzverletzungen ist das Auftreten einer Verletzung des Schutzes personenbezogenen Daten gemäß Art. 4 Nr. 12 DS-GVO bei einem Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO. Die gesetzlichen Vorgaben in Bezug auf die Dokumentations-, Melde- und Benachrichtigungspflichten, die sich bei Verletzungen des Schutzes personenbezogenen Daten ergeben, sind in den Art. 33 und 34 der DS-GVO aufgeführt.

Wenn ein Verantwortlicher bei einer Verletzung des Schutzes personenbezogener Daten im Rahmen seiner Risikobewertung zu dem Ergebnis kommt, dass voraussichtlich mindestens ein Risiko für die Rechte und Freiheiten der betroffenen Personen besteht, meldet er mir den Vorfall unverzüglich, mindestens binnen 72 Stunden gemäß Art. 33 Abs. 1 DS-GVO. Gemäß Art. 33 Abs. 4 DS-GVO kann eine solche fristwahrende Meldung auch unvollständig erfolgen, sofern die im Rahmen der Meldung erforderlichen Informationen noch nicht vorliegen. Hierbei ist aber darauf zu achten, dass die noch ausstehenden Informationen ohne unangemessene weitere Verzögerung und erforderlichenfalls schrittweise zur Verfügung gestellt werden. Unabhängig vom Risiko besteht in jedem Fall zusätzlich gemäß Art. 33 Abs. 5 DS-GVO die Pflicht, den Vorfall so zu dokumentieren, dass ich auf Basis dieser Do-

kumentation den Vorfall und die Erfüllung der Anforderungen der DS-GVO durch den Verantwortlichen nachvollziehen kann. Hierzu gehört auch die durchgeführte Risikobewertung. Mögliche Rückfragen können dann direkt aus der erstellten Dokumentation beantwortet werden. Zur Unterstützung der Meldung stelle ich auf meiner Website ein entsprechendes Meldeformular zur Verfügung.[103]

Eine Meldung gemäß Art. 33 Abs. 1 DS-GVO bildet den Ausgangspunkt für die aufsichtsbehördliche Begleitung. Gemäß Art. 31 DS-GVO besteht für Verantwortliche die gesetzliche Pflicht, hierbei mit mir zusammenzuarbeiten und u. a. meine Fragen zu einem Vorfall und dessen Behandlung durch den Verantwortlichen und ggf. Auftragsverarbeiter zu beantworten und angeforderte Informationen bereitzustellen.

Die erste und wichtigste Aufgabe muss darin bestehen, den aktuellen Vorfall zu stoppen, bevor alle notwendigen Schritte zur Wiederherstellung eines sicheren Regelbetriebs eingeleitet werden. Durch eine Verletzung des Schutzes personenbezogener Daten ergeben sich Risiken für die Rechte und Freiheiten der betroffenen Personen. Wenn es zu einem schweren Datenschutzvorfall kommt, kann dies zu einem hohen Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen führen. Die Möglichkeiten der Betroffenen, dies im Nachhinein zu verhindern, sind begrenzt, etwa wenn es bereits zu einer Veröffentlichung der Daten betroffener Personen durch die Angreifer gekommen ist. Umso wichtiger ist es, dass die betroffenen Personen unverzüglich und in verständlicher Form über den Vorfall und die möglichen Folgen durch den Verantwortlichen gemäß Art. 34 Abs. 1 DS-GVO informiert werden.

Art. 34 Abs. 1 DS-GVO

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Aufgrund der besonderen Bedeutung solcher Informationen für von Verletzungen des Schutzes personenbezogener Daten Betroffene richte ich ein besonderes Augenmerk auf die Risikobetrachtung des Verantwortlichen zum Vorfall. Wenn notwendig, kann ich auch gemäß Art. 34 Abs. 4 DS-GVO und Art. 58 Abs. 2 Buchst. e DS-GVO die Information der betroffenen Personen

103 https://datenschutz.hessen.de/service/meldung-nach-art-33-ds-gvo.

anordnen, etwa wenn ein Verantwortlicher seinen Pflichten nach Art. 34 Abs. 1 DS-GVO nicht nachkommt.

Orientierung, Optimierung, Sicherstellen

Die aufsichtsbehördliche Praxis zeigt, dass in der Behandlung von Datenschutzvorfällen durch Verantwortliche oder Auftragsverarbeiter häufig Verbesserungspotenzial besteht und aus Sicht des Datenschutzes potenziell relevante Aspekte übersehen oder nicht im Sinne der DS-GVO eingeordnet werden. Dafür kann es unterschiedlichste Gründe geben, wie fehlendes Wissen oder Erfahrung im Bereich der Anwendung der DS-GVO oder speziell bei der Behandlung von Datenschutzvorfällen, fehlende Ressourcen, mangelnde Priorisierung oder eine falsche Einordnung der Relevanz des Vorfalls. Seltener liegt es auch an Unwillen, Widerstand oder Angst vor Reputationsverlusten durch den Verantwortlichen. Eines meiner wichtigsten Werkzeuge bei der Begleitung Verantwortlicher bei gemeldeten Datenschutzverletzungen ist daher das gezielte Stellen von Rückfragen und das Anfordern weitergehender Informationen zum Vorfall und dessen Behandlung durch den Verantwortlichen. Relevante Informationen können im ersten Schritt über ein Telefonat eingeholt oder Hinweise an den Verantwortlichen gegeben werden. In der Regel erfolgten die Kontaktaufnahme und das Stellen von Rückfragen aber schriftlich. Diese Schreiben mit Rückfragen sind auf den jeweiligen Fall angepasst, bauen auf den bisher gemachten Erfahrungen mit ähnlichen Arten von Vorfällen auf und berücksichtigen häufig übersehe Aspekte.

Gezielt gestellte Rückfragen bieten den Verantwortlichen zusätzlich eine Orientierung bei der Behandlung von Datenschutzvorfällen. Insbesondere bei umfangreichen und komplexen Vorfällen sind die Fragen so aufgebaut, dass damit eine Struktur angeboten wird, die aufzeigt, wie ein solcher Vorgang aufgearbeitet werden kann und welche Aspekte dabei berücksichtigt und untersucht werden sollten. Durch die Fragen unterstütze ich die Verantwortlichen dabei, den Vorfall zu untersuchen, zu verstehen und angemessen zu behandeln. Die damit eingeleitete Interaktion zwischen verantwortlicher Stelle und meiner Behörde erhöht die Transparenz und den Informationsaustausch. Oftmals ergeben sich auch bei den meldenden Stellen Fragen bezüglich der Behandlung des konkreten Vorfalls. Die Verantwortlichen erhalten dann die Kontaktinformationen der in meiner Behörde zuständigen Beschäftigen, die bei weitergehenden Fragen helfen können.

Die Rückfragen haben jedoch primär das Ziel, meinen Aufgaben im Rahmen der Datenschutzaufsicht nachzukommen. Sollte aus den von den Verantwortlichen bereitgestellten Informationen hervorgehen, dass ein Datenschutzvorfall

nicht hinreichend behandelt wurde, wirke ich auf den Verantwortlichen ein, um die Erfüllung der Anforderungen der DS-GVO durchzusetzen.

Durch die Fragen unterstütze ich die Verantwortlichen zusätzlich bei ihrem Erkenntnisgewinn, damit diese die Optimierungspotenziale bezüglich der Ermittlung und Beseitigung von Defiziten ausschöpfen können. Ein integraler Bestandteil einer Meldung gemäß Art. 33 DS-GVO ist daher die Beschreibung der durch den Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen (Art. 33 Abs. 3 Buchst. d DS-GVO). Diese Maßnahmen beziehen sich auf die unmittelbare Reaktion und konkrete Behandlung des gemeldeten Vorfalls durch den Verantwortlichen oder Auftragsverarbeiter. Um aus dem Vorfall entsprechende Erkenntnisse gewinnen zu können, muss auch ermittelt werden, welche Gründe oder Auslöser zu der Verletzung des Schutzes personenbezogener Daten geführt haben. Dabei zeigt sich immer wieder, dass die getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO nicht geeignet oder dem Risiko nicht angemessen waren. In diesen Fällen besteht selbstverständlich die Notwendigkeit für den Verantwortlichen, die bisher getroffenen Maßnahmen zu überprüfen, zu bewerten und zu evaluieren sowie ggf. anzupassen oder zu ergänzen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Daher werden auch zu diesen Maßnahmen bereits im Meldeformular Informationen abgefragt. Im Rahmen der Begleitung des Verantwortlichen nutze ich ebenfalls gezielte Rückfragen, um sicherzustellen, dass diese Überlegungen durchgeführt wurden und die getroffenen Maßnahmen angemessen und hinreichend sind.

Ein weiteres Optimierungspotenzial liegt darin, die gewonnenen Erkenntnisse auch auf andere Bereiche, die nicht vom Vorfall betroffen waren, zu übertragen und dort bei Bedarf entsprechend Maßnahmen zu ergreifen. Wenn beispielsweise eine fehlende Mehr-Faktor-Authentifikation zur Übernahme eines Benutzer-Accounts oder eines IT-Dienstes des Verantwortlichen geführt hat, dann sollten auch die anderen betriebenen oder genutzten IT-Dienste auf diese Problematik hin untersucht und ggf. um entsprechende Maßnahmen ergänzt werden. Über passende Rückfragen kann ich entsprechende Überlegungen beim Verantwortlichen initiieren. Grundsätzlich bieten Vorfälle immer auch die Chance, aus diesen zu lernen. Diese Chance sollten Verantwortliche auf keinen Fall ungenutzt lassen.

Meine weitere Aufgabe ist es sicherzustellen, dass die Rechte der betroffenen Personen gewahrt werden. Sollte der Vorfall voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten betroffener Personen führen,

müssen diese gemäß Art. 34 Abs. 1 DS-GVO durch die Verantwortlichen benachrichtigt werden. Zusätzlich muss die Sicherheit der Verarbeitung der personenbezogenen Daten wiederhergestellt werden. Auch bei der Wahrung der Rechte der betroffenen Personen sind gezielte Rückfragen an die Verantwortlichen ein wichtiges Werkzeug, um die Umsetzung der Anforderungen der DS-GVO zu überwachen und bei Bedarf die Notwendigkeit einer Durchsetzung zu erkennen.

Grundlage für die Feststellung, dass ein Datenschutzvorfall zu einem hohen Risiko für Rechte und Freiheiten betroffener Personen geführt hat, ist eine vom Verantwortlichen durchzuführende Risikobetrachtung. Hierbei kann ich über entsprechende Rückfragen feststellen, ob die relevanten Aspekte und Risikoszenarien für die betroffenen Personen durch den Verantwortlichen berücksichtigt wurden. Auch hier ist der direkte Austausch zwischen Verantwortlichen und mir möglich.

Fazit

Meine aufsichtsbehördliche Begleitung von verantwortlichen Stellen, bei gemeldeten Verletzungen des Schutzes personenbezogener Daten ist zunächst darauf gerichtet, eine datenschutzrechtskonforme Behandlung durch Verantwortliche sicherzustellen. Hierzu zählen insbesondere das Ergreifen von Maßnahmen zur Beendigung des Vorfalls, die etwaig erforderliche Benachrichtigung der betroffenen Personen und Maßnahmen zur Verhinderung eines erneuten Auftretens des Vorfalls.

Darüber hinaus zielt meine Befassung mit einem Vorfall darauf ab, Orientierung zu bieten und Optimierungsprozesse zu unterstützen. Hierdurch sollen Verantwortliche über die Behandlung des eigentlichen Vorfalls hinaus dabei unterstützt werden, Lehren aus dem Vorfall zu ziehen. Wenn es gelingt, die Verantwortlichen durch die angebotene Orientierung dabei zu unterstützen, aus Datenschutzvorfällen ein vertieftes Datenschutzbewusstsein und neue, zusätzliche Erkenntnisse für die Umsetzung der DS-GVO zu gewinnen, profitieren auch die Personen, deren Daten verarbeitet werden. Dies wird von mir in einem offenen und konstruktiven Dialog mit den Verantwortlichen unterstützt.

14.5
Herausforderungen der Cloud-Transformation für den Datenschutz

Grundlage der digitalen Transformation sind zunehmend leistungsfähigere und flexiblere IT-Infrastrukturen. Der Rückgriff auf Cloud-Lösungen erscheint vielversprechend, um umfassend Abhilfe zu schaffen, neue Potenziale zu

erschließen und völlig neue Möglichkeiten zu eröffnen. Jedoch ergeben sich hierbei auch völlig neue Fragestellungen und Herausforderung für den Datenschutz.

„Die Cloud“ als Fundament der digitalen Transformation

„Die Cloud“ bietet die Möglichkeit, bedarfsgerecht über ein Netzwerk zeitnah und flexibel erforderliche IT-Ressourcen bereitzustellen, zu nutzen und wieder freizugeben. Gleichzeitig befreit sie Verantwortliche von langfristig bindenden Entscheidungen und Investitionen sowie von administrativen und operativen Aufgaben der Verwaltung einer physischen Infrastruktur.

Das Spektrum von als Cloud-Lösungen bereitgestellten IT-Ressourcen und Diensten ist äußerst vielschichtig. Zur grundlegenden Einordnung unterschiedlicher Arten von Cloud-Lösungen bieten sich die sogenannten „Servicemodelle“ an. Sie reichen von der Bereitstellung virtualisierter Hardware als Grundlage zur Umsetzung von virtuellen IT-Infrastrukturen (Infrastructure as a Service – IaaS) über virtualisierte Laufzeitumgebungen für die Entwicklung und den Betrieb eigenentwickelter IT-Dienste und Anwendungen (Platform as a Service – PaaS) bis hin zur Bereitstellung einzelner oder mehrerer IT-Dienste und Anwendungen (Software as a Service – SaaS). Auch einzelne Funktionalitäten können als cloudbasierte IT-Dienste angeboten werden (Function as a Services – FaaS). Innerhalb der einzelnen Servicemodelle steht wiederum häufig ein sehr breites Spektrum an alternativen Lösungen zur Verfügung. So bieten z. B. verschiedene Anbieter von Videokonferenzsystemen ihre Lösungen auf Basis des SaaS-Servicemodells an. Die verfügbaren Lösungen weichen hierbei hinsichtlich ihrer Möglichkeiten, Eigenschaften und Spezifika sowie der Anforderungen und Rahmenbedingungen für ihren Einsatz teils stark voneinander ab, auch und nicht zuletzt in datenschutzrechtlicher Hinsicht.

Ein weiteres Schema zur Klassifikation von Cloud-Lösungen orientiert sich an der Art der Bereitstellung oder am Kreis der Nutzenden einer oder mehrerer Cloud-Lösungen. Zur Unterscheidung dienen hierbei unterschiedliche „Liefermodelle“. So können Nutzende eine Cloud-Umgebung selbst betreiben und exklusiv nutzen (Private Cloud). Alternativ können Nutzende auf am Markt verfügbare Lösungen von Cloud-Anbietern zurückgreifen, die häufig über das Internet bereitgestellt werden (Public Cloud). Der Kreis möglicher Nutzender ist von Seiten der Anbieter i. d. R. nicht oder nur unwesentlich beschränkt. Bestimmte Cloud-Lösungen werden allerdings auch nur einer begrenzten Gruppe von Nutzenden zur Verfügung gestellt (Community Cloud). Schließlich lassen sich IT-Ressourcen und -Dienste aus unterschiedlichen Cloud-Lösungen sowie in Kombination mit selbstbetriebenen IT-Systemen und -Diensten einsetzten (Hybrid Cloud).

Die beiden genannten Schemata sind erweiterbar, lassen sich kombinieren und erlauben so eine zweidimensionale Klassifikation von Cloud-Lösungen. Dies bedeutet auch, dass es „die Cloud“ als homogene Lösung gar nicht gibt. „Die Cloud“ beschreibt vielmehr ein allgemeines Modell zur Bereitstellung und Nutzung virtualisierter IT-Ressourcen und Dienste mit einer Vielzahl unterschiedlicher Ausprägungen und jeweils spezifischen Eigenschaften, Rahmenbedingungen, Anforderungen und Implikationen.

Viele Verantwortliche und Auftragsverarbeiter im öffentlichen Bereich in Hessen und darüber hinaus haben für sich den Bedarf nach dem Einsatz von Cloud-Lösungen identifiziert. Die Hintergründe hierfür sind unterschiedlich und reichen von der Reaktion auf Ankündigungen von Auftragsverarbeitern, ihre Lösungen in absehbarer Zeit nur noch cloudbasiert anzubieten, über den Einsatz von Cloud-Lösungen in einzelnen, isolierten IT-Projekten bis hin zur Festlegung und Umsetzung übergeordneter Cloud-Strategien.

Die hessische Landesregierung hatte im Berichtszeitraum den Vorsitz im IT-Planungsrat inne, dem zentralen politischen Steuerungsgremium zwischen Bund und Ländern in Fragen der Informationstechnik und der Digitalisierung von Verwaltungsleistungen. Für ihren Vorsitz hatte die Landesregierung das Thema Cloud-Transformation unter drei besonderen Themenschwerpunkten priorisiert.[104] Bereits im Jahr 2020 hatte der IT-Planungsrat die Einrichtung einer Arbeitsgruppe „Cloud-Computing und Digitale Souveränität“[105] (AG Cloud) beschlossen. In der im Berichtszeitraum aktualisierten Strategie Digitale Verwaltung Hessen[106] (DVH) der hessischen Landesregierung wird dem Einsatz von Cloud-Technologien und -Lösungen zudem eine besondere Bedeutung beigemessen. In diesem Zusammenhang setzte die Hessische Zentrale für Datenverarbeitung (HZD) im Berichtszeitraum ihr Programm zur Cloud-Transformation[107] fort.

104 Die Hessische Ministerin für Digitale Strategie und Entwicklung, IT-Planungsrat, https://digitales.hessen.de/moderne-verwaltung/it-planungsrat.

105 IT-Planungsrat, AG Cloud Computing und Digitale Souveränität, https://www.it-planungsrat.de/foederale-zusammenarbeit/gremien/ag-cloud-computing-und-digitale-souveraenitaet.

106 Hessische Staatskanzlei, Ministerin für Digitale Strategie und Entwicklung, Digitale Verwaltung Hessen, https://digitales.hessen.de/sites/digitales.hessen.de/files/2023-12/dvh_4.1_barrierefrei_0.pdf.

107 HZD: Der Weg zum anerkannten Cloud-Service-Provider, https://hzd.hessen.de/portfolio/cloud-transformation.

Herausforderungen aus Sicht des Datenschutzes

Auf dem Weg in die Cloud müssen datenschutzrechtliche Anforderungen als unverzichtbarer Bestandteil verstanden und entsprechend umgesetzt werden. Dies sollte anhand eines ganzheitlichen Ansatzes erfolgen. Auf der einen Seite ist das Querschnittsthema Datenschutz zentral zu adressieren und zu koordinieren. Auf der anderen Seite sind datenschutzrechtliche Anforderungen in jedem einzelnen Teilbereich eines Cloud-Projektes oder einer Cloud-Transformation als integraler Bestandteil umzusetzen. Mindestens zwischen zentraler Koordination und dezentraler Umsetzung sollte unbedingt eine enge Abstimmung erfolgen.

Ansätze, bei denen das Thema Datenschutz demgegenüber ausschließlich separat und isoliert behandelt wird, etwa in Form einer ausgelagerten Stabsstelle oder eines Beratungsgremiums, ohne dass gleichzeitig eine tiefgehende Integration in die tatsächliche Umsetzung sichergestellt wird, bergen schwerwiegende Risiken. Im ungünstigsten Fall werden datenschutzrechtliche Anforderungen im Projektgeschehen vernachlässigt oder sogar gänzlich ausgeklammert, da davon ausgegangen wird, dass sich eine zentrale Stelle „um das Thema kümmert“. Gerade bei umfangreichen und komplexen Vorhaben mit weitreichenden Folgen, wie etwa der Konzeption und Umsetzung einer Cloud-Transformation, könnte ein solches unzureichendes Vorgehen überaus nachteilige Folgen haben. Schließlich werden in solchen Vorhaben die Grundlagen für eine Vielzahl zukünftiger IT-Projekte und für die mit diesen verbundene Verarbeitung personenbezogener Daten gelegt. Wäre ein solches Fundament unzureichend, fehlerhaft oder gar als Grundlage für die datenschutzrechtskonforme Verarbeitung personenbezogener Daten ungeeignet, hätte dies gravierende und direkte Auswirkungen auf alle auf dieser Basis umgesetzten Verarbeitungstätigkeiten.

