21. Wahlperiode

Drucksache **21/1516**

HESSISCHER LANDTAG

20. 05. 2025

Dreiundfünfzigster Tätigkeitsbericht zum Datenschutz und Siebter Tätigkeitsbericht zur Informationsfreiheit

Hessischer Beauftragter für Datenschutz und Informationsfreiheit

vorgelegt zum 31. Dezember 2024
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 20. Mai 2025 Ausgegeben am 20. Mai 2025
Gestaltung: Satzbüro Peters, Taunusstein · Herstellung: AC medienhaus, Wiesbaden · Landtagsinformationssystem: www.Hessischer-Landtag.de

Dreiundfünfzigster Tätigkeitsbericht zum Datenschutz
und
Siebter Tätigkeitsbericht zur Informationsfreiheit

des

Hessischen Beauftragten für Datenschutz
und Informationsfreiheit

Professor Dr. Alexander Roßnagel

vorgelegt zum 31. Dezember 2024
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 21/1516

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

Inhaltsverzeichnis

Zweiter Teil

7. Tätigkeitsbericht zur Informationsfreiheit

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. Im Berichtszeitraum sind diese weiter von 3.520 auf 3.839 gestiegen. Die Datenschutzaufsicht geht diesen Beschwerden nach und stellt, soweit sie Verstöße feststellt, diese 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. Datenverarbeitung in hessischen Unternehmen und Behörden ist stark abhängig von den IT-Systemen und -Dienstleistungen internationaler Digitalkonzerne – hauptsächlich aus USA und China. Dies wird sich durch die zunehmende Nutzung von Systemen Künstlicher Intelligenz noch verstärken. Diese Abhängigkeit hat zwei Nachteile: Zum einen entsprechen diese Systeme und Dienstleistungen meist nicht den Datenschutzanforderungen. Dies hat zur Folge, dass auch Verantwortliche in Hessen, die diese Techniken und Dienste nutzen, ihre datenschutzrechtlichen Pflichten nicht erfüllen können. Zum anderen erhöht die Abhängigkeit das Erpressungspotenzial anderer Staaten, auf notwendige Regelungen auch im Datenschutz und ihre Anwendung auf die Digitalkonzerne zu verzichten. Daher kommt es darauf an, soweit möglich technisch-organisatorische Alternativen zu diesen Systemen und Diensten zu nutzen und dadurch digitale Souveränität zu erringen und datenschutzgerechte Datenverarbeitung zu gewährleisten.
3. Soweit und solange diese Abhängigkeit besteht, kommt es darauf an, eine Anpassung von Angeboten und Vertragsregelungen an die europäischen Datenschutzanforderungen zu erreichen. Daher bin ich mit Microsoft in intensiven und schwierigen Gesprächen, die dieses Ziel verfolgen. Gesucht wird nach Wegen, wie die Nutzer von Microsoft 365 in Hessen ihre Datenverarbeitung datenschutzgerecht durchführen können (Teil 1 Kap. 1).
4. Das Datenschutzrecht wird vor allem durch die europäische DS-GVO geprägt. Auch für die Weiterentwicklung des Datenschutzes in Hessen ist entscheidend, wie die unbestimmten Rechtsbegriffe und die inhaltlich

offenen Rechtsregeln dieser Unionsverordnung verstanden werden. Im Berichtsjahr hat der Europäische Gerichtshof (EuGH) wieder in einer hohen Zahl von Entscheidungen zum Datenschutzrecht viele umstrittene Rechtsfragen geklärt. Auch der Europäische Datenschutzausschuss (EDSA) hat mit vielen Leitlinien, Empfehlungen und Stellungnahmen zu einer Konsolidierung des Datenschutzrechts und zu einem unionsweit einheitlichen Vollzug beigetragen. Wer auf diese Entwicklung Einfluss nehmen will, muss sich in die europäischen Diskussionen – vor allem durch engagierte Mitarbeit in Arbeitskreisen des EDSA – einbringen. Die Anzahl der europaweiten Verfahren, an denen ich beteiligt war, ist von 1.062 im Jahr 2023 auf 848 im Jahr 2024 gesunken. (Teil I Kap. 1 und Kap. 2).