Im Berichtszeitraum hat die Europäische Kommission am 10. Juli 2023 den Angemessenheitsbeschluss für den Datenschutzrahmen zwischen der EU und den USA[108] – EU-U.S. Data Privacy Framework (EU-U.S. DPF) – angenommen, mit dem nun ein Transferinstrument für die Übermittlung personenbezogener Daten, gemäß Art. 45 DS-GVO, in die USA vorliegt (s. Kap. 2.2).

Viele große Cloud-Anbieter, sogenannte Hyperscaler, haben ihren Sitz in den USA. Soll auf die Cloud-Dienste eines solchen Anbieters zurückgegriffen werden, stellt die datenschutzrechtliche Zulässigkeit der Übermittlung personenbezogener Daten auf Basis des Angemessenheitsbeschlusses an

108 Europäische Kommission: Adequacy decision for the EU-US Data Privacy Framework, https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

einen solchen Cloud-Anbieter jedoch nur eine notwendige Voraussetzung dar. Sie ist für sich genommen bei weitem nicht hinreichend für eine datenschutzrechtskonforme Verarbeitung personenbezogener Daten.

Durch den Einsatz cloudbasierter Angebote kommt es im Vergleich zum vollständigen Eigenbetrieb einer IT-Infrastruktur zumindest zu einem partiellen Kontrollverlust in Bezug auf die zugrundeliegenden IT-Systeme und Dienste. Auch binden sich Verantwortliche beim Einsatz eines oder mehrerer Cloud-Angebote je nach Art, Umfang und Ausmaß der Nutzung an ein solches Angebot und letztlich an den Cloud-Anbieter. Bereits diese beiden Aspekte machen deutlich, dass sich mit dem Einsatz von Cloud-Angeboten immer auch Fragen der digitalen Souveränität stellen. Im öffentlichen Bereich wurde dies im Rahmen der deutschen Verwaltungscloud-Strategie als wichtiges Thema identifiziert.[109] Auch am Markt wurde der Bedarf nach Cloud-Lösungen erkannt, welche die digitale Souveränität der Nutzenden unterstützen. Die DSK hat sich mit dem Themenkomplex souveräner Cloud-Lösungen befasst und dazu ein Positionspapier mit Kriterien für souveräne Cloud-Lösungen aus der Perspektive des Datenschutzes veröffentlicht.[110] An der Erstellung dieses Positionspapiers war ich sowohl hinsichtlich der juristischen als auch der technischen und organisatorischen Fragestellungen maßgeblich beteiligt.

Ich stehe im öffentlichen Bereich für die Beratung von Verantwortlichen und Auftragsverarbeitern auch hinsichtlich des Einsatzes von Cloud-Lösungen zur Verfügung. Dies gilt in besonderem Maße auch und vor allem für Cloud-Transformations-Vorhaben. Auch wenn solche Vorhaben bereits fortgeschritten sind, möchte ich die handelnden Akteure ermutigen, von meinem Beratungsangebot Gebrauch zu machen. Es ist nie zu spät, sich an mich zu wenden.

14.6
Meldungen von Datenschutzverletzungen

Die Zahl der Meldungen von Datenschutzverletzungen stieg im Berichtsjahr um ca. 10 % auf insgesamt 1.934 Meldungen und erreichte damit erneut ein hohes Niveau. Auch im Berichtsjahr 2023 hatten Cyberangriffe auf Verantwortliche und Auftragsverarbeiter daran großen Anteil. Die Rolle und die

109 IT-Planungsrat, Deutsche Verwaltungscloud-Strategie, https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-54_Deutsche_Verwaltungscloud_Strategie.pdf.

110 DSK, Kriterien für Souveräne Clouds, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf.

Pflichten der für verantwortliche Stellen tätigen Auftragsverarbeiter blieben im Fokus.

Überblick und Entwicklungen

Nachdem im letzten Jahr ein leichter Rückgang der Meldungen 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, stieg die Anzahl der im Berichtsjahr 2023 eingereichten Meldungen wieder an und erreichte mit 1.934 gemeldeten Datenschutzverletzungen erneut ein hohes Niveau. Die Bearbeitung der Meldungen von Datenschutzverletzungen stellte damit weiterhin einen großen Teil der täglichen Arbeit meiner Behörde dar.

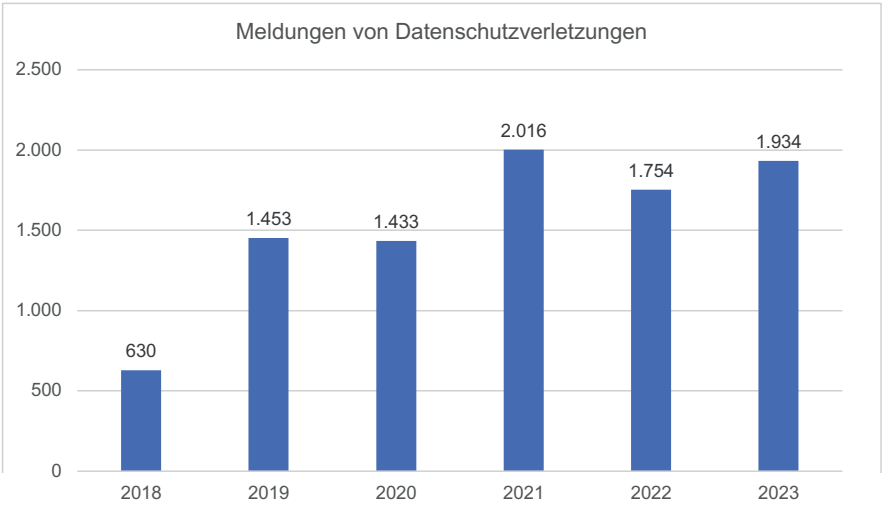

Abbildung: Entwicklung der Anzahl der Meldungen von Datenschutzverletzungen beim HBDI seit Wirksamwerden der DS-GVO

Der Großteil der gemeldeten Datenschutzverletzungen war wiederholt auf Vorfälle von Fehlversand und falscher Zuordnung von Daten sowie auf Vorfälle im Rahmen von Cyberkriminalität zurückzuführen. Am stärksten betroffen waren auch im Jahr 2023 der Wirtschaftssektor einschließlich Kreditwirtschaft, Inkasso, Dienstleister, Handel und Gewerbe sowie die Bereiche Beschäftigte und Gesundheit.

Cyberangriffe

Wie auch in den letzten Jahren war die Cyberkriminalität ein Hauptthema bei den Datenschutzverletzungen. Die Anzahl der gemeldeten Hackerangriffe und Phishingvorfälle stieg im Vergleich zum Vorjahr von 475 auf 502 Meldungen. Desgleichen gab es wieder viele Hackerangriffe auf Auftragsverarbeiter aus verschiedenen Bereichen. Insgesamt waren sowohl Unternehmen als auch öffentliche Einrichtungen und kritische Infrastrukturen von solchen Cyberangriffen betroffen. Gerade bei kritischen Infrastrukturen, wie z. B. Krankenhäusern, können solche Vorfälle die Versorgungssicherheit der Bürgerinnen und Bürger bemerkbar gefährden.

Sehr dynamisch ist die Entwicklung der Cyberangriffe auf Bereiche der öffentlichen Verwaltung. Im Berichtsjahr ist die Anzahl der Meldungen von Cyberangriffen auf Kommunen und kommunale Einrichtungen bedeutsam gestiegen. Darüber hinaus gab es Meldungen, die eine mögliche Ausnutzung von Sicherheitslücken in zentral zur Verfügung gestellter kommunaler Software zum Thema hatten. Im kommunalen Bereich können besonders große Datenmengen von Beschäftigten, aber auch von Bürgerinnen und Bürgern erbeutet werden.

Die Rolle der Auftragsverarbeiter

Die Cyberangriffe auf Auftragsverarbeiter stellen grundsätzlich alle Beteiligten aufgrund ihrer Komplexität vor besondere Herausforderungen. Oftmals muss aufwändig eruiert werden, welche Daten welches Verantwortlichen in welchem Umfang betroffen sind. Diese Entwicklung prägte auch in diesem Berichtsjahr die Praxis der Zusammenarbeit der deutschen Datenschutzaufsichtsbehörden. Neben den Fragen der Zuständigkeit bei bundeslandübergreifenden Meldungen von Datenschutzverletzungen erforderte die Aufklärung und Bewertung der Fälle einen stetigen Austausch der Datenschutzbehörden untereinander. Dies gestaltete sich im Berichtsjahr in allen Fällen einwandfrei, zielgerichtet und konstruktiv.

In meinem letzten Bericht ging ich ausführlich auf die Bedeutung einer datenschutzkonformen Gestaltung der Auftragsverarbeitung ein (s. 51. Tätigkeitsbericht Kap. 17.2). Im Hinblick auf den erneuten Anstieg von Cyberangriffen verlor diese Thematik auch 2023 nicht an Aktualität. Im Gegenteil ist es mir auch jetzt ein großes Anliegen, den hohen Stellenwert einer datenschutzkonformen Gestaltung der Auftragsverarbeitung zu betonen. Nach wie vor bedarf es zur Vermeidung von kriminellen Cyberangriffen sowie zur effektiven Schadensbegrenzung nach einer Datenschutzverletzung unter anderem einer kooperativen und gut organisierten Zusammenarbeit aller Beteiligten. Ich kann festhalten, dass die bereits gute Zusammenarbeit zwischen den

verantwortlichen Stellen und den Auftragsverarbeitern ausgebaut wurde und vor allem in umfangreichen Fällen effizienter und strukturierter gestaltet werden konnte.

Meldungen von Cyberangriffen auf Auftragsverarbeiter

In einem Fall wurde ich über einen Cyberangriff auf einen IT-Dienstleister informiert, der wiederum als Auftragsverarbeiter für einen Leasingdienstleister tätig war und sehr große Datenmengen über Beschäftigungsverhältnisse bundesweit tätiger Beschäftigter verarbeitet. Nachdem einige dieser Daten im Darknet abrufbar waren und die Medien erste Meldungen verbreiteten, war die Verunsicherung selbstverständlich auch bei den hessischen Betroffenen groß. Da beide Dienstleister ihren Sitz nicht in Hessen haben, musste im ersten Schritt der komplexe Sachverhalt, insbesondere die zugrundeliegenden Vertragsverhältnisse der Verantwortlichen mit den Dienstleistern, eruiert werden. Wer ist für welche Daten verantwortlich? Welche Aufsichtsbehörde übernimmt in der Folge die federführende Bearbeitung?

In einem weiteren Fall gab es einen Malwareangriff auf einen Dienstleister, der seinen Sitz ebenfalls außerhalb Hessens hat und der eine bundesweit genutzte Buchhaltungssoftware zur Verfügung stellt. Auch hier wandten sich zahlreiche Betroffene mit Sitz in Hessen an mich. In der Folge mussten bundeslandübergreifende Verantwortlichkeiten und die federführende Bearbeitung organisiert und geklärt werden.

Die beiden Fälle zeigen exemplarisch, dass eine strukturierte Zusammenarbeit zwischen allen Akteuren sehr wichtig und die Einhaltung von datenschutzrechtlichen Vorgaben in der Auftragsverarbeitung essenziell sind.

Meldung der Vorbereitung eines Cyberangriffs auf ein Klinikum

Auch im Gesundheitssektor gingen im Berichtsjahr Meldungen über die Verletzungen des Schutzes personenbezogener Daten im Zusammenhang mit Cyberangriffen ein.

In einem Fall stellte ein Klinikum bei einer Routinekontrolle die Vorbereitung zu einem Cyberangriff auf seine IT-Infrastruktur fest. Durch die sofortige Trennung des Netzwerks des Klinikums vom Internet konnten die Vollendung des Angriffs sowie Schäden verhindert werden, jedoch waren Mitarbeitende und Einrichtungen der Klinik von außen nicht erreichbar und konnten ihrerseits auch nicht nach außen kommunizieren. Dies führte im Rahmen der Meldung der Datenschutzverletzung u. a. zu der Frage, wie in einem solchen Fall ein sicherer digitaler Kommunikationsweg mit der Aufsichtsbehörde gewährleistet werden kann. Die Webseite des Klinikums wurde ebenfalls vom Netz

genommen. Die internen IT-Systeme funktionierten glücklicherweise weiter, die Patientenversorgung war nicht eingeschränkt.

Dieser Fall zeigt jedoch, dass der Schutz der kritischen Infrastruktur vor Cyberangriffen immens bedeutsam ist. Ein wesentlicher Aspekt dabei ist selbstverständlich die datenschutzkonforme Ausstattung und Einrichtung der IT-Infrastruktur. Ein erfolgreicher Cyberangriff hätte im vorliegenden Fall zu einer direkten Einschränkung der Gesundheitsversorgung von Bürgerinnen und Bürgern geführt.

Fazit und Empfehlung

Trotz der hohen Anzahl an gemeldeten Datenschutzverletzungen verfuhren in den meisten Fällen die verantwortlichen Stellen und Auftragsverarbeiter im Umgang mit und bei der Bewältigung von Datenschutzvorfällen auch in diesem Berichtsjahr entsprechend den datenschutzrechtlichen Anforderungen.

Aufgrund der anhaltenden bedrohlichen Cybersicherheitslage sowie der konstant hohen Anzahl von bekanntgewordenen Datenschutzverletzungen empfehle ich weiterhin allen verantwortlichen Stellen und Auftragsverarbeitern ausdrücklich, ein funktionierendes Datenschutzmanagementsystem zu etablieren. Denn nur durch entsprechende technische und organisatorische Maßnahmen einschließlich intensiver Schulungen von Mitarbeitenden in Fragen der IT-Sicherheit und des Datenschutzes lassen sich Datenschutzverletzungen abwehren oder eindämmen.

Darüber hinaus weise ich darauf hin, dass es unerlässlich ist, bezüglich des Umgangs mit Datenschutzvorfällen einen klaren Prozess zu definieren und diesen ständig weiterzuentwickeln. Dieser soll unter anderem gewährleisten, dass die betroffenen Stellen in kürzester Zeit ihren Melde- und Benachrichtigungspflichten gegenüber den Behörden und den betroffenen Personen in vollem Umfang nachkommen können.

14.7
Ransomware-Angriff auf eine hessische Kommune

Im Jahr 2023 kam es zu einem erfolgreichen Ransomware-Angriff auf eine hessische Kommune und deren Stadtwerke. Dabei wurden große Teile, des von diesen verantwortlichen Stellen selbst verarbeiteten Datenbestandes, verschlüsselt und es kam zu umfangreichen Einschränkungen für die öffentliche Verwaltung und die betroffenen Personen in der Kommune. Aufbauend auf einer Zusammenfassung des Vorfalls, den Auswirkungen und meiner aufsichtsbehördlichen Begleitung leite ich mögliche Lehren für kommunale

Verantwortliche in Hessen ab. Denn die Frage ist nicht, ob ein vergleichbarer Angriff eine andere Gemeinde treffen wird, sondern wann.

Risiken schwerer IT-Sicherheitsvorfälle

Einer auf gesetzlichen Vorgaben basierenden Verarbeitung personenbezogener Daten öffentlicher Stellen können sich betroffene Personen nicht entziehen. Daher stellen sowohl die DS-GVO als auch das BDSG und das HDSIG hohe Anforderungen an die Rechtmäßigkeit der Verarbeitung, den Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung ihrer Daten und insbesondere auch an die Sicherheit der Verarbeitung.

Schwere IT-Sicherheitsvorfälle in Kommunen, bei denen die Verfügbarkeit, Integrität und Vertraulichkeit der dort verarbeiteten Daten in Gefahr gerät, haben direkte Auswirkungen auf die jeweils betroffenen Personen. Ein bekanntes Beispiel dafür ist der erfolgreiche Ransomware-Angriff auf den Landkreis Anhalt-Bitterfeld in Sachsen-Anhalt im Jahr 2021. Dieser führte dazu, dass erstmals der Katastrophenfall wegen eines IT-Sicherheitsvorfalls ausgerufen werden musste und die Unterstützung der Bundeswehr notwendig war, um die IT-Systeme des Landkreises wiederherzustellen.

Im Berichtszeitraum wurde mir ein erfolgreicher Ransomware-Angriff auf eine hessische Kommune und deren Stadtwerke gemeldet. Im Rahmen meiner aufsichtsbehördlichen Begleitung des Vorfalls habe ich die Kommune bei der Erfüllung ihrer datenschutzrechtlichen Anforderungen unterstützt und konnte beobachten, welche Auswirkungen ein solcher Vorfall für die betroffenen Personen in einer Kommune haben kann. Aus der Beschreibung des Vorfalls und meiner Begleitung der verantwortlichen Stellen lässt sich aufzeigen, welche Lehren für andere Kommunen und allgemein den öffentlichen Bereich in Hessen aus einem solchen Vorfall gezogen werden können und müssen. Dieser Vorfall dient daher auch als warnendes Beispiel und Appell an die hessischen öffentlichen Stellen. Sie sollten ihn zum Anlass nehmen, um das aktuell umgesetzte Schutzniveau in der eigenen IT-Landschaft zu überprüfen, zu bewerten, zu evaluieren sowie bei Bedarf Anpassungen vorzunehmen und dies entsprechend zu dokumentieren.

Ablauf des Ransomware-Angriffs

Der Angriff auf die hessische Kommune ist dem bereits aus der Vergangenheit bekannten Ablauf von Ransomware-Angriffen gefolgt. Die generellen Hintergründe zu Ransomware-Angriffen, deren Ablauf und die resultierenden Risiken für Rechte und Freiheiten betroffener Personen hatte ich bereits unter

dem Titel „Ransomware und Ransomware-Angriffe“ in Kap. 18.2 meines 50. Tätigkeitsberichts erläutert.

Der Angriff auf die Kommune und ihre Stadtwerke begann mit einer authentisch erscheinenden Phishing-E-Mail, die aus dem kompromittierten E-Mail-Account eines Dritten verschickt wurde und sich auf eine bereits bestehende E-Mail-Kommunikation mit der verantwortlichen Stelle zu beziehen schien. Über diese Phishing-E-Mail wurde Schadsoftware auf einen Arbeitsplatzrechner eingeschleust und dort ausgeführt. Hierzu wurde eine Schwachstelle in der Notizbuchanwendung des eingesetzten Office-Produkts ausgenutzt. Die Schwachstelle war dem Hersteller zwar bekannt, zum Zeitpunkt des Angriffs hatte er aber noch kein entsprechendes Sicherheits-Update zur Verfügung gestellt. Nachdem die Angreifer Zugriff auf den ersten Arbeitsplatzrechner erlangt hatten, konnten sie sich weitergehende Zugriffsrechte verschaffen und sich in den IT-Systemen lateral ausbreiten, d. h. Zugriff auf weitere IT-Systeme erlangen. In diesem Zusammenhang erfolgte auch der Übergang von den IT-Systemen der Stadtwerke in die der Kommune. Wie bei Ransomware-Angriffen häufig vorkommend, wurden dabei auch die Domänen-Controller bzw. Active Directory Server der beiden verantwortlichen Stellen übernommen und dedizierte Domänen-Administratoren-Accounts angelegt. Mittels dieser speziellen Administratoren-Accounts erlangten die Angreifer den vollständigen Zugriff auf alle angebundenen IT-Systeme und Dienste und die darauf gespeicherten Daten. Das Ausbringen und Ausführen der eigentlichen Ransomware, also der Software, welche die auf den IT-Systemen gespeicherten Daten letztendlich verschlüsselt, erfolgte dann mittels dieser Domänen-Administratoren-Accounts. Dabei wurden die Daten auf nahezu allen im Zeitraum des Angriffs angeschalteten IT-Systemen der Kommune und der Stadtwerke verschlüsselt, insbesondere Server und Arbeitsplatzrechner.

Im Rahmen der IT-forensischen Analyse des Vorfalls wurden Hinweise darauf gefunden, dass die Angreifer von einem IT-System größere Datenmengen kopiert und heruntergeladen haben. Da die Angreifer dabei aber aktiv ihre Spuren verwischten, war es während der Analyse und Aufarbeitung des Vorfalls nicht möglich nachzuvollziehen, um welche Daten es sich dabei genau gehandelt hatte. Eine Veröffentlichung der Daten durch die Angreifer ist bis Ende 2023 nicht erfolgt.

Reaktion und Behandlung des Ransomware-Angriffs

Nachdem die verantwortlichen Stellen den Ransomware-Angriff entdeckt hatten, begannen sie mit den entsprechenden Notfallprozessen und beauftragten noch am selben Tag spezialisierte IT-Dienstleister für eine Unterstützung bei

der Behandlung und der IT-forensischen Analyse des Vorfalls. Auch erfolgten umgehend Meldungen an und die Einbindung von weiteren zuständigen Stellen in Hessen, wie der Polizei, des Hessen CyberCompetenceCenter (Hessen3C) und auch meiner Behörde.

Die Behandlung eines schweren IT-Sicherheitsvorfalls stellt einen Verantwortlichen in der Regel vor große Herausforderungen. Einen Überblick über das empfohlene Vorgehen und eine Handreichung aus Sicht der IT-Sicherheit gibt das BSI-Arbeitspapier „Erste Hilfe bei einem schweren IT-Sicherheitsvorfall“.[111]

Für die betroffene Kommune und ihre Stadtwerke hatte der Vorfall direkte und umfangreiche Auswirkungen. Betroffen waren unterschiedliche Personengruppen, insbesondere Einwohnerinnen und Einwohner sowie Mandatsträgerinnen und Mandatsträger der Kommune, Kundinnen und Kunden der Stadtwerke sowie Beschäftigte der Kommune und der Stadtwerke. Durch den Ausfall der gesamten IT-Infrastruktur kam es zu umfangreichen Einschränkungen für die Betroffenen. Als Teil der ersten Reaktion auf den Ransomware-Angriff mussten die verantwortlichen Stellen daher nicht nur den Vorfall selbst behandeln, sondern auch zeitnah einen Notbetrieb bereitstellen, um die Verfügbarkeit der wichtigsten Dienste für die betroffenen Personengruppen wiederherzustellen. Da wichtige Dienste der Kommune bei der ekom21, dem kommunalen IT-Dienstleistungsunternehmen in Hessen, betrieben wurden und dieses nicht vom Vorfall betroffen war, konnte durch die schnelle Unterstützung seitens der ekom21 und der Nachbargemeinden zeitnah ein Notbetrieb aufgebaut werden.

Die IT-forensische Untersuchung und Aufarbeitung des Ransomware-Angriffs und damit die Ermittlung der Aktivitäten der Angreifer und des Umfangs der Kompromittierung sind nicht nur aus Sicht der IT-Sicherheit ein unbedingtes Muss. Auch zur Erfüllung der gesetzlichen Anforderungen des Datenschutzes waren diese Maßnahmen als Reaktion unbedingt notwendig. Der entsprechende Untersuchungsauftrag beinhaltete daher nicht nur die Fragestellungen aus Sicht der IT-Sicherheit, sondern auch die aus Sicht des Datenschutzes. Ein zentrales Ziel des Datenschutzes ist nach Art. 1 DS-GVO der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Verantwortlichen mussten daher ermitteln und abschätzen, welche personenbezogenen Daten und Personen von dem Vorfall betroffen waren sowie welche Risiken durch die Verletzungen des Schutzes dieser Daten für die Rechte und Freiheiten der betroffenen Personen entstanden sind. Da die verantwortlichen Stellen umfangreiche Datenbestände verarbeiten, war zu-

111 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.html.

nächst nicht abzusehen, ob und wann die IT-forensische Analyse Gewissheit darüber liefern würde, welche Daten tatsächlich betroffen waren. Um sich auf alle Möglichkeiten vorzubereiten, wurden dedizierte Dienstleister beauftragt, alle potenziell betroffenen Daten zu erfassen, für diese mögliche Folgen der Verletzung des Schutzes personenbezogener Daten zu ermitteln und auf dieser Basis eine Risikobetrachtung durchzuführen. Diese vorausschauende Vorgehensweise wurde durch die verantwortlichen Stellen gewählt, um die Zeitspanne von der Verfügbarkeit der Analyseergebnisse über eine angepasste Risikobewertung zu einer gezielten Benachrichtigung betroffener Personen gemäß Art. 34 DS-GVO zu verkürzen. Aufgrund der potenziell großen Datenmengen ging es dabei insbesondere um die Frage, welche Daten die Angreifer exfiltriert und damit deren Vertraulichkeit verletzt haben könnten.

Wenn es zu einem schweren Datenschutzvorfall kommt, kann dies zu einem hohen Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen führen. Die Möglichkeiten der Betroffenen, dies im Nachhinein zu verhindern, sind begrenzt, etwa wenn es bereits zu einer Veröffentlichung der Daten betroffener Personen durch die Angreifer gekommen ist. Umso wichtiger ist es, dass die betroffenen Personen unverzüglich und in verständlicher Form über den Vorfall und die möglichen Folgen informiert werden. Art. 34 Abs. 1 DS-GVO verpflichtet Verantwortliche im Falle eines „hohen Risikos“ grundsätzlich zu einer individuellen Benachrichtigung der betroffenen Personen. Diese muss insbesondere auf die Art der Verletzung des Schutzes personenbezogener Daten eingehen (Art. 34 Abs. 2 DS-GVO) und die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (Art. 34 Abs. 2 in Verbindung mit Art. 33 Abs. 3 Buchst. c DS-GVO) sowie Maßnahmen zur Minderung möglicher Schäden aufzeigen (Art. 34 Abs. 2 in Verbindung mit Art. 33 Abs. 3 Buchst. d DS-GVO). Hierbei kann es zu einem Zielkonflikt zwischen der möglichst schnellen Benachrichtigung auf der einen und der detaillierten und individualisierten Benachrichtigung auf der anderen Seite kommen, da für letztere häufig umfangreiche, zeitaufwändige Analysen und Vorarbeiten notwendig sind. Auch kann der Aufwand für diese Analysen und die individuelle Benachrichtigung unverhältnismäßig hoch sein. Art. 34 Abs. 3 Buchst. c DS-GVO sieht daher Alternativen wie eine öffentliche Bekanntmachung vor.

Art. 34 DS-GVO

(1) Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

a) der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;

b) der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;

c) die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Art. 33 Abs. 3 DS-GVO

(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.

Die von dem Ransomware-Angriff betroffene Kommune und ihre Stadtwerke haben früh über Presseerklärungen, öffentliche Aushänge, die eigene Webseite und Anzeigen in einer lokalen Zeitung über den Vorfall und die Auswirkungen für betroffene Personen informiert. Damit haben sie nach derzeitigem Sachstand den Maßgaben des Art. 34 Abs. 3 Buchst. c DS-GVO entsprochen. Im Falle einer Veröffentlichung von personenbezogenen Daten oder aufgrund anderer Entwicklungen können sich gleichwohl die Risiken für die Rechte und Freiheiten der betroffenen Personen ändern. Die verantwortlichen Stellen müssen dann prüfen, ob es erforderlich ist, die betroffenen Personen erneut und ggf. individuell über den geänderten Sachverhalt und die daraus entstehenden Risiken zu benachrichtigen. Auch

müssen sie ggf. weitere Personen informieren, falls aufgrund der neuen Erkenntnisse nun auch für sie von einem hohen Risiko für ihre Rechte und Freiheiten auszugehen ist.

Um den Normalbetrieb wieder aufnehmen zu können, waren umfangreiche und zeitintensive Arbeiten notwendig. Die Umsetzung dieser Arbeiten wurde auf mehrere Monate veranschlagt. Daher planten die verantwortlichen Stellen, zusammen mit ihren spezialisierten IT-Dienstleistern einen Übergangsbetrieb für diesen Zeitraum, in dem sie Teile der alten IT-Systeme und Daten isoliert und besonders geschützt wieder in Betrieb nahmen. Im Rahmen des vollständigen Wiederherstellungsplans sollen die IT-Systeme neu konzeptioniert und dabei die Erfahrungen aus dem Vorfall sowie der Stand der Technik berücksichtigt werden.

Die datenschutzrechtliche Begleitung des Vorfalls

Auf Grund der Bedeutung und Dringlichkeit des Ransomware-Angriffs auf die Kommune und ihre Stadtwerke führte ich nach dem Vorfall einen Ortstermin durch, um mich über den aktuellen Sachstand informieren zu lassen (allgemein zur Begleitung von schweren Datenschutzverletzungen s. Kap. 14.4). Vier meiner Beschäftigten aus juristischen und technischen Referaten besuchten dazu die Kommune. Bei diesem Austausch waren alle relevanten Beteiligten vertreten, insbesondere auch Vertreter der engagierten Dienstleister und des Hessen3C. Neben der Erläuterung des aktuellen Sachstands besprachen wir auch das weitere Vorgehen im Hinblick auf die Anforderungen des Datenschutzes. Ein wichtiges Thema war mir dabei die Aufklärung und Benachrichtigung der betroffenen Personen.

Im Rahmen des Gesprächs zeigte sich, dass die Kommune den Datenschutz und die IT-Sicherheit grundsätzlich sehr ernst genommen hat. Die engagierte IT-Abteilung war im Rahmen ihrer finanziellen und personellen Möglichkeiten bereits vor dem Vorfall aktiv damit befasst, die Sicherheit der Datenverarbeitung kontinuierlich zu verbessern. Unter anderem war bereits vor dem Vorfall für die folgende Woche eine umfangreiche Sensibilisierungskampagne eines externen Dienstleisters geplant, um die Beschäftigten für typische Angriffe auf IT-Umgebungen wie Phishing mit simulierten Angriffen zu sensibilisieren. Auch war geplant, die IT-Systeme der Kommune mit neuen Arbeitsplatzrechnern auszustatten und dabei die IT-Systemarchitektur zu verbessern. Glücklicherweise waren die dafür notwendigen IT-Systeme bereits beschafft und eingelagert worden. Sie konnten daher direkt für den Übergangsbetrieb und die Wiederherstellung der IT-Landschaft genutzt werden. Dieser Umstand hat sicherlich dazu beigetragen, die Wiederherstellungszeit um Wochen, ggf. auch Monate verkürzen zu können.

Die verantwortlichen Stellen sind bei dem Vorfall auch den Empfehlungen des BSI gefolgt und haben keinen Kontakt zu den Angreifern aufgenommen und sind auch deren Forderungen nicht nachgekommen. Als Gründe für diese Empfehlung kann hier genannt werden, dass es selbst bei einer Zahlung keine Garantien gibt, dass die kriminellen Angreifer ihre Zusagen einhalten, d. h. funktionierende Entschlüsselungs-Software bereitstellen und alle Kopien der exfiltrierten Daten löschen, ohne diese an weitere Kriminelle weitergegeben oder verkauft zu haben. Für die Bewertung des Risikos aus Sicht des Datenschutzes für die Rechte und Freiheiten der betroffenen Personen wäre daher eine Zahlung auch grundsätzlich keine geeignete Maßnahme, um Risiken zuverlässig und hinreichend zu reduzieren. Darüber hinaus muss festgestellt werden, dass diese Ransomware-Angriffe durch organisierte Kriminelle durchgeführt werden, um damit Geld zu verdienen und damit u. a. ihre „Beschäftigten" zu bezahlen. Durch die Zahlungen von Lösegeld entsteht entsprechend erst der Anreiz für organisierte Kriminelle, Ransomware-Angriffe durchzuführen. Sollten die Angreifer aus Russland stammen, könnten Lösegeldzahlungen auch gegen Boykott-Vorschriften verstoßen.

Zum Zeitpunkt des Treffens konnten viele Fragen zum Hergang und den Auswirkungen des Angriffs, insbesondere welche personenbezogenen Daten betroffen waren, nicht abschließend beantwortet werden. Bezüglich der Verfügbarkeit konnte aber bereits klargestellt werden, dass die Angreifer zwar das Online-Datensicherungssystem der Kommune kompromittieren konnten, aber nicht die regelmäßige Offline-Sicherung auf Magnetbändern. Um die Datenlücke von einem Tag seit der letzten Sicherung auf den Bändern vor dem Vorfall zu kompensieren, hatte die verantwortliche Stelle umgehend die Beschäftigten aufgefordert, die letzten Vorgänge manuell aus dem Gedächtnis zu erfassen. Durch die zeitnahe Reaktion und das Engagement der Beschäftigten schätzten die Verantwortlichen die entstandenen Datenverluste als vernachlässigbar ein. Bezüglich der Identifikation der betroffenen Daten und Personen erläuterten die verantwortlichen Stellen und ihre Dienstleister das geplante Vorgehen. Durch die Berücksichtigung meiner Anmerkungen und Hinweise konnte dieses bereits sehr gute Konzept weiter verbessert werden.

Nach dem Termin vor Ort kamen die verantwortlichen Stellen bei Fragen oder relevanten Sachstandsänderungen auf mich zu. Zur Klärung der offenen Fragen und zur Ermittlung des Gesamtzusammenhangs des Ransomware-Angriffs und seiner Folgen schickte ich den Verantwortlichen einen umfangreichen Fragenkatalog, den diese sehr detailliert und nachvollziehbar beantwortet haben. Bis zur vollständigen Wiederherstellung der IT-Systeme und der Umsetzung der geplanten technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durch die verantwortlichen Stellen wird meine Behörde den Vorfall weiter begleiten.

Lehren für andere hessische Kommunen

Die vollständige Bewältigung der Folgen des Vorfalls und die Wiederherstellung des regulären IT-Betriebs wird diese öffentlichen Stellen wahrscheinlich mehrere Jahre beschäftigen. Allerdings kann ich auf Basis meiner aufsichtsbehördlichen Praxiserfahrung auch feststellen, dass die Auswirkungen wesentlich gravierender hätten ausfallen können, wenn die betroffene Kommune und deren Stadtwerke hinsichtlich der IT-Sicherheit nicht bereits relativ gut aufgestellt gewesen wären und über gut motiviertes und belastbares IT-Personal verfügt hätten.

Was lässt sich daher aus dem Fallbeispiel für andere hessische Kommunen ableiten? Das BSI hat in seinem Lagebericht für 2023 „Die Lage der IT-Sicherheit in Deutschland 2023“[112] festgestellt, dass KMUs und Kommunalverwaltungen sowie kommunale Versorgungsbetriebe überproportional häufig von Ransomware-Gruppen angegriffen wurden. Dem Lagebericht folgend ist die Bedrohungslage so hoch wie nie zuvor. Auf Basis der mir im Berichtszeitraum gemeldeten Vorfälle in Bezug auf Ransomware- oder andere schwere IT-Sicherheitsvorfälle kann ich dieser Schlussfolgerung des BSI zustimmen. Mit Blick auf die wachsende Professionalisierung der Angreifer stellt sich nicht mehr die Frage, ob ein vergleichbarer Angriff auch andere öffentliche Stellen in Hessen treffen wird, sondern wann. Für jede Kommune und andere öffentliche Stelle in Hessen ist es mehr denn je notwendig, sich diesem Gedanken zu stellen. Denn der Umfang und die Schwere der durch einen solchen Vorfall verursachten Auswirkungen für die betroffenen Personen wird auch maßgeblich davon abhängen, wie gut diese Stelle darauf vorbereitet sein wird und reagieren kann. Die hessischen Kommunen sind hier stark gefordert, mit der fortschreitenden Professionalisierung der Angreifer Schritt zu halten.

Grundsätzlich müssen verantwortliche Stellen, wie Kommunen und kommunale Versorgungsbetriebe, die Anforderungen der DS-GVO und des HDSIG erfüllen. Dazu gehört, dass sie nach Art. 32 DS-GVO für die Verarbeitung von personenbezogenen Daten ein dem Risiko angemessenes Schutzniveau gewährleisten müssen. Die Anforderungen des Datenschutzes können hierbei von denen der IT-Sicherheit abweichen. Eine wichtige Voraussetzung dazu ist die Sicherstellung der Verfügbarkeit von qualifiziertem Personal in hinreichender Zahl, um diese Aufgaben erfüllen zu können. Dazu gehört es nicht nur, eine entsprechende IT-Infrastruktur aufzubauen und zu betreiben, sondern es müssen auch kontinuierlich die Angemessenheit und Wirksamkeit der

112 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410

umgesetzten Maßnahmen überprüft, bewertet und evaluiert werden (s. auch Art. 32 Abs. 1 Buchst. d DS-GVO). Sie müssen auch ggf. einen identifizierten Anpassungsbedarf entsprechend umsetzen. Ein Erfahrungsaustausch der Kommunen untereinander, gerade mit denen, die einen Vorfall überwunden haben, wäre aus Sicht des technischen Datenschutzes zu begrüßen.

Für verantwortliche Stellen in Hessen, nicht nur für Kommunen und kommunale Versorgungsbetriebe, gibt es unterschiedliche Hilfs- und Beratungsangebote, um die Verbesserung der Sicherheit der Verarbeitung zu unterstützen. Diese sollten insbesondere auch dann genutzt werden, wenn es zu einem schweren Vorfall gekommen ist. Das BSI bietet u. a. für Kommunen umfangreiche Unterstützungsangebote, die auch über den IT-Grundschutz hinausgehen.[113]

In Hessen bietet das Hessen3C zusätzlich verschiedene Leistungen gezielt für Kommunen an.[114] Weiterhin betreibt das Hessen3C eine Notfall-Hotline, um rund um die Uhr eine Soforthilfe bei IT-Sicherheitsvorfällen für Stellen in Hessen anbieten zu können.[115]

Auch meine Behörde berät verantwortliche Stellen auf Anfrage bei konkreten Fragen zur Umsetzung der DS-GVO und Maßnahmen des technischen und organisatorischen Datenschutzes. Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, mit Risiken für die betroffenen Personen, muss mir diese gemäß Art. 33 Abs. 1 DS-GVO gemeldet werden.

14.8
Vorsicht beim Einsatz privater Endgeräte zu dienstlichen Zwecken

Gestattet eine verantwortliche Stelle, dass Mitarbeiterinnen und Mitarbeiter private Endgeräte und von ihnen selbst ausgewählte Apps zum Zugriff auf ihre IT-Systeme und -Dienste nutzen, muss sie darauf bezogene, geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Tut sie dies nicht, kann darin ein Datenschutzverstoß – insbesondere gegen die Vorschriften des Art. 32 Abs. 1 DS-GVO – liegen, da sie ihre IT-Systeme und -Dienste der Gefahr eines unbefugten Zugriffs durch Dritte aussetzt, beispielsweise wenn das durch den Mitarbeiter oder die Mitarbeiterin genutzte Endgerät mit einer Schadsoftware infiziert ist oder eine genutzte App ein maliziöses Verhalten zeigt.

113 https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitsberatung/Laender-und-Kommunen/laender-und-kommunen.html.

114 https://hessen3c.de/unsere-leistungen/fuer-kommunen.

115 https://hessen3c.de/soforthilfe-bei-cyberangriffen.

Im Berichtszeitraum erreichte mich die Meldung einer Hochschule über eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 1 DS-GVO, die durch den Zugriff unbefugter Dritter auf das E-Mail-Konto eines Mitarbeiters der Hochschule verursacht wurde. Im Unterschied zu vielen anderen Meldungen im Zusammenhang mit E-Mail-Konten war in diesem Fall jedoch kein erfolgreicher Phishing-Angriff Grundlage für den Zugriff auf das E-Mail-Konto. Stattdessen hatte der Mitarbeiter eine von ihm selbst gewählte E-Mail-App auf seinem privaten Endgerät installiert, seine Zugangsdaten darin eingegeben und anschließend diese App für die Kommunikation mit dem dienstlichen E-Mail-Server verwendet. Der Verantwortliche hatte keine Dienstanweisung erlassen oder sonstige Maßnahmen getroffen, die diesem Einsatz entgegengestanden hätten. Die installierte App schien für den Mitarbeiter den gewünschten Zweck zu erfüllen, da sie ihm den Abruf sowie den Versand von E-Mails über das dienstliche E-Mail-Konto ermöglichte. Verborgen für den Mitarbeiter versendete diese App jedoch im Hintergrund die von dem Mitarbeiter preisgegebenen Zugangsdaten an Dritte. Diese nutzten die erbeuteten Zugangsdaten, um mehrfach auf Inhalte des betroffenen E-Mail-Kontos zuzugreifen und das Konto für den Versand von Spam- und Phishing-Mails zu missbrauchen.