5. Die Aufsichtstätigkeit wird weiterhin stark durch die Verwaltungsverfahren zur Aufklärung von Beschwerden und deren gerichtliche Kontrolle geprägt. Hierzu hat der EuGH wichtige Feststellungen getroffen, die den Ermessensspielraum der Aufsichtsbehörden bestimmen (Teil I Kap. 1). Die Zahl der verhängten Geldbußen sank von 124 im Jahr 2023 auf 47 im Jahr 2024. Dagegen nahmen die Gerichtsverfahren von 27 im Jahr 2023 auf 37 im Jahr 2024 zu (Teil I Kap. 3). Die Bedeutung des Justiziariats bleibt weiterhin hoch.
6. Ein besonderer Schwerpunkt der Aufsichtstätigkeit ist die Bearbeitung von Beschwerden, Nachfragen und Beratungen zur Ausübung von Betroffenenrechten sowie zur Unterstützung von Verantwortlichen. Die Zahl der schriftlich zu bearbeitenden Vorgänge stabilisierte sich sieben Jahre nach dem Wirksamwerden der DS-GVO auf einem sehr hohen Niveau. Sie stieg um mehr als 700 von 7.162 im Jahr 2023 auf 7.892 im Jahr 2024. Durch die zunehmende Digitalisierung wird der Bedarf an Beratung und Hilfestellungen größer und qualitativ anspruchsvoller. Dadurch steigt die Arbeitsbelastung stärker als die Zahl der Vorgänge (Teil I Kap. 16).
7. Die Meldungen von Datenschutzverstößen gemäß Art. 33 DS-GVO nahmen im Berichtszeitraum wieder zu: von 1.934 im Jahr 2023 auf 2.141 im Jahr 2024. Dies ist die bisher höchste Zahl gemeldeter Datenschutzverstöße. Sie zu analysieren und zu bewerten und vor allem dazu beizutragen, sie in ihrem Schadenspotenzial zu beschränken und ihre Wiederholung zu verhindern, ist ein weiterer Arbeitsschwerpunkt der Aufsichtstätigkeit. Angriffe auf IT-Systeme nahmen quantitativ von 502 im Jahr 2023 auf 482 im Jahr 2024 leicht ab, werden aber 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. Bei der Polizei, dem Landesamt für Verfassungsschutz und mehreren Staatsanwaltschaften stellten Datenschutzprüfungen keine gravierenden

Verstöße gegen datenschutzrechtliche Vorgaben fest. Neue technische Entwicklungen im Sicherheitsbereich führen im Regelfall dazu, dass die durch sie verursachten Eingriffe in Grundrechte umfangreicher und tiefgehender werden. Sie müssen daher an bestimmte und verhältnismäßige gesetzliche Regelungen gekoppelt werden. Um solche wurde sowohl im Bereich des Verfassungsschutzes als auch den der Polizei gerungen. Im Gesetzgebungsverfahren zu den Novellen des HSOG und des HVSG habe ich kritische Anmerkungen vorgetragen, die zu einem großen Teil zu Änderungen in dem jeweiligen Gesetz geführt haben (Teil I Kap. 4).

9. In den Verwaltungsbehörden des Landes und der Kommunen werden derzeit große und anspruchsvolle Projekte der Verwaltungsmodernisierung konzipiert, geplant und umgesetzt. Daneben waren viele alltägliche Probleme des Datenschutzes in Kommunen und Landesbehörden zu klären. Aber auch für die konventionelle Datenverarbeitung ergeben sich immer wieder grundlegende Fragen zum Datenschutz. Eine Untersuchung zur Benennung und zur Stellung von kommunalen Datenschutzbeauftragten hat ein weitgehend befriedigendes Ergebnis erbracht (Teil I Kap. 5).
10. In Schulen und in schulnahen Gremien werden viele personenbezogene Daten verarbeitet, die immer wieder zahlreiche Datenschutzthemen hervorrufen. Zum Beispiel konnten mit den Schulträgern viele Fragen der datenschutzrechtlichen Beziehungen zwischen ihnen und den Schulen geklärt und Mustervorlagen für Vereinbarungen zur gemeinsamen Verantwortung oder Auftragsverarbeitung erstellt werden. Elternbeiräte sind keine privaten Vereinigungen, sondern gesetzlich vorgesehene Gremien. Sie müssen daher bei der Auswahl von Messenger-Diensten auf deren Datenschutzkonformität achten und für ihre Mitglieder auch gleichwertige alternative Kommunikationsmöglichkeiten vorsehen (Teil I Kap. 6).
11. Im Bereich des Beschäftigtendatenschutzes erhalten wir viele Beschwerden, die es oft erfordern, korrigierend einzugreifen. Dies gilt insbesondere für Fälle, in denen das Verhalten und die Leistung von Beschäftigten überwacht werden (Teil I Kap. 7).
12. Bezogen auf das Internet ist die wichtigste Entwicklung der letzten Jahre die Verbreitung cloud-gestützter Systeme Künstlicher Intelligenz. Diese erfordert, die „alten“ Regelungen der DS-GVO für deterministische IT-Systeme auf völlig neue Verarbeitungsweisen personenbezogener Daten anzuwenden, die für sie nicht unmittelbar passen. Eine wichtige, vergleichsweise konventionelle Frage war vielfach, ob und wann Einwilligungen der richtige Erlaubnistatbestand für Datenverarbeitungen im Internet darstellen (Teil I Kap. 8).