Das Gestatten der Nutzung von privaten mobilen Endgeräten wie beispielsweise Handys und Tablets in der Organisation, auch als „Bring Your Own Device“ (BYOD) bezeichnet, kann mitunter zwar funktionale Vorteile, aber auch Risiken in den Bereichen des Datenschutzes oder der IT-Sicherheit für verantwortliche Stellen mit sich bringen. Die Beispiele für solche Risiken sind mannigfaltig und abhängig von den Gegebenheiten, bei denen der Einsatz von BYOD-Geräten im Organisationsbereich stattfindet. Aus technischer Sicht des Datenschutzes ergeben sich u. a. folgende Gefährdungen beim Einsatz von BYOD-Geräten im Organisationsnetzwerk, falls dieser ohne geeignete technische und organisatorische Maßnahmen erfolgt:

– Durch die Nutzung von BYOD-Geräten kann Schadsoftware in das Organisationsnetzwerk eingeschleust werden.
– Schadsoftware auf den BYOD-Geräten kann für die Nutzerin oder den Nutzer unbemerkt personenbezogene Daten an unbefugte Dritte übermitteln.
– Durch den Diebstahl oder Verlust von BYOD-Geräten können personenbezogene Daten Unbefugten offengelegt werden.

Aktuell gängige Plattformen für mobile Endgeräte wie Android oder Apple iOS bieten der Nutzerin oder dem Nutzer ferner die Möglichkeit, aus einer sehr großen Vielzahl von Apps auszuwählen und diese auf ihrem eigenen Gerät zu installieren. Hierbei können Nutzerinnen und Nutzer beispielsweise ungewollt Apps mit schädigendem Verhalten installieren, etwa wenn eine

vermeintlich valide und sichere App aus einer unsicheren Quelle bezogen wird. Zu beachten ist hierbei, dass die bloße Anforderung an Nutzerinnen und Nutzer von BYOD-Geräten, Apps ausschließlich aus offiziellen Apps-Stores zu beziehen, ohne die Implementierung weiterer geeigneter Maßnahmen aus technischer Sicht des Datenschutzes regelmäßig noch nicht ausreichend ist, um ein angemessenes Schutzniveau zu gewährleisten. In dem vorliegenden Fall hatte der Mitarbeiter die maliziöse E-Mail-App für sein BYOD-Gerät aus dem offiziellen App-Store des Anbieters des Geräts bezogen.

Um diesen und auch weiteren Risiken zu begegnen, haben verantwortliche Stellen gemäß Art. 32 Abs. 1 DS-GVO die Pflicht, geeignete technische und organisatorische Maßnahmen (TOM) zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Die im Folgenden beschriebenen Maßnahmen stellen beispielhaft gängige Vorgehensweisen zur Minderung von Risiken im Zusammenhang mit BYOD-Geräten dar. Die Darstellung der Maßnahmen ist an dieser Stelle jedoch nicht abschließend. Verantwortliche Stellen müssen stets selbst und ausgehend von ihrer eigenen Verarbeitung – insbesondere anhand der Bewertungsmaßstäbe der Art. 24 Abs. 1, 25 Abs. 1, 32 Abs. 1 DS-GVO – geeignete Maßnahmen auswählen, prüfen, umsetzen und fortlaufend auf ihre Geeignetheit prüfen sowie ggf. anpassen.

Auf organisatorischer Ebene sollten Verantwortliche beispielsweise klare BYOD-Richtlinien definieren, die Sicherheitsanforderungen, Verhaltensregeln und Datenschutzbestimmungen umfassen. Ferner können geeignete Schulungen der Mitarbeiterinnen und Mitarbeiter in Bezug auf bewusstes und sicheres Verhalten im Umgang mit den BYOD-Geräten dazu beitragen, mögliche Risiken zu reduzieren.

Auf technischer Ebene kann der Einsatz von Mobile Device Management (MDM)- oder Enterprise Mobility Management (EMM)-Lösungen helfen, die Sicherheit und das Management von BYOD-Geräten zu verbessern. Eine Möglichkeit zur Kontrolle der auf den BYOD-Geräten genutzten Apps ist beispielsweise, eine geeignete MDM- oder EMM-Lösung durch den Einsatz eines Whitelistings zu erweitern. Hierbei wird durch die zuständigen IT-Fachbereiche eine Liste von zugelassenen Anwendungen (Whitelist) erstellt und in der Lösung hinterlegt. Mitarbeiterinnen und Mitarbeiter können daraufhin nur Apps aus dieser Whitelist installieren und verwenden, während die Installation von Apps ohne Freigabe durch die Whitelist unterbunden wird.

Eine weitere Möglichkeit zur Einflussnahme auf die genutzten Apps stellt der Einsatz einer Verwaltungstechnik in Form eines getrennten Arbeitsbereiches oder eines speziellen App-Containers auf den BYOD-Geräten dar. Bei Geräten auf Android-Basis wird diese Technologie als Arbeitsprofil bezeichnet.

Ein Arbeitsprofil erstellt zwei separate Bereiche auf einem Android-Gerät, einen für persönliche und einen für berufliche Anwendungen und Daten. Diese Bereiche sind voneinander isoliert und können grundsätzlich nicht miteinander kommunizieren. Das Arbeitsprofil ermöglicht es den zuständigen IT-Fachbereichen, das berufliche Profil im Sinne der beruflich zu nutzenden Anwendungen und Daten zu verwalten sowie Richtlinien und Sicherheitsmaßnahmen umzusetzen, ohne dass hierbei die persönlichen Daten der Nutzerin oder des Nutzers beeinträchtigt werden. Der Anbieter Apple spricht bei seinen Geräten hingegen von einer sogenannten Verwaltungsarchitektur. Bei dieser ist die Funktionsweise ähnlich wie bei Android-Arbeitsprofilen, jedoch speziell auf Apple-Geräte und das Apple-Ökosystem abgestimmt.

Darüber hinaus sollten verantwortliche Stellen, wenn sie den Einsatz von BYOD-Geräten in ihrem Organisationsnetzwerk erlauben möchten, sicherstellen, dass ihre zuständigen IT-Fachbereiche fachlich und organisatorisch in der Lage sind, die getroffenen technischen und organisatorischen Maßnahmen umzusetzen und die verschiedenen Gerätetypen und -plattformen der Nutzer zu unterstützen. Das Management von Softwareupdates und Sicherheitsrichtlinien für diese verschiedenen Gerätetypen und -plattformen kann für diese Fachbereiche ebenso eine Herausforderung darstellen und sollte entsprechend fachlich und organisatorisch sichergestellt sein, z. B. durch das Bereitstellen angemessener personeller, technischer und finanzieller Ressourcen sowie die Festlegung geeigneter Prozesse, idealerweise unter Unterstützung durch Managementsysteme.

In dem vorliegenden Fall hat mir die Hochschule nach Rücksprache zum Sachverhalt zugesagt, geeignete technische und organisatorische Maßnahmen zu prüfen und umzusetzen, um den Risiken beim Einsatz von BYOD-Geräten zu begegnen und ein angemessenes Schutzniveau zu gewährleisten. Für die Nutzung von Apps auf BYOD-Geräten möchte die Hochschule als erste Maßnahme zukünftig Empfehlungen für geprüfte Apps aussprechen und den Zugriff von bekannten schadhaften Apps auf das Hochschulnetzwerk an den Firewall-Systemen der Hochschule blockieren.

In dem hier behandelten Beispielfall gehe ich davon aus, dass diese zusätzlichen Maßnahmen grundsätzlich geeignet sind, einen angemessenen Schutz personenbezogener Daten bei der Hochschule künftig zu gewährleisten.

15. Öffentlichkeitsarbeit

Nach Art. 57 Abs. 1 Buchst. b DS-GVO habe ich die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung von Daten zu sensibilisieren und sie darüber aufzuklären. Darüber hinaus habe ich nach Art. 57 Abs. 1 Buchst. d DS-GVO die Verantwortlichen und die Auftragsverarbeiter für die ihnen, aus dieser Verordnung entstehenden Pflichten, zu sensibilisieren. Um diesen Aufgaben noch besser nachzukommen, habe ich die Öffentlichkeitsarbeit im Berichtsjahr intensiviert. Neben Veranstaltungen (Kap. 15.1) und dem Erscheinen in dem sozialen Netzwerk Mastodon (Kap. 15.2) haben meine Mitarbeiterinnen und Mitarbeiter und ich durch Vorträge und verschiedene Veröffentlichungen den Austausch mit der Öffentlichkeit gesucht (Kap. 15.3).

15.1 Veranstaltungen

Die von mir durchgeführten Veranstaltungen dienten einerseits der Diskussion von Fachfragen mit Fachpublikum (z. B. Tagung) und andererseits der Vorstellung meiner Behörde in der Öffentlichkeit (z. B. Messe).

Hessentag 2023

Meine Behörde hat sich im Berichtsjahr zum ersten Mal auf dem Hessentag vorgestellt, der 2023 in Pfungstadt stattfand. Mit Blick auf die Verpflichtung aus Art. 57 DS-GVO habe ich mich dazu entschieden, als Aussteller am Hessentag teilzunehmen. Der HBDI hatte einen Stand im Zelt des Landtages, das Teil des Areals „Treffpunkt Hessen“ war.

Die Erfahrung aus den zehn Tagen Hessentag hat gezeigt, dass dies ein guter und richtiger Schritt war. Die Mitarbeiterinnen und Mitarbeiter am Stand waren im regen Austausch mit fachlich Interessierten, die großes Interesse daran zeigten, die Personen hinter dem langen Behördennamen kennenzulernen. Darüber hinaus bestand die Gelegenheit, sich mit Bürgerinnen und Bürgern über ihre Fragen zum Datenschutz auszutauschen und so auch einen direkten Eindruck davon zu bekommen, „wo der Schuh drückt“. Das Interesse war sehr groß, Meinungen und Fragen in dem jeweiligen Kontext zu diskutieren. Großer Bedarf bestand insbesondere bei der Beratung im Zusammenhang mit Tracking und Cookies. Hier entwickelten sich unterschiedlichste Gespräche vom allgemeinen Austausch über das Thema bis hin zur Bitte um direkte Hilfe am eigenen Mobiltelefon einer Besucherin.

Neben den Gesprächen kam es auch zu Fragen und einem Austausch rund um die Datenschutzgrundprinzipien des Art. 5 DS-GVO. Anhand verschiedener Plakate konnten Besucherinnen und Besucher sich darüber informieren und diskutieren. Ebenso haben meine Mitarbeitenden und ich über Arbeit, Zuständigkeiten und Abläufe im Beschwerdeverfahren und im Fall von Datenschutzverletzungen informiert. Für manch eine Besucherin oder einen Besucher war meine Behörde auch ganz neu. Hier haben wir überhaupt erst auf unsere Existenz und unsere Arbeit sowie die Möglichkeit von Beschwerden und Meldungen von Datenschutzverletzungen aufmerksam gemacht.

Im Ergebnis war der Stand auf dem Hessentag für beide Seiten so fruchtbar, dass ich beschlossen habe, auch 2024 am dem Hessentag in Fritzlar als Aussteller teilzunehmen.

Datenschutztag Hessen-Rheinland-Pfalz

Darüber hinaus war ich bei zwei großen Veranstaltungen Mitveranstalter. Am 5. Juli 2023 fand unter dem Motto „Datenschutz & Digitalisierung Hand in Hand voraus“ der 2. Datenschutztag Hessen & Rheinland-Pfalz statt. Die Fachtagung in Kooperation mit dem BvD e. V. und dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz war wieder ein voller Erfolg. Der Datenschutztag richtete sich zuallererst an Datenschutzbeauftragte öffentlicher Stellen, die sich dort unter anderem über aktuelle Fragen des internationalen Datentransfers und der Künstlichen Intelligenz in der öffentlichen Verwaltung ebenso wie über die Struktur der Landesdatenschutzgesetze und deren Zusammenspiel mit europäischen Regelwerken, wie der Datenschutz-Grundverordnung und der Datenschutz-Richtlinie im Bereich von Justiz und Innerer Sicherheit, informieren konnten. Daneben gab es Foren, die sich zum Beispiel mit Fragen rund um Datenschutzverletzungen befassten. Die Veranstaltung gab insbesondere Datenschutzbeauftragten öffentlicher Stellen die Gelegenheit, sich mit Fachleuten aus den Aufsichtsbehörden über Themen auszutauschen, die sie in ihrer alltäglichen Berufspraxis beschäftigen. Die Teilnehmenden konnten sich dabei nicht nur untereinander austauschen, sondern mit ihren Fragen auch direkt an die Fachleute aus den Aufsichtsbehörden herantreten. Ein positiver Nebeneffekt war die Gelegenheit der Vernetzung über die Landesgrenzen hinaus.

Ich habe eine Keynote zum Thema „Datenschutz – Wie gelingt eine gute Umsetzung?“ gehalten. Mein Kollege Prof. Dr. Dieter Kugelmann, der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz, sprach zum Thema „Fünf Jahre DS-GVO – Fünf Fragen“. Dr. Fedor Ruhose, Staatssekretär im Ministerium für Arbeit, Soziales, Transformation und Digitalisierung des Landes Rheinland-Pfalz, sprach über „Datenschutz

und Digitalisierung – Hand in Hand voraus“. Die Abschluss-Keynote hielt Lisa-Marie Lange, stellvertretende Hessische Beauftragte für Datenschutz und Informationsfreiheit, zum Thema „Data Privacy Framework – Eine (vertane) Chance?“. Die Schlussrunde der Tagung unter dem Motto „Die Aufsichtsbehörden beantworten Ihre Fragen“ mit den beiden Landesdatenschutzbeauftragten fand regen Zuspruch.

Streit-Gespräch: 40 Jahre Volkszählungsurteil

Am 15. Dezember 2023 hatte das Volkszählungsurteil des Bundesverfassungsgerichts seinen 40. Geburtstag. Aus diesem Anlass habe ich einen Beitrag in der Zeitschrift „Juristische Ausbildung“ 2023, S. 1363–1375, unter dem Titel „40 Jahre Volkszählungsurteil des Bundesverfassungsgerichts“ veröffentlicht. Zusätzlich habe ich am 15. Dezember 2023 im Museum für Kommunikation in Frankfurt ein Streitgespräch mit dem Titel „40 Jahre Volkszählungsurteil des Bundesverfassungsgerichts – 40 Jahre Datenschutz als Grundrecht. Notwendiger Schutz oder übertriebene Bürokratisierung?“ veranstaltet. Die Veranstaltung hat meine Behörde in Kooperation mit der Plattform Privatheit[116] und dem Museum für Kommunikation organisiert.[117]

Am Tag der Veranstaltung lag die Verkündung der Entscheidung des Bundesverfassungsgericht auf den Tag genau 40 Jahre zurück. Selten hat ein Urteil so tiefgreifende und weitreichende Folgen gehabt. In ihm konkretisierte das Gericht die Grundrechte auf Menschenwürde und Persönlichkeitsentfaltung für die damals neuen Bedingungen der automatisierten Datenverarbeitung. Es erkannte ein neues ungeschriebenes Grundrecht auf informationelle Selbstbestimmung als Ausprägung dieser beiden Grundrechte an. Neue Risiken bedurften eines neuen Schutzes durch das Grundgesetz. Diese Risiken sah das Bundesverfassungsgericht darin, dass personenbezogene Daten „technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschelle abrufbar“ sind. „Sie können darüber hinaus … zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich … die Möglichkeiten einer Einsicht- und Einflussnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.“

Dem stellte das Bundesverfassungsgericht das Recht jedes Einzelnen entgegen, „grundsätzlich selbst über die Preisgabe und Verwendung seiner

116 https://www.forum-privatheit.de/.

117 https://www.mfk-frankfurt.de/.

persönlichen Daten zu bestimmen“. Dieses Grundrecht auf informationelle Selbstbestimmung ist seitdem die verfassungsrechtliche Grundlage des Datenschutzrechts und der wichtigste Maßstab, um Entwicklungsschritte der Digitalisierung der Gesellschaft verfassungsrechtlich zu bewerten.

Anlässlich dieses besonderen Jubiläums sollte die Veranstaltung das Urteil mit Blick auf seine Entstehungsbedingungen, seine Bedeutung und seine Wirkungsgeschichte erläutern, vor allem aber wurde kontrovers darüber diskutiert, was informationelle Selbstbestimmung heute bedeuten kann – in einer Welt, in der sich Daten zu einer entscheidenden wirtschaftlichen Ressource, zu einem Mittel für Forschung und Entwicklung, zu einer zentralen Grundlage von Machtausübung und nicht zuletzt zum einem Mittel der individuellen und kollektiven Verhaltenssteuerung entwickelt haben.

Mit mir diskutierten Dr. h.c. Marit Hansen, Vorsitzende der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), und Axel Voss, Mitglied des Europäischen Parlaments und Rechtspolitischer Sprecher sowie Digitalisierungsexperte der Fraktion der Europäischen Volkspartei (EVP). Moderiert wurde die Veranstaltung von Marion Kuchenny vom Hessischen Rundfunk.

15.2
Soziale Medien datenschutzgerecht nutzen – Der HBDI auf Mastodon

Mir ist es ein besonderes Anliegen, über den Datenschutz, die Informationsfreiheit und seine Tätigkeit zu informieren und aufzuklären. In einer Zeit, in der immer mehr Bürgerinnen und Bürger soziale Medien nutzen, ist es daher von großem Interesse, als Aufsichtsbehörde dort ebenfalls mit einer Präsenz vertreten zu sein. Daher habe ich mich dazu entschlossen, beim Kurznachrichtendienst Mastodon einen Account zu eröffnen, mich damit entsprechenden Bemühungen der Landesregierung anzuschließen und zugleich Vorbild zu sein.

Mastodon stellt eine datenschutzrechtlich vorzugswürdige Alternative zu den gängigen Sozialen Netzwerken dar, gegen deren Nutzung teilweise erhebliche datenschutzrechtliche Bedenken bestehen (s. Kap. 1.2). Insbesondere im Fall von Facebook-Seiten haben sowohl Datenschutzaufsichtsbehörden als auch Gerichte in der Vergangenheit immer wieder deutlich gemacht, dass öffentliche Stellen diese nicht datenschutzkonform betreiben können.

Der Dienst Mastodon unterscheidet sich von anderen Sozialen Medien wie Facebook, Instagram oder X in mehreren Aspekten: Zum einen handelt es sich um ein dezentrales Netzwerk. Das heißt, es gibt nicht nur einen einzigen Betreiber, sondern es handelt sich um eine Software, die auf zahlreichen

Servern weltweit betrieben wird. Anbieter können dabei Privatpersonen, Vereine, Institutionen oder Unternehmen sein. Zum anderen wird das Netzwerk nicht kommerziell betrieben und verzichtet auf die Einblendung von Werbung und damit auch auf personalisierte Werbeanzeigen. Es werden daher keine Nutzerdaten gesammelt oder persönliche Profile erstellt. Zudem ist Mastodon Teil des Fediverse, eines Netzwerks aus zahlreichen miteinander kompatiblen sozialen Netzwerken, zu denen auch Facebook- und Instagram-Alternativen zählen.

Aufgrund der dezentralen Struktur des Netzwerks wird zum Betreiben eines Accounts zunächst ein entsprechender Server, genannt Instanz, benötigt. Für die Landesbehörden des Landes Hessen stellt die Staatskanzlei diese bereit. So ging im Februar 2023 die Mastodon-Instanz der Hessischen Landesregierung online, auf der die Ministerien seitdem mit eigenen Accounts vertreten sind. Im April folgte auf derselben Instanz der HBDI mit seinem Account. Die neue Präsenz erfreute sich schnell großer Beliebtheit, so stieg die Zahl der Follower bis zum Jahresende auf über 600 an. Das hohe Interesse an den Veröffentlichungen des HBDI auf Mastodon dürfte nicht zuletzt mit der hohen Präsenz von Personenkreisen auf dieser Plattform zusammenhängen, die sich insbesondere für Themenbereiche wie Datenschutz oder Informationssicherheit interessieren. Ich informiere über meinen Mastodon-Account aktiv über meine Arbeit, neue Veröffentlichungen und anstehende Veranstaltungen. Daneben stehe ich auf Mastodon auch für Anfragen zu konkreten Sachverhalten zur Verfügung. Auch diese Möglichkeit wird von Nutzerinnen und Nutzern rege genutzt. Im Vergleich zu anderen Sozialen Medien zeichnet sich die Öffentlichkeitsarbeit auf Mastodon durch eine ungewöhnlich hohe Interaktionsrate in Form von geteilten Beiträgen, Likes und Kommentaren aus. Dennoch finden auf Mastodon keine Hassreden und kein Hetzen statt. Die bisherigen Erfahrungen zeigen, dass die Nutzung von Sozialen Medien durch Behörden auch abseits kommerzieller und datenschutzrechtlich problematischer Plattformen lohnenswert sein kann.

15.3
Vorträge und Veröffentlichungen

Auch in diesem Jahr waren meine Mitarbeiterinnen, meine Mitarbeiter und ich rege als Referentinnen und Referenten in Deutschland unterwegs. Ich selbst habe Vorträge beim Presserechtsforum 2023, bei der Frühjahrstagung 2023 der „Zentren für Kommunikation und Informationsverarbeitung in Lehre und Forschung e. V.“ (ZKI), beim Deutschen Ethikrat, bei der Nationalen Konferenz IT-Sicherheitsforschung des Bundesministeriums für Bildung und Forschung, beim CAST-Forum Recht und Informationstechnik zu „Di-

gitaler Souveränität“, bei der Datenschutzfachtagung 2023 des TÜV Nord, beim 129. Kongress der deutschen Gesellschaft für Innere Medizin (DGIM), beim 21. FFD-Jahreskongress, beim Datenschutzrechtstag 2023 „Arbeiten in der Cloud und Cybersicherheit“, in der Ringvorlesung „Datenschutz und Datensicherheit und ihre gesellschaftlichen Auswirkungen“ der Goethe-Universität Frankfurt, beim 24. Datenschutzkongress des Euroforums 2023, bei der Podiumsdiskussion im Livestream „#ONKOdigital“ der Ärztezeitung, vor dem Rechtsausschuss des Bundes der Deutschen Industrie (BDI), auf der Sommerakademie des ULD in Schleswig-Holstein, auf der Tagung des ZEVEDI „Zeitenwende beim Datenzugang?“, beim Fachgespräch des Landesbeauftragten für Datenschutz und Informationsfreiheit Rheinland-Pfalz „Was passiert mit unseren Gesundheitsdaten“, auf der Fachtagung Arbeitsrecht 2023 des Bundesverbands der Arbeitsrechtler in Unternehmen e. V. (BVAU), in der Veranstaltung des HBDI, der Plattform Privatheit und des Museums für Telekommunikation zu 40 Jahre Volkszählungsurteil des Bundesverfassungsgerichts“ und im Studiengang „Informationstechnologie und Recht“ der Universität des Saarlandes gehalten. Meine Mitarbeiter waren unter anderem vertreten beim BvD Verbandstag in Berlin, bei der Deutschen Compliance Konferenz 2023, beim BvD Herbstgespräch 2023 in München und beim Risc Kongress 2023 an der School of Finance in Frankfurt.

Darüber hinaus haben wir diverse Aufsätze in verschiedenen juristischen Fachzeitschriften und Beiträge in Gesetzeskommentaren veröffentlicht. Dazu zählen unter anderem:

Friedrichsen/Rapp: Aufsichtsrechtliche Maßnahmen gegenüber öffentlichen Stellen, ZD 2023, 535–543.

Rapp/Roßnagel/Franke: Datenschutz bei Wahl- und Abstimmungswerbung. ZD 2023, 247–251.

Roßnagel: 40 Jahre Volkszählungsurteil des Bundesverfassungsgerichts, JA 2023, 1363–1375.

Roßnagel: Videokonferenzen als Telekommunikationsdienste?, NJW 2023, 400–405.

Roßnagel: Digitale Souveränität im Datenschutzrecht. Voraussetzung für die Umsetzung daten-schutzrechtlicher Anforderungen, MMR 2023, 64–68.

Roßnagel: Kommentierung der §§ 175 bis 181 TKG, in: Geppert/Schütz (Hrsg.), Beck’scher Kommentar zum TKG, 5. Aufl. München 2023, 2071–2114.

Roßnagel/Richter: Commentary of Art. 5, 40 and 41 GDPR, in: Spiecker gen. Döhmann, /Papakonstantinou/Hornung/De Hert (Eds.), General Data Protection Regulation, Article-by-Article Commentary, 2023, 261-291, 736–756.

Roßnagel/Rost: Eine Geldbuße kommt selten allein, ZD 2023, 502.

Roßnagel/Wetzstein/Horlbeck, Unionsrechtliche Vorgaben für das Recht des Beschäftigtendatenschutzes – Auswirkungen des EuGH-Urteils vom 30.3.2023, DuD 2023, 429–434.

16. Arbeitsstatistik

16.1 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 2022	Fallzahlen 20232
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).	3.738	**3.520**
Beratungen Anzahl von schriftlichen Beratungen. Dies umfasst summarisch Beratungen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. **Nicht:** (Fern-)mündliche Beratungen, Schulungen, Vorträge etc.	1.334	**1.115**
Hinweise Anzahl der Hinweise auf Datenschutzverstöße, die nicht als Beschwerden im Sinne von Artikel 77 DS-GVO gewertet werden (etwa anonyme Hinweise und Hinweise von nicht selbst betroffenen Personen)		**593***
Abhilfemaßnahmen Anzahl der getroffenen Maßnahmen, die im Berichtszeitraum getroffen wurden.		
(1) nach Art. 58 Abs. 2 a (Warnungen)	1	**0**
(2) nach Art. 58 Abs. 2 b (Verwarnungen)	37	**31**
(3) nach Art. 58 Abs. 2 c–g und j (Anweisungen und Anordnungen)	16	**16**

(4) nach Art. 58 Abs. 2 i (Geldbußen)	113	**124**
(5) nach Art. 58 Abs. 2 h (Widerruf von Zertifizierungen)	0	**0**
Genehmigungsverfahren		
(1) BCR-Verfahren (Art. 58 Abs. 2j) mit deutscher oder europaweiter Federführung des HBDI	10	**14**
(2) Akkreditierungsverfahren (Art. 52 Abs. 2e) mit deutscher oder europaweiter Federführung des HBDI	–	**1**
Europäische Verfahren		
(1) Anzahl der Verfahren mit Betroffenheit (Art.56)	11	**13**
(2) Anzahl der Verfahren mit Federführung (Art. 56)	2	**4**
(3) Anzahl der Verfahren gemäß Kap. VII DS-GVO (Art. 60 ff.)	982	**1.062**
Begleitung bei Rechtsetzungsvorhaben		
Anzahl der Beratungen in Rechtssetzungsverfahren	35	**30**

* im Jahr 2023 erstmalig gesondert erfasst, bis 2022 als Beschwerden in der Statistik geführt

16.2
Ergänzende Erläuterungen zu Zahlen und Fakten

Die nachstehenden Darstellungen erläutern und ergänzen die Auswertungen in Kap. 16.1 auch im Vergleich mit dem Vorjahr und den weiteren Arbeitsgebieten im Berichtsjahr. Insgesamt hält sich die Zahl der Fälle, die dem HBDI zur Kenntnis gelangen, acht Jahre nach dem Inkrafttreten und sechs Jahre nach dem Wirksamwerden der DS-GVO auf einem sehr hohen Niveau. Dabei gilt weiterhin, dass sich in vielen Bereichen die Qualität der Beschwerden und des Beratungsbedarfes 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 auch in diesem Berichtsjahr zu befassen hatte, mehr in die Tiefe und werfen nach wie vor grundsätzliche Fragen auf.

Beschwerden und Beratungen

Die nachfolgende Übersicht stellt die Zahl der Eingabe (Beschwerden und Beratungen) des Berichtsjahres im Vergleich zum Vorjahr dar:

Fachgebiete	2022			2023			
	Beschwerden	Beratungen	Eingaben insgesamt	Beschwerden	Beratungen	Hinweise	**Eingaben insgesamt**
Auskunfteien, Inkasso	485	2	487	456	6	0	**462**
Schule, Hochschule, Archive	97	200	297	146	109	8	**263**
e-Kommunikation, Internet	436	63	499	289	36	98	**423**
Beschäftigtendatenschutz	280	151	431	267	136	16	**419**
Videobeobachtung	408	80	488	232	88	219	**539**
Kreditwirtschaft	306	5	311	441	4	7	**452**
Handel, Handwerk, Gewerbe	135	15	150	167	21	8	**196**
Verkehr, Geodaten, Landwirtschaft	288	22	310	318	16	55	**389**
Gesundheit, Pflege	222	107	329	160	81	48	**289**
Betriebliche/ Behördliche DSB	8	193	201	5	187	0	**192**
Kommunen, Wahlen	108	143	251	97	139	0	**236**
Polizei, Justiz, Verfassungsschutz	153	100	253	152	90	34	**276**
Vereine, Verbände	97	35	132	111	32	8	**151**
Adresshandel, Werbung	302	4	306	313	4	18	**335**
Wohnen, Miete	80	76	156	71	36	10	**117**
Soziales	63	31	94	72	38	4	**114**
Versorgungsunternehmen	71	13	84	60	8	25	**93**
IT-Sicherheit, DV-Technik*	18	2 Korr.: 47	20	7	45	20	**72**
Versicherungen	51	7	58	76	9	3	**88**
Rundfunk, Fernsehen, Presse	22	0	22	42	6	10	**58**
Religionsgemeinschaften	12	1	13	7	1	0	**8**
Forschung, Statistik	13	5	18	5	12	0	**17**

Ausländerrecht	2	7	9	5	4	0	**9**
Steuerwesen	18	4	22	18	3	0	**21**
Zensus	60	53	113	1	0	0	**1**
Sonstige Themen < 10 (z. B. Kammern, Ausländerwesen, Finanzwesen)	3	15	18	2	4	2	**8**
Zwischensumme Beschwerden und Beratungen	3.738	1.334	5.072	3.520	1.115	593	**5.228**
Meldungen von Datenpannen*			**1.754**				**1.934**

Gesamtsumme dokumentierter Eingaben	**6.836**	**7.162**
Zzgl. Summe telefonischer Beratungen und Auskünfte von mehr als 10 Min.**	**4.644**	**3.576**
Gesamtsumme dokumentierter + telefonischer Eingaben	**11.480**	**10.738**

*Weitere IT-Themen waren begleitend zu einer rechtlichen Anfrage oder einer Datenpannenmeldung zu prüfen und wurden deshalb nicht eigenständig gezählt.

**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.

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 **32** Auskunftsersuchen von Bürgerinnen und Bürgern zur Verarbeitung ihrer Daten beim HBDI bearbeitet sowie **10** 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 2023 **93** Presseanfragen. Zahlreiche Veröffentlichungen und Hilfestellungen wurden Verantwortlichen, Bürgern und Bürgerinnen auf meiner Homepage (z. B. zum Thema Videokonferenztechnik) zur Verfügung gestellt.

– **Ausbildungsleistungen**

  Es wurden **neun** Rechtsreferendare und -referendarinnen in ihren Wahl- bzw. Verwaltungsstationen ausgebildet. Das war die bislang höchste Zahl von Referendaren, die innerhalb eines Jahres in meiner Dienststelle ihre Verwaltungs- oder Wahlstation des Juristischen Vorbereitungsdienstes absolviert haben.

– **Fortbildung und Vorträge**

  Mitarbeitende meiner Behörde haben **37**, zum Teil mehrtägige, datenschutzrechtliche Schulungen, Seminare, Fortbildungen und Vorträge im öffentlichen und nichtöffentlichen Bereich durchgeführt. Ich selbst habe 20 Vorträge zu unterschiedlichsten Datenschutzfragen gehalten sowie 9 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. 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. Darüber hinaus fanden fünf Konferenzen der DSK und zwei Treffen, in denen sich die DSK mit den spezifischen Aufsichtsbehörden ausgetauscht hat, statt. Die Ergebnisse der DSK des Jahres 2023 sind in 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 meine Mitarbeiterinnen und Mitarbeiter. In den Arbeitskreisen Organisation und Struktur sowie Wissenschaft und Forschung führe ich den Vorsitz, 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) konnten sich meine Mitarbeiterinnen und Mitarbeiter einbringen, in der Visa Information System Supervision Coordination Group (VIS SCG) führe ich den Vorsitz. Daneben erfolgten auch Unterstützungsleistungen an die EU-Kommission, wie z. B. durch die Teilnahme als „lead expert“ an der Schengen-Evaluation in Estland

Abhilfemaßnahmen und Gerichtsverfahren

Abhilfemaßnahmen	2022	2023
(1) Warnungen (Art. 58 Abs. 2 a DS-GVO)	1	**0**
(2) Verwarnungen (Art. 58 Abs. 2 b DS-GVO)	37	**31**
(3) Anweisungen und Anordnungen (Art. 58 Abs. 2 c-g, j DS-GVO)	16	**16**
(4) Geldbußen (Art. 58 Abs. 2 i DS-GVO)	113	**124**
(5) Widerruf von Zertifizierungen (Art. 58 Abs. 2 h DS-GVO)	0	**0**
Gesamt	167	**171**

Gerichtsverfahren	2021	2022
Klagen gemäß Art. 78 Abs. 1 DS-GVO	13	**12**
Klagen gemäß Art. 78 Abs. 2 DS-GVO	4	**4**
Verfahren vor dem VGH in 2. Instanz		**6**
Verfahren vor dem Bundesverfassungsgericht		**3**
Eilverfahren		**1**
Sonstige	18*	1
Gesamt	35	**27**

* 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	**2022**	**2023**
Fehlversand/Fehlzuordnung von Daten/Dokumenten	661	**728**
Hackerangriffe, Phishing, Schadsoftware, Sicherheitslücke	475	**502**
Verlust/ Diebstahl von Unterlagen, Geräten etc.	135	**143**
Unrechtmäßige Offenlegung/Weitergabe von Daten	189	**209**
Unzulässige Einsichtnahme (fehlerhafte Einrichtung von Zugriffsrechten u. a.)	90	**117**
Offener E-Mail-Verteiler	85	**102**
Missbrauch von Zugriffsrechten	69	**79**
Unzulässige Veröffentlichung	22	**25**
Nicht datenschutzkonforme Entsorgung	2	**6**
Unverschlüsselter E-Mail-Versand	12	**17**
Sonstige	14	**6**
Gesamt	1.754	**1.934**

am stärksten von Datenschutzverletzungen betroffene Bereiche	2022	2023
Kreditwirtschaft, Auskunfteien, Handel und Gewerbe	533	**718**
Beschäftigtendatenschutz	367	**362**
Gesundheitsbereich	267	**299**

Anhang zu I

1. Ausgewählte Entschließungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

1.1
Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz! vom 11.05.2023

https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Beschaeftigtendatenschutz.pdf

1.2
Verfassungsrechtliche Anforderungen bei automatisierter Datenanalyse durch Polizei und Nachrichtendienste beachten! vom 11.05.2023

https://www.datenschutzkonferenz-online.de/media/en/2023-05-11_DSK-Entschliessung_Datenanalyse-Polizei.pdf

1.3
Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung! vom 17.10.2023

https://www.datenschutzkonferenz-online.de/media/en/20231017DSK EntschliessungChatkontrolle.pdf

1.4
Datenschutz in der Forschung durch einheitliche Maßstäbe stärken vom 23.11.2023

https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_DS.pdf

1.5
Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register vom 22./23.11.2023

https://www.datenschutzkonferenz-online.de/media/en/2023-11-23_DSK-Entschliessung_medRegister.pdf

2. Ausgewählte Beschlüsse der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder

2.1
Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten vom 03.02.2023

https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf

2.2
Bewertung von Pur-Abo-Modellen auf Websites vom 29.03.2023

https://www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf

2.3
Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten vom 27.09.2023

https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Positionspapier_audiovisuelle_Umgebungserfassung.pdf

2.4
Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen vom 06.11.2023

https://www.datenschutzkonferenz-online.de/media/dskb/2023_11_06_Beschluss_cloudbasierte_digitale_Gesundheitsanwendungen.pdf

II
Zweiter Teil
6. Tätigkeitsbericht zur Informationsfreiheit

1. Einführung Informationsfreiheit

Der vorliegende sechste Tätigkeitsbericht zur Informationsfreiheit beschreibt und analysiert die Informationsfreiheit in Hessen im Jahr 6 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 die Wahrung schützenswerter Geheimnisse. Vom Informationsanspruch betroffene Dritte 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 zur Wahl stehenden Leiter der öffentlichen Verwaltung nachzuvollziehen und zu bewerten. Sie sollen zum anderen über die Wissensgrundlagen und Handlungsmöglichkeiten der Verwaltung informiert werden und 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 und stärkt die bürgerschaftliche Partizipation und die Kontrolle staatlichen Handelns.

Die Bundesrepublik Deutschland und 14 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 sechs Jahren Regelungen zur Umsetzung der Informationsfreiheit erlassen. Hierfür hat Hessen 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 weiterentwickeln.

Inzwischen zeigt sich jedoch, dass die Daten, über die öffentliche Stellen verfügen, nicht nur für Demokratie und Rechtsstaat von großer Bedeutung sind, sondern dass 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. In Hessen hat sich der Landtag diesen Entwicklungen angeschlossen und ein Open-Data-Gesetz beschlossen, das am 24. März 2023 in Kraft getreten ist (Kap. 2).

Wie die Regelungen zur Informationsfreiheit gelten die Regelungen des Open-Data-Gesetzes unmittelbar für die Landesverwaltung. Für Gemeinden, Gemeindeverbände und Landkreise gelten die Verpflichtungen für die Bereitstellung von offenen Daten nicht. Ihnen steht es frei, ob sie offene Daten bereitstellen. Soweit die Daten in Auftragsangelegenheiten erhoben worden sind, ist für ihre Bereitstellung das Einvernehmen der zuständigen Aufsichtsbehörde erforderlich.

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 sechste Tätigkeitsbericht eine kleine Auswahl. Er stellt das neue Hessische Open-Data-Gesetz vor (Kap. 2), untersucht am Beispiel einer Anfrage des Hessischen Ministeriums für Soziales und Integration (HMSI) die Frage, wie Informationsfreiheit und Datenschutz zusammenhängen (Kap. 3), erläutert die Beschränkung der Informationsfreiheit bei rein wirtschaftlichen Interessen und plädiert dafür, diese aufzuheben (Kap. 4), und vergleicht die Kostenregelungen für die Zulassung von Informationsfreiheitsanträgen im Bund, in anderen Bundesländern und in Hessen (Kap. 5).

2. Das Hessische Open-Data-Gesetz

Am 24. März 2023 ist das Hessische Gesetz über offene Daten der Träger der öffentlichen Verwaltung (HODaG) in Kraft getreten.

Bereits im Jahr 2021 hatte die FDP-Fraktion des Hessischen Landtags vorgeschlagen, die Pflicht zur Veröffentlichung von sogenannten „offenen Daten“ (Open Data) in Hessen zu etablieren (s. 50. TB 2021, 2. Teil Kap. 5). Dieser Gesetzentwurf war damals abgelehnt worden. Stattdessen sollte eine Änderung des Hessischen E-Government-Gesetzes die Bereitstellung von offenen Daten durch hessische öffentliche Stellen verpflichtend regeln. Das nun verabschiedete und in Kraft getretene Gesetz – auf der Grundlage eines Entwurfs der Fraktionen von CDU und Bündnis 90/Die Grünen – geht weit über den damaligen Gesetzentwurf hinaus. Damit wurde ein eigenes Gesetz geschaffen, das Hessische Open Data-Gesetz (HODaG). Ich wurde im Rahmen des Gesetzgebungsverfahrens frühzeitig eingebunden und angehört. Im Folgenden werde ich auf einzelne Regelungen des HODaG aus dem Blickwinkel des Datenschutzes und der Informationsfreiheit eingehen und auch darstellen, in welchen Punkten ich Änderungen des Gesetzentwurfs angeregt habe.