13. Im Bereich Werbung und Adresshandel musste ich mehrfach intervenieren, weil Mitarbeitende, die das Unternehmen verlassen hatten, wertvolle Adress- oder Profildaten mitgenommen und im Rahmen des neuen Arbeitsverhältnisses rechtswidrig für Werbezwecke verwendet haben. Unzulässig ist es auch, Interessenten, die einen Online-Einkauf abbrechen, nachdem sie die Waren bereits in den Warenkorb gelegt haben, mit Follow-Up-E-Mails doch noch zum Kauf der Waren zu verleiten (Teil I Kap. 9).
14. Im Bereich der Wirtschaft waren die neuen Verhaltensregeln für die Prüf- und Speicherfristen von rechtmäßig gespeicherten personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien zu verhandeln und zu genehmigen. Dabei konnten viele datenschutzrechtliche Verbesserungen erzielt werden. Wichtig war auch, die datenschutzrechtliche Rolle von Inkassounternehmen als Verantwortlichen im Sinne des Art. 4 Nr. 7 DS-GVO zu klären. Gegenüber der Deutschen Bahn konnte erreicht werden, dass sie beim Verkauf von Sparpreistickets nicht mehr fordert, dass die Daten eines E-Mail-Kontos oder eines Smartphones angegeben werden müssen (Teil I Kap. 11).
15. Im Gesundheitsbereich war es in vielen Fällen notwendig, zum Schutz von Patientendaten in Kliniken, Arztpraxen und Apotheken zu intervenieren. Außerdem habe ich die Kammern für Gesundheitsberufe in Hessen aufgefordert, das Recht des Patienten auf kostenlose Kopie der Patientenakte auch in ihren Berufsordnungen zu berücksichtigen. In mehreren Fällen war der Schutz von Gesundheitsdaten in besonderer Weise gefährdet, weil Krankenhäuser geschlossen wurden und niemand mehr für den Schutz der Patientenakten verantwortlich war. Daher mussten wir mit den zuständigen Gemeinden und Polizeistellen Schutzmöglichkeiten für diese Akten finden. Für solche Fälle bedarf es ausdrücklicher Regelungen zur Letztverantwortung für die Aufbewahrung von Patientenakten (Teil I Kap. 12).
16. Der Zweck der „wissenschaftlichen Forschung“ erfährt von der DS-GVO mehrere Bevorzugungen. Daher war es sehr wichtig, dass die DSK auf meine Vorarbeiten hin diesen Begriff definiert und abgegrenzt hat. Diese Klarstellungen führt zu einer einheitlichen Praxis im deutschen Datenschutzrecht (Teil I Kap. 13).
17. Zur Auswahl, zur Gestaltung und zum Einsatz von Software und IT-Diensten bei Unternehmen und Behörden, zu angemessenen technischen und organisatorischen Schutzmaßnahmen, zum Löschen und Vernichten nicht mehr benötigter Daten sowie zu software-gestützter Schwärzung von PDF-Dateien hat meine Behörde viele Beratungen durchgeführt. Technische Überprüfungen erfolgten z. B. zu einer großen Zahl von Websites

und zu den Softwaresystemen bei hessischen Gesundheitsämtern (Teil I Kap. 14).

18. 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 stiegen von 99 auf 116.

Vorwort

Dies ist der 53. Tätigkeitsbericht zum Datenschutz und der 7. 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.

Die Tätigkeitsberichte haben die Funktion, die aktuelle Praxis des Datenschutzes und der Informationsfreiheit in Hessen zu beschreiben und zu analysieren sowie über die Maßnahmen der Aufsichtsbehörde zu berichten.

Der 53. Tätigkeitsbericht zum Datenschutz, der die Entwicklungen im Jahr 2024 umfasst, beschreibt Bedingungen und Ergebnisse der Aufsichtstätigkeit im Bereich des Datenschutzes. Das Grundrecht auf Datenschutz schützt die Selbstbestimmung des Individuums über seine Daten und ist zugleich eine Zielsetzung der gesellschaftlichen Ordnung und Entwicklung zum Schutz von Demokratie und Rechtsstaat. Die Datenschutzaufsicht hat die grundsätzliche Aufgabe, diese individuelle und gesellschaftliche Selbstbestimmung im Rahmen der Rechtsordnung gegenüber den Stellen, die die Verarbeitung personenbezogener Daten zur Steigerung ihrer Informationsmacht nutzen, zu verteidigen und Machtungleichgewichte, die durch die Datenverarbeitung entstehen, auszugleichen.

Diese Aufgabe wird jedoch immer schwieriger und verursacht neue Herausforderungen für die Hessische Datenschutzaufsicht. Die Digitalisierung aller Gesellschaftsbereiche führt zu einer intensiveren Verarbeitung personenbezogener Daten und die Geschäftsmodelle weltweiter Konzerne erschweren die Durchsetzung von Datenschutz, weil sie sich vielfach der Datenschutzaufsicht entziehen. Das Eindringen der Informationstechnik in den Alltag erfasst alltägliche Handlungen und führt zu einer Vervielfachung personenbezogener Daten. Dennoch ist es der Hessischen Datenschutzaufsicht gelungen, auch im Jahr 2024 an vielen Stellen und vielen Verfahren Datenschutz durchzusetzen.

Zusätzlich zu den Aufgaben des Datenschutzes in Hessen hatte ich im Jahr 2024, als Vorsitzender der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, verstärkt auch die deutsche und europäische Perspektive einzunehmen. Dies war mit zusätzlichen Aufgaben der politischen Bewertung und strategischen Entwicklung sowie der Repräsentation und Koordination verbunden.

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.

Wiesbaden, den 31. März 2025

Prof. Dr. Alexander Roßnagel

I
Erster Teil
53. Tätigkeitsbericht zum Datenschutz

1. Neue Aufgaben und Rahmenbedingungen

Meine Tätigkeit als Hessischer Beauftragter für Datenschutz war im Berichtsjahr stark davon geprägt, dass ich im Jahr 2024 den Vorsitz in der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) innehatte (Kap. 1.1). Auch im siebten Jahr seit dem Geltungsbeginn der Datenschutz-Grundverordnung in Deutschland am 25. Mai 2018 wird der Datenschutz in Hessen immer stärker durch die Europäisierung des Datenschutzrechts geprägt. Daher war die Mitwirkung in europäischen Datenschutzgremien besonders wichtig, um auf diese Entwicklung Einfluss zu nehmen (Kap. 1.2). Auch die Rechtsprechung des Europäischen Gerichtshofs ist für das einheitliche Verständnis von Datenschutz in der Europäischen Union von hoher Relevanz. Im Berichtszeitraum hat er insbesondere die Aufgaben und Handlungsmöglichkeiten der Datenschutzaufsichtsbehörden durch drei Entscheidungen konturiert (Kap. 1.3) und wichtige Entscheidungen zum Verständnis von personenbezogenen und anonymen Daten getroffen (Kap. 1.4). Im Berichtszeitraum musste ich mich erstmals mit zwei normativen Innovationen auseinandersetzen, nämlich mit Settlement-Verfahren im Rahmen der Anordnung von Sanktionen (Kap. 1.5) und mit der Genehmigung von datenschutzrechtlichen Verhaltensregeln am Beispiel der Wirtschaftsauskunfteien (Kap. 1.6). In der Umsetzung des Datenschutzrechts tun sich die Aufsichtsbehörden vor allem gegenüber den internationalen Digitalkonzernen schwer, die ihre große Wirtschaftsmacht dazu benutzen, eigene Rechtsordnungen in ihren Plattformen gegenüber dem europäischen Datenschutzrecht durchzusetzen. In Gesprächen mit Microsoft könnte sich eine Entwicklung abzeichnen, dass ein Digitalkonzern sich an europäische Datenschutzvorgaben anpasst (Kap. 1.7). Besonders stark war ich auch mit der datenschutzgerechten Gestaltung und Nutzung von Systemen der Künstlichen Intelligenz befasst (s. hierzu Kap. 8.1 (aktuelle Entwicklungen), Kap. 2 (EDSA-Beschluss zu Sprachmodellen) und Kap. 5.1 (Künstliche Intelligenz in der öffentlichen Verwaltung). Schließlich ist noch die Wahl meiner bisherigen Mitarbeiterin Frau Maria Christina Rost zur Landesbeauftragten für den Datenschutz in Sachsen-Anhalt zu vermelden (Kap. 1.8).

1.1 Vorsitz in der Datenschutzkonferenz

Die Aufsichtstätigkeit war im Berichtsjahr stark davon geprägt, dass ich den Vorsitz der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) (https://www.datenschutzkonferenz-online.de/) innehatte.

Die DSK ist der Zusammenschluss der unabhängigen Datenschutzaufsichtsbehörden, der deren Aufsichtstätigkeiten in Deutschland koordiniert (s. näher 51. Tätigkeitsbericht, Kap. 1 und 52. Tätigkeitsbericht, Kap. 1) und dadurch zu einem einheitlichen Verständnis der Datenschutzregelungen und einer einheitlichen Handhabung der Datenschutzvorgaben führt.