2.1 Was sind offene Daten?

Eine Definition des Begriffs „Open Data“ und der Zweck der Bereitstellung von Open Data findet sich in Erwägungsgrund (ErwG) 16 zur Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (Open Data-Richtlinie).[118] Danach sind „offene Daten“ (Open Data) entsprechend dem allgemeinen Verständnis Daten in einem offenen Format, die von allen zu jedem Zweck frei verwendet, weiterverwendet und weitergegeben werden können. Die grundsätzliche Verpflichtung der Behörden des Landes zur Bereitstellung offener Daten ist in § 1 Abs. 1 Satz 1 HODaG normiert. § 1 Abs. 1 Satz 3 HODaG stellt klar, von wem und in welcher Form die offenen Daten genutzt werden können.

118 EU-Amtsblatt 172, S. 56; s. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019L1024.

§ 1 Abs. 1 Satz 1 und 3 HODaG

(1) Die Behörden des Landes sollen maschinenlesbare unbearbeitete Daten, die sie selbst zur Erfüllung ihrer Aufgaben erhoben haben oder durch Dritte in ihrem Auftrag haben erheben lassen (offene Daten), zum Abruf über öffentlich zugängliche Netze bereitstellen. (…) Bereitgestellte offene Daten können durch jede Person im Rahmen der Rechtsordnung genutzt, weiterverbreitet und weiterverwendet werden.

Allerdings ist zu beachten, dass die Möglichkeit des Zugangs zu Open Data keinen Zugang zu personenbezogenen Daten eröffnen soll. Soweit personenbezogene Daten in den bereitgestellten Daten enthalten sind, müssen Verantwortliche und Auftragsverarbeiter sicherstellen, dass diese vor der Bereitstellung anonymisiert werden und dass auch unter Zuhilfenahme von Zusatzwissen keine Re-Identifikation betroffener Personen erfolgen kann.

2.2 Geltungsbereich

Das Hessische Open Data-Gesetz gilt grundsätzlich für alle öffentlichen Stellen in der Hessischen Landesverwaltung.

Definition

Der Geltungsbereich des Gesetzes wird in § 1 Abs. 3 und 4 HODaG genauer definiert.

§ 1 Abs. 3 und Abs. 4 HODaG

(3) Abs. 1 Satz 1 und 2 gilt nur für unbearbeitete Daten, die

1. *einer Behörde elektronisch gespeichert und in Sammlungen strukturiert vorliegen, insbesondere in Form von Tabellen, Listen oder Datenbanken,*
2. *ausschließlich Tatsachen enthalten, die außerhalb der Behörde liegende Verhältnisse betreffen und*
3. *nicht personenbezogen oder nach einer erfolgten vollständigen Anonymisierung nicht mehr personenbezogen sind.*

(4) Abs. 1 Satz 1 und 2 gilt nicht für unbearbeitete Daten, die

1. *die Wettbewerbsfähigkeit öffentlicher Unternehmen sicherstellen, geistiges Eigentum Dritter betreffen oder Geschäftsgeheimnisse einschließlich Betriebs-, Berufs- und Unternehmensgeheimnisse beinhalten;*
2. *aufgrund eines übergeordneten öffentlichen Interesses an der Geheimhaltung oder ihrer Eigenschaft als vertrauliche Informationen über den Schutz kritischer Infrastrukturen nicht oder nur eingeschränkt zugänglich sind;*

3. *im Fall ihrer Bereitstellung nachteilige Auswirkungen auf die Belange der äußeren Sicherheit, die inter- und supranationalen Beziehungen, die Beziehungen zum Bund oder zu einem anderen Land, die öffentliche Sicherheit und Ordnung oder behördliche Entscheidungsprozesse haben können;*
4. *Forschungsdaten betreffen, soweit die Bereitstellung eine Beeinträchtigung der Grundrechte nach Art. 5 Abs. 3 Satz 1 des Grundgesetzes für die Bundesrepublik Deutschland darstellen würde oder durch öffentlich-rechtliche Rundfunkanstalten oder deren Beauftragte verarbeitet werden und unmittelbar der Wahrnehmung der Grundrechte nach Art. 5 Abs. 1 Satz 2 des Grundgesetzes für die Bundesrepublik Deutschland dienen oder durch kulturelle Einrichtungen mit Ausnahme von Bibliotheken, Museen oder Archiven verarbeitet werden;*
5. *aufgrund einer gesetzlichen Regelung nicht, nur eingeschränkt oder erst nach Beteiligung Dritter zugänglich sind, insbesondere in Fällen, in denen ein rechtliches oder berechtigtes Interesse nachzuweisen ist, um Zugang zu den Informationen zu erhalten oder für die eine ausschließliche Veröffentlichung über einen spezifischen Kanal vorgegeben ist;*
6. *über öffentlich zugängliche Netze bereits maschinenlesbar und entgeltfrei zur Verfügung stehen;*
7. *von öffentlichen Stellen des Bundes, eines anderen Landes oder der Gemeinden, Gemeindeverbände und Landkreise zur Erfüllung ihrer Aufgaben erhoben oder erstellt wurden und bei einer Behörde des Landes vorhanden sind.*

Bei der Anonymisierung gem. Abs. 3 Nr. 3 ist darauf zu achten, dass eine De-Anonymisierung auch unter Zuhilfenahme von technischen Mitteln nicht erfolgen kann.

Ausnahmen für Gemeinden, Gemeindeverbände und Landkreise

In § 1 Abs. 1 Satz 2 HODaG ist klargestellt, dass für Gemeinden, Gemeindeverbände und Landkreise die Verpflichtung für die Bereitstellung von offenen Daten nicht gelten soll.

§ 1 Abs. 1 Satz 2 HODaG

(…)

Gemeinden, Gemeindeverbände und Landkreise können offene Daten bereitstellen, soweit sie zur Erfüllung von Aufgaben ihres eigenen Wirkungskreises oder in Auftragsangelegenheiten erhoben wurden; im Falle der Datenerhebung in Auftragsangelegenheiten ist für die Bereitstellung das Einvernehmen der zuständigen Aufsichtsbehörde erforderlich. (…)

Die Ausnahmeregelung korrespondiert mit der Ausnahmeregelung in § 81 Abs. 1 Nr. 7 HDSIG, nach der Gemeinden, Gemeindeverbände und Landkreise nur verpflichtet sind, einen Informationszugangs zu eröffnen, wenn sie dies selbst durch Satzung so festgelegt haben. Diese Regelung bringt

dem Land Hessen bundesweit große Kritik ein und hat dafür gesorgt, dass das Land beim bundesweiten Transparenzranking auf dem drittletzten Platz landete, wobei die beiden letzten Plätze von Bundesländern belegt werden, die keinen Anspruch auf Informationsfreiheit rechtlich verankert haben.[119] Sinnvoll erscheint allerdings die Regelung, dass für das Bereitstellen von offenen Daten in Auftragsangelegenheiten das Einvernehmen der zuständigen Aufsichtsbehörde erforderlich ist. So kann das Risiko der Weitergabe von sensitiven Daten zusätzlich eingedämmt werden.

2.3
Begriffsbestimmungen

Die im HODaG verwendeten Begriffe sind in § 2 HODaG definiert.

§ 2 HODaG

Im Sinne dieses Gesetzes

1. *sind „Daten" vorhandene Aufzeichnungen, unabhängig von der Art ihrer Speicherung;*
2. *sind Daten „unbearbeitet", wenn und solange sie nicht interpretiert, bewertet oder in sonstiger Weise bearbeitet sind; nicht als Bearbeitung gelten insbesondere eine Anonymisierung nach Nr. 8, eine Aufbereitung im Rahmen des gesetzlichen Auftrags der Behörde einschließlich einer erforderlichen Plausibilitätsprüfung und eine Aufbereitung zur Erfüllung der Standards der Bereitstellung nach § 4;*
3. *sind Daten „maschinenlesbar", wenn sie durch Software automatisiert ausgelesen und verarbeitet werden können;*
4. *ist „Nutzung" jede Verwendung von Daten für kommerzielle oder nichtkommerzielle Zwecke, die über die Erfüllung einer öffentlichen Aufgabe oder die Erbringung von Dienstleistungen von allgemeinem Interesse hinausgeht oder die neben der Erfüllung öffentlicher Aufgaben auch zu eigenen Zwecken erfolgt;*
5. *sind „dynamische Daten" Daten in digitaler Form, die häufig oder in Echtzeit aktualisiert werden, insbesondere aufgrund ihrer Volatilität oder ihres raschen Veraltens;*
6. *sind „Metadaten" Daten, die offene Daten beschreiben und es ermöglichen, diese zu ermitteln, in Verzeichnisse aufzunehmen und zu nutzen;*
7. *sind „Forschungsdaten" Daten, die zu Forschungszwecken erhoben wurden;*
8. *ist „Anonymisierung" von Daten ein Prozess, durch den personenbezogene Daten in einer Weise geschützt werden, dass die betroffene Person nicht oder nicht mehr identifiziert werden. Eine natürliche Person ist identifizierbar, wenn sie unter Berücksichtigung aller Mittel, die von der verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die Identität der natürlichen Person direkt oder indirekt zu ermitteln, identifiziert werden kann. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, insbesondere die Kosten der*

119 https://transparenzranking.de/.

Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

§ 1 Abs. 1 Satz 1 HODaG bestimmt, dass „unbearbeitete Daten" bereitgestellt werden sollen. In § 1 Abs. 3 Nr. 3 HODaG wird ferner klargestellt, dass eine Veröffentlichung gemäß § 1 Abs. 1 HODaG nur für nicht personenbezogene oder wirksam anonymisierte, unbearbeitete Daten zulässig ist. Außerdem legt § 4 Abs. 1 Satz 1 fest, dass die Bereitstellung offener Daten „in elektronischer Form in offenen, maschinenlesbaren und interoperablen Formaten auf dem Stand der Technik" erfolgt. Sofern die unbearbeiteten Daten nicht in einem solchen Format vorliegen, wäre vor der Veröffentlichung eine Überführung in ein den Anforderungen entsprechendes Format erforderlich.

Sowohl eine Anonymisierung als auch eine Überführung in ein den Anforderungen entsprechendes Format stellt jedoch eine Bearbeitung personenbezogener Daten dar. Die Begriffsbestimmung in § 2 Nr. 2 HODaG wurde auf meinen Vorschlag dahingehend ergänzt, dass eine Aufbereitung und Anonymisierung von unbearbeiteten Daten zur Erfüllung der Anforderungen des HODaG zulässig ist.

In § 2 Nr. 8 HODaG wird der Begriff „Anonymisierung" bestimmt. In § 2 Abs. 4 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) ist der Begriff bereits definiert, wobei auch auf Aspekte der Identifizierbarkeit eingegangen wird. Um Abweichungen zu vermeiden, habe ich im Rahmen des Gesetzgebungsverfahrens darauf hingewirkt, dass hier die Definition des § 2 Abs. 4 HDSIG verwendet wird.

2.4
Anforderungen und Ansprüche

Das Hessische Open Data-Gesetz enthält vor allem Anforderungen an die verpflichteten öffentlichen Stellen. Diesen entsprechen Ansprüche der an offenen Daten Interessierten.

Metadatenportal

§ 3 Abs. 1 Satz 2 HODaG sieht vor, dass ein Metadatenportal einen zentralen Zugriff zu den offenen Daten ermöglicht. Der Zugang ist vom Zugriff zu unterscheiden. Bei dem Begriff „Zugang" handelt es sich um einen bereits

vorbelegten Begriff aus dem Identitäts- und Berechtigungsmanagement.[120] Während der Begriff „Zugang“ die Nutzung von IT-Systemen, System-Komponenten und Netzen bezeichnet, adressiert der Begriff „Zugriff“ die Nutzung von Informationen oder Daten. Hier habe ich die Verwendung des korrekten Begriffs angeregt, was vom Gesetzgeber auch umgesetzt wurde.

Standards der Bereitstellung, Verfahren der Veröffentlichung

Die Standards der Bereitstellung und das Verfahren der Veröffentlichung sind in § 4 HODaG geregelt.

§ 4 HODaG

(1) Die Bereitstellung offener Daten nach § 1 Abs. 1 erfolgt in elektronischer Form in offenen, maschinenlesbaren und interoperablen Formaten auf dem Stand der Technik. Unbearbeitete Daten sollen vollständig und zusammen mit den zugehörigen Metadaten bereitgestellt werden. Die zugehörigen Metadaten sind in dem Metadatenportal gemäß § 1 Abs. 1 zu veröffentlichen.

(2) Bei der Erhebung dynamischer Daten sollen sich am Zweck der Datenerhebung orientierende Zwischenstände auch als Massendownload bereitgestellt werden. Abs. 1 gilt hierfür entsprechend. Bei einer erfolgten Anonymisierung von Daten mit dem Ziel, deren Personenbezug auszuschließen, ist eine Datenschutzfolgeabschätzung durchzuführen.

(3) Vor einer Bereitstellung über öffentlich zugängliche Netze ist durch die Behörde die rechtliche Zulässigkeit der Bereitstellung sicherzustellen. Insbesondere sind die Belange des Datenschutzes und Rechte Dritter zu beachten. Veröffentlichte Daten sollen dauerhaft bereitgestellt werden. Bereitgestellte Daten einschließlich der zugehörigen Metadaten sind mit einer zur Nutzung berechtigenden Lizenz zu versehen. Die Lizenz ist so zu wählen, dass die bereitgestellten Daten frei und uneingeschränkt genutzt werden können.

(4) Verantwortlich für die Einhaltung der Standards nach Abs. 1 bis 3 ist die Behörde, die für die Erhebung der unbearbeiteten Daten zuständig ist und diese Daten erstmalig erhebt oder erheben lässt. Werden die Daten von einer anderen öffentlichen Stelle, von Beliehenen oder von Dritten aufgrund einer gesetzlichen oder rechtlichen Verpflichtung an eine Behörde übermittelt, soll die empfangende Behörde diese Standards festlegen.

(5) Die Behörden des Landes berücksichtigen frühzeitig die Einhaltung der Standards nach Abs. 1 bis 4, insbesondere bei der Optimierung von Verwaltungsabläufen, dem Abschluss von Verträgen zur Erhebung oder Verarbeitung der Daten sowie der Festlegung von Anforderungen an IT-Systeme und der Beschaffung von IT-Systemen.

120 Bundesamt für Sicherheit in der Informationstechnik (BSI), Umsetzungshinweise zum Baustein: ORP.4. Identitäts- und Berechtigungsmanagement, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf.

Der Schutz der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung von personenbezogenen Daten ist eines meiner zentralen Anliegen. Daher befürworte ich die explizite Benennung der Beachtung von Belangen des Datenschutzes in § 3 Abs. 3 Satz 1 HODaG ausdrücklich.

Ansprüche, Verantwortlichkeit, Haftung

Der Anspruch auf Bereitstellung offener Daten, die Verantwortlichkeit und die Haftung sind in § 5 HOdAG geregelt.

§ 5 HODaG

(1) Werden offene Daten bereitgestellt, ist der Abruf durch Nutzende jederzeit und ohne eine gesonderte Registrierung, die Darlegung eines besonderen Interesses oder mengenmäßige Beschränkungen zu gewährleisten. Ein Anspruch auf die Bereitstellung, die Einrichtung von besonderen Schnittstellen oder anderen technischen Zugangsformen sowie auf bestimmte zeitliche oder mengenmäßige Bereitstellungen von Daten besteht nicht.

(2) Behörden sind nicht verpflichtet, die bereitgestellten Daten über das zur Erfüllung ihres gesetzlichen Auftrags erforderliche Maß hinaus auf Richtigkeit, Vollständigkeit, Plausibilität, Aktualität oder in sonstiger Weise zu prüfen.

(3) Der Abruf und die Nutzung von offenen Daten erfolgt in eigener Verantwortung der Nutzenden. Eine Haftung der Träger der öffentlichen Verwaltung aufgrund dieses Gesetzes oder für Schäden, die durch die Weiterverwendung oder Nutzung von aufgrund dieses Gesetzes bereitgestellten unbearbeiteten Daten verursacht werden, ist ausgeschlossen. Dies gilt insbesondere für die nach Abs. 2 geltende beschränkte Prüfpflicht.

Nach § 5 Abs. 1 HODaG sind Behörden nicht verpflichtet, die bereitgestellten Daten über das zur Erfüllung ihres gesetzlichen Auftrags erforderliche Maß hinaus auf Richtigkeit, Vollständigkeit, Plausibilität, Aktualität oder in sonstiger Weise zu prüfen. Aus meiner Sicht könnte diese Regelung einer größtmöglichen Transparenz entgegenstehen. Ich vertrete die Auffassung, dass bei Anträgen auf Informationszugang den antragstellenden Personen, soweit möglich, ein Kontext gegeben werden sollte, um die erhaltenen Informationen einordnen und verstehen zu können. Diese Verpflichtung würde bei der Bereitstellung von offenen Daten zwar zu weit gehen, jedoch sollte zumindest die größtmögliche Sorgfalt bei der Bereitstellung von offenen Daten angewendet und offenkundig unrichtige Daten verpflichtend korrigiert werden.

Der Abruf offener Daten durch Nutzende ist nach § 5 Abs. 1 Satz 1 HODaG „jederzeit“ zu gewährleisten. Daraus ergeben sich entsprechende Verfügbarkeitsansprüche der Nutzenden gegenüber der technischen Lösung des unter § 3 HODaG definierten Medienportals. In § 5 Abs. 1 Satz 2 HODaG

sind jedoch Einschränkungen genannt, die die zeitliche Bereitstellung von Daten ausschließt.

Zeitpunkt der Bereitstellung, Übergangsregelung

Grundsätzlich bestimmt sich der Zeitpunkt der Bereitstellung nach § 1 Abs. 5 HODaG, wonach die Unverzüglichkeit das maßgebliche Kriterium ist.

§ 1 Abs. 5 HODaG

(5) Die Bereitstellung von Daten nach Abs. 1 Satz 1 soll erfolgen:

1. *soweit fachlich eine Überprüfung der Plausibilität der Daten erforderlich ist, unverzüglich nach der Plausibilitätsprüfung,*
2. *soweit der Zweck der Erhebung der Daten durch die Bereitstellung beeinträchtigt wird, unverzüglich nach dem Wegfall der Beeinträchtigung,*
3. *soweit aus technischen oder sonstigen gewichtigen Gründen eine Bereitstellung nicht möglich ist, unverzüglich nach Wegfall der Hinderungsgründe,*
4. *im Übrigen unverzüglich nach der Erhebung.*

Nach § 8 Abs. 1 Satz 1 HODaG kann die Bereitstellung offener Daten, die nach dem Inkrafttreten des HODaG und vor Ablauf des zweiten auf das Inkrafttreten des Gesetzes folgenden Jahres erhoben wurden, in Abweichung davon spätestens bis zum Ablauf des dritten auf das Inkrafttreten des Gesetzes folgenden Jahres erfolgen. Eine weitere abweichende Übergangsregelung findet sich in § 8 Abs. 1 Satz 2 HODaG. Diese gilt dann, wenn die Bereitstellung erhebliche technische Anpassungen erfordert und sie deshalb innerhalb des vorgenannten Zeitraums nur mit unverhältnismäßig hohem Aufwand möglich ist. In dem Fall kann die Bereitstellung spätestens bis zum Ablauf des vierten auf das Inkrafttreten des HODaG folgenden Jahres erfolgen.

2.5
Fazit

Grundsätzlich begrüße ich die Verpflichtung der Behörden des Landes zur Bereitstellung von offenen Daten. Dies fördert die erstrebenswerte Transparenz der öffentlichen Hand als Ausdruck des Demokratieprinzips. Außerdem ist die Bereitstellung von offenen Daten auch unter wirtschaftlichen Gesichtspunkten gerade für kleine und mittelständische Unternehmen von Bedeutung.