Regulär hatte Frau Dr. Imke Sommer, die damalige Datenschutzbeauftragte des Landes Bremen, am 1. Januar 2024 den jährlich wechselnden Vorsitz von Schleswig-Holstein übernommen. Ende Januar wurde sie jedoch zur Präsidentin des Rechnungshofs des Landes Bremen gewählt und konnte daher den Vorsitz nicht mehr ausüben. Auf Drängen von Kolleginnen und Kollegen habe ich mich bereit erklärt, den Vorsitz der DSK 2024 spontan und ohne Vorbereitung zu übernehmen. Hessen wurde daraufhin auf der 1. Zwischenkonferenz am 29. Januar 2024 zum Vorsitzland gewählt. Um wichtige Aufsichtstätigkeiten wie z. B. die Genehmigung der Verhaltensregeln des Verbands „Die Wirtschaftsauskunfteien“ (s. Kap. 1.5 und Kap. 11.1) zu Ende führen zu können, übernahm Schleswig-Holstein ersatzweise den Vorsitz bis zum 15. Mai 2024.

Als Vorsitzender der DSK hatte ich die deutschen Datenschutzaufsichtsbehörden nach außen zu vertreten und nach innen zu koordinieren. In der Außenvertretung hielt ich Vorträge, nahm an Besprechungen teil, führte Korrespondenzen und vertrat die DSK gegenüber der Presse sowie in Anhörungen im Bundestag und in Landtagen. Zur Koordination der Aufsichtsbehörden leitete ich jeden Montag den Jour fixe der DSK, organisierte eine große Konferenz der DSK vom 13. bis zum 15. November 2024 in Wiesbaden, zwei eintägige Zwischenkonferenzen sowie zwei Treffen mit den spezifischen Aufsichtsbehörden für die öffentlich-rechtlichen Rundfunkanstalten und die Kirchen. Inhaltlich bereitete ich Stellungnahmen der DSK vor, koordinierte die Arbeiten ihrer Arbeitskreise und Task Forces, leitete inhaltliche Workshops und versuchte dabei immer wieder, inhaltliche Positionen einander anzugleichen, Kompromisse zu finden und eine einheitliche Sichtweise aller Aufsichtsbehörden zu erreichen.

Auch im Vorsitzjahr arbeiteten Vertreter meiner Behörde in allen 25 Arbeitskreisen und in den meisten Task Forces der DSK mit. Ich hatte weiterhin 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.

Durch die Mitarbeit in den Gremien der DSK und insbesondere durch den Vorsitz im Jahr 2024 konnte Hessen entscheidenden Einfluss auf das Ver-

ständnis und die Auslegungen des Datenschutzrechts und auf die Arbeit der Aufsichtsbehörden nehmen.

Einige Aufsichtsbehörden wählen ein bestimmtes datenschutzrechtliches Thema, dem sie sich in ihrem Vorsitzjahr in besonderer Weise widmen wollen. Als ein solches besonderes Thema im hessischen Vorsitzjahr wählte ich die Problematik, dass immer mehr digitale Hürden zu analogen Leistungen errichtet werden, die nur durch Preisgabe zusätzlicher personenbezogener Daten überwunden werden können. Diese Leistungen wurden bisher ohne Erhebung personenbezogener Daten angeboten und konnten anonym genutzt werden. Zunehmend können sie jedoch nur noch digital beantragt, bestellt oder angefordert werden. Dabei müssen personenbezogene Daten angegeben werden, die nicht erforderlich sind, um die Leistung als solche zu erbringen. Soweit der digitale Zugang ohne Alternative ist, werden all die Personen ausgeschlossen, die diesen Zugang nicht nutzen können oder nutzen wollen. Das kann bei Leistungen, auf die man zur Lebensführung angewiesen ist, zu der Zwangssituation führen, auf sie zu verzichten oder über den digitalen Zugang die geforderten personenbezogenen Daten preiszugeben. Vorbereitet durch Arbeiten in Hessen sowie im AK Grundsatz konnte die DSK zu dieser Problematik am 19. Dezember 2024 eine Entschließung „Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen!“ (https://www.datenschutzkonferenz-online.de/media/en/2024-12-19_DSK-Entschliessung_Menschenzentrierte-Digitalisierung.pdf) verabschieden.

Außerdem wurde das Thema in der 19. Veranstaltung der DSK zum Europäischen Datenschutztag am 28. Januar 2025 unter dem Titel „Digitalisierung um jeden Preis? Kein Zwang zur Preisgabe personenbezogener Daten“ in der Hessischen Landesvertretung in Berlin ausführlich diskutiert. Diese Veranstaltung in Erinnerung an die Europäische Datenschutzkonvention, die der Europarat am 28. Januar 1981 angenommen hat, organisiert immer der Vorsitz des letzten Jahres als Abschluss und Höhepunkt des Vorsitzjahres.

Diesem besonderen Thema des Vorsitzjahres lag auch ein im Berichtszeitraum durchgeführtes Aufsichtsverfahren gegen die Deutsche Bahn zugrunde. Dieses Verfahren und die datenschutzrechtliche Bewertung von digitalen Zugangshürden wird in Kap. 11.3 näher erläutert (s. ausführlich auch Roßnagel, Kein Zwang zur Preisgabe personenbezogener Daten. Datenschutzrechtlicher Rahmen für digitale Zugangshürden zu analogen Leistungen, Zeitschrift für Datenschutz (ZD) 2025, Heft 4, 184–189).