3. Datenschutz als eine Determinante der Informationsfreiheit

In Hessen erfährt der Datenschutz durch die Informationsfreiheit keine Einbuße. Das hessische Datenschutzrecht prägt nämlich das hessische Informationsfreiheitsrecht mit.

Das Hessische Ministerium für Soziales und Integration (HMSI) fragte infolge eines an ihn gerichteten Informationsfreiheitsantrages bei mir an, ob und inwieweit die in der Angelegenheit vom Antragsteller begehrte Übermittlung personenbezogener Daten Dritter die Beteiligung oder die Einwilligung der betroffenen Personen voraussetzt. Darüber hinaus stellten sich datenschutzrechtliche Verfahrensfragen im Informationsfreiheitsrecht.

Das hessische Informationsfreiheitsrecht wurde gezielt so konzipiert, dass das hessische Datenschutzniveau keine Einbuße erfährt. Diese Rechtslage kommt in § 83 HDSIG prägnant zum Ausdruck, der den normativen Maßstab für die Zulässigkeit der Übermittlung personenbezogener Daten durch öffentliche Stellen an antragstellende Personen auf dem Gebiet der Informationsfreiheit festlegt.

§ 83 HDSIG

Der Informationszugang zu personenbezogenen Daten ist nur dann und soweit zulässig, wie ihre Übermittlung an eine nicht öffentliche Stelle zulässig ist.

Infolge dieser Regelung wird der datenschutzrechtliche § 22 Abs. 2 HDSIG zum rechtlichen Maßstab für die Übermittlung personenbezogener Daten infolge eines Antrages auf Informationszugang.

§ 22 Abs. 2 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 öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden.

In der Praxis ist vor allem § 22 Abs. 2 Nr. 2 HDSIG von Bedeutung, der eine Interessenabwägung in der Angelegenheit verlangt. Damit eine Interessenabwägung möglichst auf solider Tatsachengrundlage stattfindet, ist der Antragsteller gemäß § 85 Abs. 3 HDSIG gegenüber der öffentlichen Stelle im Fall von Drittbetroffenheit verpflichtet, seinen Antrag zu begründen, und die Stelle muss gemäß § 86 HDSIG der Person, um deren Daten es geht, die Möglichkeit zur Stellungnahme geben, wenn Anhaltspunkte dafür vorliegen, dass sie ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann.

Dem mit einem solchen Verfahren erhöhten Zeitaufwand trägt § 87 Abs. 1 HDSIG dadurch Rechnung, dass die Bescheidungsfrist für die öffentliche Stelle um zwei Monate verlängert wird (drei Monate statt nur ein Monat). In den Fällen des § 86 HDSIG (also bei Drittbetroffenheit) ist gemäß § 87 Abs. 1 Satz 2 HDSIG die Entscheidung auch dem Dritten bekannt zu geben. Der Informationszugang darf erst gewährt werden, wenn die Entscheidung dem Dritten gegenüber auch bestandskräftig geworden ist oder die, so der Wortlaut des § 87 Abs. 2 Satz 2 HDSIG, sofortige „Vollstreckung“ (richtig: „Vollziehung“ entsprechend § 80 Abs. 2 Nr. 4 VwGO) angeordnet wurde und seit der Bekanntgabe der Anordnung an den Dritten zwei Wochen verstrichen sind.

Diese Regelungen werden durch weitere Vorschriften ergänzt, die den Datenschutz auf dem Gebiet der Informationsfreiheit zusätzlich optimieren, nämlich soweit mit Blick auf die von antragstellenden Personen begehrten personenbezogener Daten eines Dritten (sogar) dessen zum persönlichen Lebensbereich gehörende Geheimnisse betroffen sind. In diesem Fall gibt es gemäß § 82 Nr. 4 HDSIG einen Einwilligungsvorbehalt.

§ 82 Nr. 4 HDSIG

Ein Anspruch auf Informationszugang besteht nicht

(…)

4. bei zum persönlichen Lebensbereich gehörenden Geheimnissen oder Betriebs- oder Geschäftsgeheimnissen, sofern die betroffene Person nicht eingewilligt hat oder

(…)

Diese Regelung komplettierend, legt § 86 Satz 2 HDSIG fest, dass die Einwilligung des Dritten zum Informationszugang der antragstellenden Person als verweigert gilt, wenn sie nicht innerhalb eines Monats nach Anfrage durch die zuständige Stelle vorliegt.

Die beschriebene Rechtslage habe ich mit dem Ministerium für Soziales und Integration erörtert.

Zusammenfassend kann festgehalten werden, dass der Datenschutz nicht der Informationsfreiheit entgegensteht, sondern sie durch die im HDSIG gefundenen Verfahrens- und Abwägungsregeln erst ermöglicht.

4. Rein wirtschaftliche Interessen im Informationsfreiheitsrecht

Soweit ein Informationszugangsantrag (ausschließlich) wirtschaftlichen Interessen der antragstellenden Person dient, besteht kein Anspruch auf Information. Falls es etwa um die Geltendmachung von Schadensersatzansprüchen gegenüber Dritten geht, ist die öffentliche Stelle jedoch datenschutzrechtlich befugt, personenbezogene Daten des Dritten an die antragstellende Person zu übermitteln. Die informationsrechtliche Regelung ist gleichwohl – jedenfalls mittlerweile – überprüfungsbedürftig.

Die maßgebende Regelung des § 82 Nr. 5 HDSIG

Im Rahmen meiner Beratungspraxis ist in den vergangenen Jahren mehrfach thematisiert worden, inwieweit rein wirtschaftliche Interessen den Informationszugang ausschließen können.

Dieses Thema stellt sich – anders als in den Informationsfreiheits- oder Transparenzgesetzen von Bund und Ländern – deshalb, weil Hessen den Anspruch auf Informationszugang in § 82 Nr. 5 HDSIG gesetzlich negiert, soweit ein rein wirtschaftliches Interesse an den Informationen besteht.

> *§ 82 Nr. 5 HDSIG*
> *Ein Anspruch auf Informationszugang besteht nicht*
> *(…)*
> *5. soweit ein rein wirtschaftliches Interesse an den Informationen besteht.*

§ 82 HDSIG befasst sich also laut seiner amtlichen Überschrift mit dem „Schutz besonderer öffentlicher und privater Belange“, und diesem Aspekt entsprechen die in § 82 Nr. 1 bis 4 HDSIG getroffenen Regelungen durchaus. Mit Blick auf die anschließende Regelung, dass rein wirtschaftliche Interessen dem Informationszugang entgegenstehen, kann man diesen Sachzusammenhang freilich nicht behaupten. Insoweit ist der in § 82 Nr. 5 HDSIG gesetzlich verfügte Informationsausschluss gesetzessystematisch merkwürdig platziert.

Klärung rein wirtschaftlicher Interessen

Gibt es hierfür, also für rein wirtschaftliche Interessen, Anhaltspunkte, ist die um Informationen ersuchte öffentliche Stelle nicht schon unter Hinweis auf den verwaltungsverfahrensrechtlichen Untersuchungsgrundsatz nach § 24

HVwVfG befugt, weitere personenbezogene Daten zur Antragstellerin oder zum Antragsteller zwecks Aufklärung des Sachverhalts, ob rein wirtschaftlich Interessen vorliegen, zu erheben. Denn soweit es um die Ermittlung des Sachverhalts geht, wird der Untersuchungsgrundsatz im Fall der Verarbeitung personenbezogener Daten nach § 1 Abs. 3 HDSIG vom Datenschutzrecht derogiert.

§ 1 Abs. 3 HDSIG

(3) Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

Rechtsgrundlage für die Erhebung notwendiger Informationen mit Personenbezug zwecks Verifizierung, ob rein wirtschaftliche Interessen vorliegen, ist demzufolge § 3 Abs. 1 HDSIG.

§ 3 Abs. 1 HDSIG

(1) Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie für die Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

Da bei der Klärung, ob rein wirtschaftliche Interessen vorliegen, auch keine sensiblen Daten im Sinne des Datenschutzrechtes erhoben zu werden brauchen, wird diese Generalbefugnis des § 3 Abs. 1 HDSIG auch nicht durch den die Verarbeitung besonderer Kategorien personenbezogener Daten betreffenden § 20 HDSIG ergänzt oder verdrängt.

Beispiele

Rein wirtschaftliche Interessen im Sinne von § 82 Nr. 5 HDSIG liegen etwa vor, wenn die Antragstellerin oder der Antragsteller mittels Informationszugang einen Amtshaftungsprozess vorbereiten möchte oder wenn die Informationen dazu dienen sollen, etwa die Abgabenlast gegenüber einer öffentlichen Stelle zu senken.

Es besteht auch kein Anspruch auf Informationen, wenn diese nur den Zweck haben, etwa einen Schadensersatzanspruch gegenüber einer anderen Person substanziieren zu können. In diesem Fall ist die öffentliche Stelle aber, ohne dass ein Informationszugangsanspruch besteht (also außerhalb des

Informationsfreiheitsrechts), datenschutzrechtlich befugt, auf der Grundlage einer pflichtgemäßen Ermessensausübung Daten der Person, gegenüber der ein Schadensersatzanspruch geltend gemacht wird oder werden soll, nach Maßgabe von § 22 Abs. 2 Nr. 3 HDSIG an die Antragstellerin oder den Antragsteller zu übermitteln.

§ 22 Abs. 2 Nr. 3 HDSIG

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

(…)

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.

(…)

Auf die skizzierte Rechtslage habe ich aus Anlass von Anfragen hingewiesen.

§ 82 Nr. 5 HDSIG – mittlerweile ein rechtliches Kuriosum?

Gegen die Vorschrift des § 82 Nr. 5 HDSIG sprechen mehrere Gründe.

Zum einen ist diese Regelung wirtschaftlicher Interessen, die einem Anspruch auf Informationsfreiheit entgegenstehen sollen, in § 82 HDSIG – der laut der amtlichen Überschrift dem „Schutz besonderer öffentlicher und privater Belange“ dient – rechtssystematisch unpassend platziert.

Zum anderen entsteht ein Wertungswiderspruch, weil nicht nur das Datenschutzrecht die Verfolgung wirtschaftlicher Interessen (als Hauptanwendungsfall „berechtigter Interessen“) durchaus anerkennt, wie sich z. B. aus Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO und § 22 Abs. 2 Nr. 2 HDSIG ergibt.

Schließlich wird in dem mittlerweile in Kraft getretenen Hessische Open Data-Gesetz ausdrücklich auch die Förderung wirtschaftlicher Interessen als Gesetzeszweck angeführt: „Für die Wirtschaft, insbesondere für kleinere und mittlere Unternehmen (KMU) und Startups, bieten offene maschinenlesbare Daten große Potenziale für wirtschaftliche Geschäftsmodelle … Die Bereitstellung der Daten der Behörden des Landes soll derart gestaltet werden, dass der größtmögliche Nutzen einerseits für Wirtschaft … entsteht.“[121]

Es wirkt widersprüchlich, dass das hessische gesetzliche Open-Data-Projekt wirtschaftliche Interessen per proaktiver Informationsbereitstellung einerseits

121 LT-Drucks. 20/10379, S. 8.

explizit fördern möchte, jedoch das reaktive (also nach § 85 HDSIG auf Antrag hin) gesetzliche hessische Informationsfreiheitsrecht die Wahrnehmung wirtschaftlicher Interessen weiterhin ausdrücklich exkludiert. Und dass Hessen auch das einzige Bundesland ist, dessen Informationsfreiheitsrecht eine solche, wirtschaftlichen Interessen entgegentretende Regelung aufweist, rundet den Eindruck einer überdenkenswerten hessischen Rechtslage im Informationsfreiheitsrecht ab.

Vor diesem Hintergrund bitte ich den Hessischen Landtag und die Hessische Landesregierung, diese informationsfreiheitsrechtliche Regelung in § 82 Nr. 5 HDSIG zu überprüfen.

5. Dürfen amtliche Informationen etwas kosten?

Die hessischen Regelungen für die Erhebung von Gebühren und Auslagen für Informationsfreiheitsanträge tragen den Belangen der Beteiligten Rechnung und bedürfen keiner Reform.

Dem Hessischen Landtag war im Berichtszeitraum eine Petition zugegangen, wonach die Bereitstellung von Informationen nach dem Vierten Teil des HDSIG stets kostenfrei sein solle. Als Begründung für die Petition wurde angegeben, dass das HDSIG den Bürgerinnen und Bürgern ermöglichen soll, Zugang zu amtlichen Informationen zu erhalten sowie das Handeln von Behörden zu prüfen. Der Petent machte geltend, dass dies vielen Bürgerinnen und Bürgern aufgrund der teilweise sehr hohen Gebührenbemessung nicht möglich sei. Mit der Anpassung des Gesetzes solle es jeder Person möglich sein, die notwendigen Informationen zu erhalten und Verwaltungshandeln zu überprüfen. Alternativ zur Gebührenerhebung könne die Bearbeitungszeit der Anfragen je nach Verwaltungsaufwand festgelegt werden. Ich habe zu dieser Petition Stellung genommen.

Der Anspruch auf Zugang zu amtlichen Informationen gegenüber öffentlichen Stellen in Hessen ist im Vierten Teil des HDSIG geregelt. Die Kostenregelung für die Gewährung von Informationszugang findet sich in § 88 HDSIG.

§ 88 HDSIG

(1) Die Erteilung mündlicher und einfacher schriftlicher Auskünfte sowie die Einsichtnahme in Dateien und Akten vor Ort nach dem Vierten Teil dieses Gesetzes sind kostenfrei. Für sonstige Amtshandlungen nach diesem Teil werden Kosten (Gebühren und Auslagen) nach Maßgabe des Hessischen Verwaltungskostengesetzes erhoben. Von § 9 des Hessischen Verwaltungskostengesetzes gelten nur Abs. 1 Satz 1 Nr. 6, insoweit mit der Maßgabe, dass Auslagen für Ausfertigungen, Abschriften und Kopien 0,20 Euro je Seite nicht überschreiten dürfen, und Abs. 5. Die Gebühren sind auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen, dass die antragstellenden Personen dadurch nicht von der Geltendmachung ihres Informationsanspruchs nach § 80 Abs. 1 abgehalten werden.

(2) Im Fall des § 81 Abs. 1 Nr. 7 werden Kosten nach Maßgabe der Satzung erhoben.

Stellungnahme zu der Petition

Ich habe dem Hessischen Landtag empfohlen, das Anliegen des Petenten nicht zu befürworten. Für eine Änderung des § 88 HDSIG besteht, nach meiner Auffassung, keine Veranlassung.

Das Erteilen einfacher mündlicher und schriftlicher Auskünfte sowie die Einsichtnahme in Akten vor Ort ist ohnehin gebührenfrei. Es erscheint nicht unbillig, für umfangreichere und komplexere Auskünfte eine Gebühr zu erheben. Zwar soll das Erheben von Gebühren nicht dazu führen, dass Bürgerinnen und Bürger aus Kostengründen davon abgehalten werden, ihr Recht auf Informationszugang geltend zu machen. Jedoch enthält das Hessische Verwaltungskostengesetz (HVwKostG) in § 17 eine Billigkeitsregelung.

§ 17 HvwKostG

(1) Die Behörde, welche die Kosten festsetzt, kann diese ermäßigen oder von der Erhebung absehen, wenn dies mit Rücksicht auf die wirtschaftlichen Verhältnisse des Kostenpflichtigen oder sonst aus Billigkeitsgründen geboten erscheint.

(2) Das fachlich zuständige Ministerium kann im Benehmen mit dem Ministerium der Finanzen anordnen, dass für bestimmte Arten von Amtshandlungen von der Erhebung von Kosten ganz oder zum Teil abzusehen ist, wenn sie unbillig erscheint oder dem öffentlichen Interesse widerspricht.

Mit Blick auf § 17 Abs. 1 HVwKostG ist nicht zu befürchten, dass Bürgerinnen und Bürger, die in prekären wirtschaftlichen Verhältnissen leben, aus diesem Grund von der Wahrnehmung ihrer Rechte nach dem HDSIG abgehalten werden. Der Grundgedanke der Regelung des § 17 HVwKostG wurde auch in § 88 Abs. 1 Satz 4 HDSIG aufgenommen. Dabei sind die Gebühren auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen, dass die antragstellenden Personen dadurch nicht von der Geltendmachung ihres Informationsanspruchs abgehalten werden.

Demgegenüber steht die Tatsache, dass die Bearbeitung umfangreicher und komplexer Informationszugangsanträge für die zuständigen Behörden oft mit erheblichem Aufwand verbunden ist. Es ist nicht ersichtlich, warum diese Amtshandlungen vollständig kostenfrei erfolgen sollten, zumal dies zur Folge hätte, dass die Steuerzahlerinnen und Steuerzahler diese Kosten dann zu tragen hätten.

Rechtslage in anderen Bundesländern

Die Petition habe ich zum Anlass genommen, mich beim Treffen des Arbeitskreises Informationsfreiheit der IFK im September 2023 mit den anderen Mitgliedern des Arbeitskreises über deren Kostenregelungen in Bund und Ländern auszutauschen. Da sowohl der Bund als auch die Bundesländer (mit der Ausnahme von Bayern und Niedersachsen, die den Anspruch auf Zugang zu öffentlichen Informationen nicht gesetzlich verankert haben) jeweils unterschiedliche Gesetze zur Informationsfreiheit erlassen haben, weicht die

Rechtslage zu den Kosten für bereitgestellte Informationen in Hessen von der in anderen Bundesländern und im Bund teilweise ab. Eine Übersicht über die Kostenregelungen und die dazugehörigen Gebührenordnungen und Gebührengesetze findet sich auf der Plattform FragDenStaat.[122] Exemplarisch möchte ich einige unterschiedliche Kostenregelungen darstellen:

Nach dem Recht einiger Bundesländer und des Bundes sind grundsätzlich Kosten zu erheben, wobei einfache Auskünfte kostenfrei sind. Der **Bund** erhebt nach § 10 Abs. 1 Satz 1 IFG Gebühren und Auslagen für individuell zurechenbare öffentliche Leistungen nach dem IFG. Nach § 10 Abs. 1 Satz 2 IFG gilt dies nicht für die Erteilung einfacher Auskünfte; diese sind gebührenfrei. Diese Regelung ist auch in **Schleswig-Holstein** nach § **13 Abs. 1 Satz 2 IZG-SH** vorgesehen, wobei nach schleswig-holsteinischem Recht auch die Einsichtnahme vor Ort, Maßnahmen und Vorkehrungen nach § 8 IZG-SH sowie die Unterrichtung der Öffentlichkeit nach § 11 IZG-SH kostenfrei sind. **Rheinland-Pfalz** hat eine ähnliche Regelung in § **24 Abs. 1** LTranspG RP ebenso wie **Thüringen** in § 15 Abs. 1 ThürTG. Diese Rechtslage ist ähnlich der in Hessen, wobei in Thüringen die Kosten nach § 15 Abs. 1 Satz 2 THürTG einen Betrag von 500 EUR nicht übersteigen dürfen.

Wiederum in anderen Bundesländern gibt es, wie in Thüringen, Mindest- oder Maximalbeträge für die Kosten im Rahmen von Informationszugangsanträgen. In **Baden-Württemberg** gilt, dass die informationspflichtige Stelle nach § 10 Abs. 1 LIFG grundsätzlich Gebühren und Auslagen nach dem für die informationspflichtige Stelle maßgeblichen Gebührenrecht erheben darf. Gebühren bis zu einem Höchstbetrag von 200 € können ohne Vorabinformation von der antragstellenden Person erhoben werden. Ab einer anfallenden Gebühr von 200 € Euro hat die informationspflichtige Stelle die Pflicht, die antragstellende Person vorab über Gebühren und Auslagen zu informieren. Dabei muss eine konkrete Kostenprognose oder Schätzung unter Nennung der Rechtsgrundlage erfolgen. Diese Prognose darf unterschritten, aber nicht überschritten werden. Dies gilt selbst dann, wenn im Nachhinein doch ein größerer Verwaltungsaufwand erforderlich war. Der Landesbeauftragte für Datenschutz in Baden-Württemberg selbst erhebt keine Kosten bei Informationszugängen und tritt für eine weitgehende Gebührenfreiheit ein.[123]

In **Sachsen-Anhalt** gilt nach § 10 Abs. 2a IZG LSA, dass Kosten nur erhoben werden, wenn sie eine Grenze von 50 EUR überschreiten. Ein Antrag, der abgelehnt wird, ist nach § 10 Abs. 1 IZG LSA in Verbindung mit § 13 VwKostG

122 https://fragdenstaat.de/recht/handbuch-informationsfreiheit/kosten/.