1.2
Mitwirkung in europäischen Datenschutzgremien

Obwohl die Datenschutzaufsichtsbehörden vollständig unabhängig sind, müssen sie nach Art. 51 DS-GVO zusammenarbeiten, um zu einem einheitlichen Vollzug des Datenschutzrechts in Europa zu gelangen. Daher ist die Mitarbeit im Europäischen Datenschutzausschuss (EDSA) und seinen Untergliederungen unabdingbar.

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 zwischen den Aufsichtsbehörden entstehende Streitfragen (s. Kap. 2). 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 von der 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.

Im Berichtsjahr war vor allem die Stellungnahme des EDSA vom 18. Dezember 2024 zu vier Fragen von weitreichender Bedeutung, welche die irische Aufsichtsbehörde zur datenschutzrechtlichen Bewertung Künstlicher Intelligenz gestellt hat (s. näher Kap. 2 und Kap. 8.1). Die Stellungnahme enthält Aussagen zur Frage, ob Large Language Models (LLM) personenbezogene Daten enthalten, welche Anforderungen an die Zulässigkeit der Verarbeitung

personenbezogener Daten bei der Entwicklung und der Anwendung von KI-Systemen bestehen und ob Datenschutzverstöße beim Training von LLM auf die Rechtmäßigkeit des Einsatzes von KI-Systemen mit solchen LLM fortwirken. Die deutsche Position zu dieser Stellungnahme musste ich als Vorsitz koordinieren und brachte mich auch in die inhaltliche Diskussion um diese intensiv ein.

1.3 Rechtsprechung des Europäischen Gerichtshofs zur Aufsichtstätigkeit

Das nationale Datenschutzrecht und die Tätigkeit der Aufsichtsbehörden wird immer stärker durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH) geprägt. Dabei hat er sich in jüngster Zeit auch intensiv mit den Aufgaben der Aufsichtsbehörden und ihrer Aufsichtstätigkeit sowie ihrer gerichtlichen Kontrolle befasst. Dass von den drei wichtigen Entscheidungen zu diesem Themenfeld zwei Entscheidungen wenige Tage vor dem Beginn und nach dem Ende des Berichtszeitraums verkündet worden sind, soll nicht davon abhalten, diese Rechtsprechung hier im Zusammenhang vorzustellen.

Die Prüfung von Beschwerden

Die Datenschutzaufsichtsbehörden haben nach Art. 57 Abs. 1 Buchst. a DS-GVO die Anwendung der DS-GVO zu überwachen und durchzusetzen. Hierfür sind die Untersuchungen von Beschwerden betroffener Personen nach Art. 77 DS-GVO ein wichtiges Hilfsmittel.

Beschwerden sind für die Durchsetzung des Datenschutzrechts objektiv relevant, weil sie der Aufsichtsbehörde helfen wahrzunehmen, wo Datenschutzverstöße stattfinden. Zu diesen Beschwerden können sie nach Art. 58 Abs. 1 DS-GVO gezielt Untersuchungen durchführen und bei Verstößen gemäß Art. 58 Abs. 2 DS-GVO Anordnungen treffen und Geldbußen verhängen. Beschwerden sind daher mitentscheidend, wie die DS-GVO in der Praxis durchgesetzt wird.

Für die betroffenen Personen sind sie subjektiv relevant, um ihre Rechte durchzusetzen. Sind sie der Meinung, dass eine Datenverarbeitung gegen ihre Rechte aus der DS-GVO verstößt, ist die Beschwerde das Mittel, um sich dagegen zu wehren und das eigene Recht durchzusetzen. Das Beschwerdeverfahren entscheidet darüber, wie einfach und effektiv betroffene Personen ihre Rechte in der Praxis durchsetzen können.

Die Beschwerden sorgfältig zu überprüfen, ist eine wesentliche Aufgabe der Aufsichtsbehörden. Sie hat seit Geltung der DS-GVO die Arbeit von

Aufsichtsbehörden stark verändert und zu einer weiteren Juridifizierung der Aufsichtstätigkeit geführt (s. 50. Tätigkeitsbericht, Kap. 1 und 51. Tätigkeitsbericht Kap. 1). Beschwerden binden den überwiegenden Teil der ohnehin geringen Ressourcen der Aufsichtsbehörden.

Aufsichtsbehörden stehen daher bei jeder Beschwerde vor der schwierigen Entscheidung, wie intensiv sie einer Beschwerde nachgehen und welche Maßnahmen sie ergreifen. Lehnen sie die Bearbeitung der Beschwerde oder die Anordnung von Maßnahmen zu Unrecht ab, kann es sein, dass sie einen Datenschutzverstoß dulden. Bearbeiten sie eine unberechtigte Beschwerde, vergeuden sie wertvolle Arbeitszeit, die ihnen für die Bearbeitung berechtigter Beschwerden fehlt. Treffen sie unnötige Anordnungen, um der Beschwerde abzuhelfen, greifen sie ungerechtfertigt oder unverhältnismäßig in die Rechte der Verantwortlichen ein.

Zu diesen Problembereichen geben drei Urteile des EuGH Hinweise, die zu mehr Rechtssicherheit für das Handeln der Aufsichtsbehörden beitragen.

EuGH-Urteil vom 7. Dezember 2023

In der Rechtssache C 26/22 und C-64/22 hat der EuGH in seinem Urteil vom 7. Dezember 2023 grundlegende Feststellungen zur Bearbeitung einer Beschwerde gegeben. An dem Verfahren war ich als Beklagter des Ausgangsverfahrens beteiligt. Es beruht auf einer Vorlage durch das Verwaltungsgericht Wiesbaden (s. auch 52. Tätigkeitsbericht, Kap. 3.1 und 11.3).

Nach diesem Urteil ist eine Beschwerde nicht mit einer Petition zu vergleichen, für welche die Datenschutzaufsichtsbehörde nur eine Bearbeitung schuldet. Vielmehr erfordert eine Beschwerde, zu ihrer Überprüfung ein reguläres Verwaltungsverfahren nach dem Verwaltungsverfahrensgesetz durchzuführen. Die Entscheidung der Datenschutzaufsichtsbehörde, eine Beschwerde zurückzuweisen, ist ein Verwaltungsakt mit Rechtswirkung. Dieser 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 (Rn. 68 ff.).

EuGH-Urteil vom 26. September 2024

Die Aussagen zum Ermessensspielraum der Aufsichtsbehörde präzisierte der EuGH in seiner Entscheidung vom 26. September 2024 in der Rechts-

sache C-768/21. Auch dieses Urteil beruhte auf einer Vorlage des Verwaltungsgerichts Wiesbaden in einem Klageverfahren gegen mich wegen der Zurückweisung einer Beschwerde und der Weigerung, eine Geldbuße festzusetzen (s. näher Kap. 3.1).

Der EuGH stellte klar, dass Datenschutzaufsichtsbehörden weder aus Art. 58 Abs. 2 DS-GVO noch aus Art. 83 DS-GVO verpflichtet sind, in jedem Fall, in dem sie eine Datenschutzverletzung feststellen, eine Abhilfemaßnahme zu ergreifen (Rn. 41). Auch besteht für den Beschwerdeführer kein subjektives Recht, eine solche Abhilfemaßnahme zu verlangen. Vielmehr besteht für die Aufsichtsbehörde hinsichtlich der Abhilfemaßnahmen sowohl ein Entschließungsermessen, ob sie überhaupt eine Anordnung trifft, als auch ein Auswahlermessen, welche Abhilfemaßnahme sie auswählt. Entscheidend ist allein, ob das Ergreifen einer oder mehrerer Abhilfemaßnahmen unter Berücksichtigung aller Umstände des konkreten Falles geeignet, erforderlich und verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuhelfen und die Einhaltung der DS-GVO zu gewährleisten (Rn. 42). Daher kann eine Abhilfemaßnahme „*ausnahmsweise*“ auch unterbleiben, „*sofern der Situation, die einen Verstoß gegen die DS-GVO begründete, bereits abgeholfen wurde und die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durch den hierfür Verantwortlichen gewährleistet ist*“ (Rn. 46).

EuGH-Urteil vom 9. Januar 2025

Der Umgang mit missbräuchlichen Beschwerden war Gegenstand der Entscheidung des EuGH vom 9. Januar 2025 in der Rechtssache C-416/23. Das Urteil betraf die Weigerung der österreichischen Aufsichtsbehörde, weitere Beschwerden einer betroffenen Person zu bearbeiten, die in den vorangegangenen 20 Monaten 70 Beschwerden eingereicht hatte.

Das kostenlose Rechtsmittel der Beschwerde wird vielfach auch eingesetzt, um andere Interessen als den Schutz der eigenen informationellen Selbstbestimmung durchzusetzen. Außerdem nutzen viele Querulanten die Möglichkeit, ihre Kritik an ungerechten Verhältnissen als eine datenschutzrechtliche Beschwerde vorzutragen. Oft sollen Beschwerden sogar gezielt die Arbeit von Behörden und Gerichten erschweren (s. zu missbräuchlichen Beschwerden auch Kap. 3.1 und Kap. 9.3).