123 https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/03/20210225_lfdi_evaluierung-empfehlungen-lifg-bw.pdf.

LSA auf jeden Fall gebührenpflichtig (anders als im UIG). Eine Grenze, bis zu der keine Kosten erhoben werden, gilt ebenfalls in **Sachsen**: Gemäß § **12 Abs. 5 Satz 2** SächsTG ist der Zugang zu Informationen bis zu einem Aufwand von 600 EUR gebührenfrei. Dies gilt sogar absolut: Selbst wenn z. B. Kosten in Höhe von 700 EUR anfallen, werden nur 100 EUR berechnet.

In **Hamburg** sind Informationen nach § 13 Abs. 6 HmbTG stets gebührenpflichtig. Eine vergleichbare Regelung hat **Nordrhein-Westfalen** in § 11 Abs. 1 IFG NRW erlassen.

Abweichend ist die Rechtlage zu den Kosten für Informationsfreiheitsanträge nach § 12 UIG und § 7 VIG.

Zusammenfassend kann festgehalten werden, dass die Regelung in Hessen einen guten Kompromiss darstellt. Sie verhindert, dass amtliche Informationen wegen der Kostenlast nicht abgefragt werden können, und sie schützt die Verwaltungsbehörden vor übermäßiger Belastung durch exzessive oder missbräuchliche Informationsanfragen.

6. Arbeitsstatistik Informationsfreiheit

Im Vergleich zum Vorjahr ergab sich ein Rückgang an Beschwerden und ein Anstieg an Beratungen.

IFG	2022	2023
Beschwerden	46	**55**
Beratungen	64	**44**

ANHANG zu II

Ausgewählte Entschließungen der 44. und 45. Konferenz der Informationsfreiheitsbeauftragten in Deutschland

1.
Die Demokratie braucht starke Medien – Bundespressegesetz jetzt einführen! vom 14.06.2023

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/44_Konferenz_Entschlie%C3%9Fung-Bundespressegesetz.pdf?__blob=publicationFile&v=3

2.
25 Jahre Århus-Konvention – Veröffentlichungsanspruch muss ins Gesetz! vom 07.11.2023

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/45_Konferenz_Entschlie%C3%9Fung-Arhus-Konvention.pdf?__blob=publicationFile&v=3

3.
Moderne Transparenzgesetze bundesweit – für eine lebendige Demokratie! vom 07.11.2023

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/45_Konferenz_Entschlie%C3%9Fung-Transparenzgesetze.pdf?__blob=publicationFile&v=2

4.
Künstliche Intelligenz (KI) verantwortungsvoll für die Informationsbereitstellung nutzen! vom 07.11.2023

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/45_Konferenz_Entschlie%C3%9Fung-k%C3%BCnstliche-Intelligenz.pdf?__blob=-publicationFile&v=2

Verzeichnis der Abkürzungen

Abs.	Absatz
a. E.	am Ende
Alt.	Alternative
AO	Abgabenordnung
Art.	Artikel
BMAS	Bundesministerium für Arbeit und Soziales
BCR	Binding Corporate Rules (verbindliche interne Datenschutzvorschriften)
BDI	Bundesverband der Deutschen Industrie e. V.
BDSG	Bundesdatenschutzgesetz
BDSG aF	Bundesdatenschutzgesetz alte Fassung
BeckOK DatenschutzR	Beck´scher Online-Kommentar Datenschutzrecht
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BMG	Bundesmeldegesetz
BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BTLE	Borders, Travel & Law Enforcement (Subgroup)
BTM	Betäubungsmittel
BTMK	Betäubungsmittelkonsument
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BvR	Aktenzeichen für eine Bundesverfassungsbeschwerde
BYOD	Bring your own device
BW	Baden-Württemberg
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
ca.	Circa

CDU	Christlich Demokratische Union Deutschlands
CSC	Coordinated Supervision Committee
d. h.	das heißt
DOC	Department of Commerce (US-Handelsministerium)
DPC	Data Protection Commission (irische Datenschutzbehörde)
Drs.	Drucksache
DS-GVO, DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder; kurz: Datenschutzkonferenz
DuD	Datenschutz und Datensicherheit
DVH	Digitale Verwaltung Hessen
EDSA	Europäischer Datenschutzausschuss
EHDS	European Health Data Space
E-Mail	electronic mail
EMRK	Europäische Menschenrechtskonvention
EMM	Enterprise Mobility Management
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EUR	Euro
EU-US DPF	EU-US Data Privacy Framework
f.	folgende
FaaS	Function as a Services
ff.	folgende (Seiten) / fortfolgende
FristenVO	Verordnung zur Festlegung der Regeln für die Fristen, Daten und Termine
FTC	Federal Trade Commission (US-Bundesbehörde, zuständig für Wettbewerbskontrolle sowie Verbraucherschutz)
gem.	gemäß
GDNG	Gesundheitsdatennutzungsgesetz

GG	Grundgesetz
ggf.	gegebenenfalls
GRCh	Charta der Grundrechte der Europäischen Union
GVBl.	Gesetz- und Verordnungsblatt
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
Hessen3C	Hessen CyberCompetenceCenter
HessLStatG	Hessische Landesstatistikgesetz
HGB	Handelsgesetzbuch
HKM	Hessisches Kultusministerium
HLT	Hessischer Landtag
HMdIS	Hessisches Ministerium des Innern und für Sport
HMdF	Hessisches Ministerium der Finanzen
HMinD	Hessische Ministerin für Digitale Strategie und Entwicklung
HMSI	Hessisches Ministerium für Soziales und Integration
HMUKLV	Hessisches Ministerium für Umwelt, Klimaschutz, Landwirtschaft und Verbraucherschutz
HMWEVW	Hessisches Ministerium für Wirtschaft, Energie, Verkehr und Wohnen
HODaG	Hessisches Open Data-Gesetz
HPMG	Hessisches Gesetz über privaten Rundfunk und neue Medien
HPresseG	Hessisches Pressegesetz
HSchG	Hessisches Schulgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
HVSG	Hessisches Verfassungsschutzgesetz
HVGG	Hessisches Gesetz über das öffentliche Vermessungs- und Geoinformationswesen (Hessisches Vermessungs- und Geoinformationsgesetz)
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
HVwVG	Hessisches Verwaltungsvollstreckungsgesetz

HZD	Hessische Zentrale für Datenverarbeitung
IaaS	Infrastructure as a Service
i. d. R.	in der Regel
IFK	Informationsfreiheitskonferenz
IGH AG	Initiative Gesundheitsindustrie Hessen
INA	Innenausschuss
insb.	insbesondere
IMI	Internal Market Information System (Binnenmarkt-Informationssystem)
i. S. v.	Im Sinne von
i. V. m.	in Verbindung mit
IT	Informationstechnik
IT	Information Technologie
IT-Dienst	Informationstechnischer Dienst
IT-Infrastruktur	Informationstechnisches Infrastruktur
IT-Laboratorium	Informationstechnisches Laboratorium
IT-Projekt	Informationstechnisches Projekt
IT-Ressource	Informationstechnisches Ressource
IT-System	Informationstechnisches System
Kap.	Kapitel
KI	Künstliche Intelligenz
KIM	Kommunikation im Medizinwesen
KommJur	Kommunaljurist (Zeitschrift)
KRITIS	Kritische Infrastrukturen
KWG	Gesetz über das Kreditwesen (Kreditwesengesetz)
LBIT	Landesbeauftragte für barrierefreie IT
lit.	Litera, Buchstabe
LfV Hessen	Landesamt für Verfassungsschutz Hessen
LMedienG	Landesmediengesetz
LT-Drs.	Landtagsdrucksache (Hessen)
MDM	Mobile Device Management
MII	Medizininformatik-Initiative
MStV	Medienstaatsvertrag
m. W. v.	mit Wirkung vom

NJW	Neue Juristische Wochenschrift
Nr.	Nummer
o. g.	oben genannt/oben genannte/oben genannter
OLG	Oberlandesgericht
OWASP	Open Web Application Security Projects
OWiG	Gesetz über Ordnungswidrigkeiten
OZG	Onlinezugangsgesetz
PaaS	Platform as a Service
PAuswG	Personalausweisgesetz
PHW	personenbezogener Hinweis
POLAS	Polizeiliches Auskunftssystem
RBStV	Rundfunkbeitragsstaatsvertrag
Rdnr./Rn.	Randnummer
RED	Rechtsextremismusdatei
RED-G	Rechtsextremismusdatei-Gesetz
Rs.	Rechtssache
S.	Seite *oder* Satz
s.	siehe
s. a.	siehe auch
SaaS	Software as a Service
SIS II	Schengen Information System der zweiten Generation
S/MIME	Secure / Multipurpose Internet Mail Extensions
s. o.	siehe oben
sog.	sogenannte/sogenannter/sogenanntes
SOG MV	Gesetzes über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern
SPD	Sozialdemokratische Partei Deutschlands
SPH	Schulportal Hessen
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TLS	Transport Layer Security
TMF	Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V.

TOM	Technisch-organisatorische Maßnahmen
u. a.	unter anderem
UAbs.	Unterabsatz
US(A)	Vereinigte Staaten von Amerika
UWG	Gesetz gegen den unlauteren Wettbewerb
VG	Verwaltungsgericht
VO	Verordnung
vgl.	vergleiche
V-Leute	Verbindungs- oder Vertrauenspersonen
VwGO	Verwaltungsgerichtsordnung
WWW	World Wide Web
z. B.	zum Beispiel
z. T.	zum Teil
ZD	Zeitschrift für Datenschutz
Ziff.	Ziffer

Register der Rechtsvorschriften

Zitiert werden die jeweils zum Bearbeitungszeitpunkt geltenden Fassungen.

Gesetz/Vorschrift	Fundstelle(n)
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. 10 G vom 23. Juni 2021 (BGBl. I S. 1858, 1968, ber. 2022 I S. 1045)
BDSG	Bundesdatenschutzgesetz vom 30.06.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858)
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 des Gesetzes vom 30.06.2017 (BGBl. I S. 2097)
BKAG	Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), zuletzt geändert durch Art. 3 des Gesetzes vom 19. Dezember 2022 (BGBl. I S. 2632)
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)
BMG	Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084), zuletzt geändert durch Art. 4 des Gesetzes vom 21. Juli 2022 (BGBl. I S. 1182)
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982).
BZRG	Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz – BZRG), in der Fassung der Bekanntmachung vom 21. September 1984
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)
DV-VerbundG	Datenverarbeitungsverbundgesetz in der Fassung vom 4. April 2007; letzte berücksichtigte Änderung: zuletzt geändert durch Art. 2 des Gesetzes vom 11. Dezember 2019 (GVBl. S. 416)

EGovG	Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) (BGBl I, 2749), zuletzt geändert durch Gesetz vom 16.07.2021 (BGBl I, S. 2941)
EMRK	Europäische Menschenrechtskonvention (Konvention zum Schutze der Menschenrechte und Grundfreiheiten) vom 04.11.1950, zuletzt geändert durch Protokoll Nr. 15 vom 24.06.2013 m. W. v. 01.08.2021
EU-US-Privacy Shield	EU-US-Privacy Shield (EU-US-Datenschutzschild) Durchführungsbeschluss (EU) 2016/1250 der Kommission vom 12. Juli 2016 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzes (bekanntgegeben unter Aktenzeichen C(2016) 4176)
GG	Grundgesetz Vom 23. Mai 1949, zuletzt geändert durch Art. 1 ÄndG (Art. 82) vom 19.12.2022 (BGBl. I S. 2478)
GRCh	Charta der Grundrechte der Europäischen Union, ABl. C 326 vom 26.10.2012, S. 391
GVG	Gerichtsverfassungsgesetz in der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I S. 1077), zuletzt geändert durch Art. 3 des Gesetzes vom 8. Oktober 2023 (BGBl. 2023 I Nr. 272)
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)
HessLStatG	Gesetz über die Statistik im Land Hessen (Hessisches Landesstatistikgesetz – HessLStatG) vom 19. Mai 1987, zuletzt geändert durch Gesetz vom 19. September 2016 (GVBl. S. 158)
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
HGB	Handelsgesetzbuch Gesetz vom 10.05.1897 (RGBl. I S. 219), zuletzt geändert durch Art. 7 des Gesetzes vom 21.12.2023 (BGBl. I Nr. 397)
HGO	Hessische Gemeindeordnung in der Fassung der Bekanntmachung vom 7. März 2005, zuletzt geändert durch Art. 2 des Gesetzes vom 16. Februar 2023 (GVBl. S. 90, 93)
HmbTG	Hamburgisches Transparenzgesetz vom 12. Juni 2012, zuletzt geändert durch Gesetz vom 19. Dezember 2019

HODaG	Hessisches Gesetz über offene Daten der Träger der öffentlichen Verwaltung (Hessisches Open Data-Gesetz – HODaG) vom 23. März 2023
HPVG	Hessisches Personalvertretungsgesetz vom 28. März 2023
HPresseG	Hessisches Gesetz über Freiheit und Recht der Presse, in der Fassung vom 12. Dezember 2003, zuletzt geändert durch Gesetz vom 3. Mai 2018 (GVBl. S. 82)
HSchG	Hessisches Schulgesetz vom 30.06.2017, zuletzt geändert durch Gesetz vom 07.12.2022 (GVBl. S. 734).
HSOG – alt	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung vom 14. Januar 2005 (GVBl. I S. 14), FFN 310-63, zuletzt geändert durch Art. 10 Hess. Ausländer-TeilhabeG Kommunalpolitik vom 07.05.2020 (GVBl. S. 318)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung vom 14. Januar 2005 (GVBl. I S. 14), FFN 310-63, zuletzt geändert durch Art. 2, Art. 4 G zur Änderung sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei vom 29.06.2023 (GVBl. S. 456)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung vom 14.Januar 2005 (GVBl. I 2005 S. 14), zuletzt geändert durch Art. 3 des Gesetzes vom 30. September 2021 (GVBl. S. 622)
HVGG	Hessisches Gesetz über das öffentliche Vermessungs- und Geoinformationswesen (Hessisches Vermessungs- und Geoinformationsgesetz – HVGG) vom 6. September 2007, zuletzt geändert durch Art. 1 des Gesetzes vom 30. September 2021 (GVBl. S. 602)
HVSG	Hessisches Verfassungsschutzgesetz (HVSG) in der Fassung vom 20. Juli 2023 (GVBl. S. 614) FFN 18-7 Neubekanntmachung des HVSG vom 25. Juni 2018 (GVBl. S. 302) in der ab 12.07.2023 geltenden Fassung
HVwKostG	Hessisches Verwaltungskostengesetz vom 12. Januar 2004 in der Fassung vom 23. Juni 2018
HVwVfG	Hessisches Verwaltungsverfahrensgesetz (HVwVfG) in der Fassung vom 15. Januar 2010, zuletzt geändert durch Art. 3 des Gesetzes vom 16. Februar 2023 (GVBl. S. 78, 81)
HVwVG	Hessisches Verwaltungsvollstreckungsgesetz in der Fassung vom 12. Dezember 2008, zuletzt geändert durch Art. 2 des Gesetzes vom 24. Mai 2023 (GVBl. S. 348, 352)
IFG	Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz) vom 5. September 2005 in der Fassung vom 19. Juni 2020

IFG NRW	Informationsfreiheitsgesetz Nordrhein-Westfalen vom 27. November 2001, zuletzt geändert durch Art. 46 des Gesetzes vom 1. Februar 2022
IZG LSA	Informationszugangsgesetz Sachsen-Anhalt vom 19. Juni 2008, zuletzt geändert durch Art. 4 des Gesetzes vom 18. Februar 2020
IZG-SH	Informationszugangsgesetz für das Land Schleswig-Holstein vom 19. Januar 2012, zuletzt geändert durch Art. 5 des Gesetzes vom 16. März 2022
KWG	Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 12 des Gesetzes vom 22. Februar 2023 (BGBl. 2023 I Nr. 51)
LIFG BW	Gesetz zur Regelung des Zugangs zu Informationen in Baden-Württemberg (Landesinformationsfreiheitsgesetz – LIFG) vom 17. Dezember 2015, zuletzt geändert durch Art. 5 des Gesetzes vom 12. Juni 2018
LTranspG RP	Transparenzgesetz Rheinland-Pfalz vom 27. November 2015, zuletzt geändert durch § 134 des Gesetzes vom 23.09.2020
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19.02.1987 (BGBl. I S. 602), zuletzt geändert durch Art. 5 des Gesetzes vom 14.03.2023 (BGBl. I Nr. 73)
PAuswG	Personalausweisgesetz vom 18. Juni 2009 (BGBl. I S. 1346), zuletzt geändert durch Art. 2 des Gesetzes vom 8. Oktober 2023 (BGBl. 2023 I Nr. 271)
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
RED-G	Gesetz zur Errichtung einer standardisierten zentralen Datei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern zur Bekämpfung des gewaltbezogenen Rechtsextremismus (Rechtsextremismus-Datei-Gesetz – RED-G) vom 20. August 2012
	Satzung des Hessischen Rundfunks über das Verfahren zur Leistung der Rundfunkbeiträge vom 23.12.2016
SächsTG	Sächsisches Transparenzgesetz vom 19. August 2022

SchDSV	Verordnung über die Verarbeitung personenbezogener Daten durch Schulen und Schulaufsichtsbehörden (Schul-Datenschutzverordnung – SchDSV) ABl Nr. 12/2023 S. 763 ff)
SGB I	Das Erste Buch Sozialgesetzbuch – Allgemeiner Teil – (Art. I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), zuletzt geändert durch Art. 4 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2759)
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 Art. 19 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1237
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)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 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 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 Gesetzes vom 26.07.2023 (BGBl. I Nr. 203)
ThürTG	Thüringer Transparenzgesetz vom 10. Oktober 2019
UIG	Umweltinformationsgesetz vom 22. Dezember 2004, zuletzt geändert durch Art. 2 des Gesetzes vom 25. Februar 2021
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
Verordnung (EG) 178/2002	Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl. L 31 vom 01.02.2002, S. 1)

Verordnung (EU) 2017/625	Verordnung (EU) 2017/625 des Europäischen Parlaments und des Rates vom 15. März 2017 über amtliche Kontrollen und andere amtliche Tätigkeiten zur Gewährleistung der Anwendung des Lebens- und Futtermittelrechts und der Vorschriften über Tiergesundheit und Tierschutz, Pflanzengesundheit und Pflanzenschutzmittel, zur Änderung der Verordnungen (EG) Nr. 999/2001, (EG) Nr. 396/2005, (EG) Nr. 1069/2009, (EG) Nr. 1107/2009, (EU) Nr. 1151/2012, (EU) Nr. 652/2014, (EU) 2016/429 und (EU) 2016/2031 des Europäischen Parlaments und des Rates, der Verordnungen (EG) Nr. 1/2005 und (EG) Nr. 1099/2009 des Rates sowie der Richtlinien 98/58/EG, 1999/74/EG, 2007/43/EG, 2008/119/EG und 2008/120/EG des Rates und zur Aufhebung der Verordnungen (EG) Nr. 854/2004 und (EG) Nr. 882/2004 des Europäischen Parlaments und des Rates, der Richtlinien 89/608/EWG, 89/662/EWG, 90/425/EWG, 91/496/EEG, 96/23/EG, 96/93/EG und 97/78/EG des Rates und des Beschlusses 92/438/EWG des Rates (Verordnung über amtliche Kontrollen
VIG	Verbraucherinformationsgesetz vom 5. November 2007, zuletzt geändert durch Art. 8 des Gesetzes vom 27. Juli 2021
VwKostG LSA	Verwaltungskostengesetz des Landes Sachsen-Anhalt vom 27. Juni 1991, zuletzt geändert durch Gesetz vom 15. Dezember 2022

Sachwortverzeichnis

B

J

K

L

Z