Jede ungerechtfertigte oder böswillige Beschwerde beansprucht Ressourcen, die nicht mehr für die Bearbeitung berechtigter Beschwerden, den Schutz der Grundrechte und die Durchsetzung des Datenschutzrechts genutzt werden können. Die DS-GVO bietet den Aufsichtsbehörden in Art. 57 Abs. 4 ein Mittel, sich gegen solche ungerechtfertigten Belastungen zu wehren. Sie können „*bei offenkundig unbegründeten oder exzessiven Anfragen eine*

angemessene Gebühr auf der Grundlage der Verwaltungskosten verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden“.

Die Handlungsmöglichkeiten des Art. 57 Abs. 4 DS-GVO sind auf „Anfragen“ bezogen. Unter Anfragen sind aber auch Beschwerden zu verstehen. Denn Art. 57 Abs. 4 DS-GVO soll gerade den Aufsichtsbehörden „*die Möglichkeit (geben), mit diesen Beschwerden besser umzugehen, indem sie die Belastung verringern, die diese Beschwerden bei ihnen auslösen können*“ (Rn. 40).

Grundsätzlich soll die Aufsichtsbehörde gemäß Art. 57 Abs.1 Buchst. f und Abs. 3 DS-GVO sich mit der Beschwerde unentgeltlich befassen. Darauf bezogen enthält Art. 57 Abs. 4 DS-GVO eine Ausnahme. Diese ist nur für den Fall des Rechtsmissbrauchs gerechtfertigt. Ein solcher lässt sich nicht allein anhand der Zahl der Beschwerden feststellen (Rn. 48, 50). Auch viele Beschwerden können gerechtfertigt sein (Rn. 54). Daher muss die Aufsichtsbehörde „anhand aller relevanten Umstände jedes Einzelfalls feststellen, dass eine Missbrauchsabsicht der betroffenen Person vorliegt“ (Rn. 50, 55). Hierfür kann eine hohe Zahl von Beschwerden ein Indiz sein (Rn. 57).

Nach Art. 57 Abs. 4 Satz 2 DS-GVO trägt die Aufsichtsbehörde „die Beweislast für den exzessiven Charakter der Anfrage“. Der EuGH präzisiert in praktikabler Weise, wie die Aufsichtsbehörde die gesetzliche Beweislast erfüllen kann: Sie hat bei einer großen Zahl von Beschwerden „*nachzuweisen, dass diese Zahl nicht durch den Wunsch der betroffenen Person zu erklären ist, ihre Rechte aus der DS-GVO zu schützen*“. Aus den Umständen des Falles sollte sich ergeben, „*dass die Zahl von Beschwerden darauf abzielt, das ordnungsgemäße Funktionieren der Behörde zu beeinträchtigen, indem ihre Ressourcen missbräuchlich in Anspruch genommen werden (…). Dies kann z. B. dann der Fall sein, wenn eine Person eine so große Zahl von Beschwerden bei einer Aufsichtsbehörde einreicht, die eine Vielzahl von Verantwortlichen betreffen, zu denen sie nicht unbedingt einen Bezug hat.*“ Dies erlaubt dann den Schluss, dass „*diese übermäßige Inanspruchnahme ihres Rechts, Beschwerden einzureichen, (…) ihre Absicht erkennen lässt, die Behörde zu lähmen, indem sie sie mit Anfragen überflutet*“ (Rn. 56f.).

Ist ein Rechtsmissbrauch nachgewiesen, hat die Aufsichtsbehörde nach Art. 57 Abs. 4 Satz 1 DS-GVO die Wahl, „*eine angemessene Gebühr auf der Grundlage der Verwaltungskosten (zu) verlangen oder sich (zu) weigern, aufgrund der Anfrage tätig zu werden*“. Der EuGH überlässt diese Ermessensentscheidung der Aufsichtsbehörde. Sie muss sich nur vergewissern, dass die „*gewählte Option geeignet, erforderlich und verhältnismäßig ist*“ (Rn. 67, 70). Der EuGH gibt der Aufsichtsbehörde jedoch die Empfehlung zu prüfen, ob ein zweistufiges Verfahren den Umständen angemessen ist. Sie könnte auf einer ersten Stufe für ihre Tätigkeit Verwaltungsgebühren fordern, bevor

sie in einer zweiten Stufe diese verweigert. Die erste Stufe beeinträchtigt die Rechte der betroffenen Personen in geringerem Maße und erhält ihr die Möglichkeit, Grundrechtsschutz durch das Beschwerdeverfahren zu erlangen (Rn. 69 – s. zu dieser Entscheidung auch Roßnagel, Anmerkung zu diesem Urteil in Europäische Zeitschrift für Wirtschaftsrecht (EuZW), 35. Jg. (2025) Heft 5, 227–229).

1.4 Rechtsprechung des Europäischen Gerichtshofs zur Anonymität

Auch zum Verständnis der Begriffe personenbezogene Daten und Anonymität in Verbindung mit Erwägungsgrund 26 DS-GVO hat der EuGH seine bisherige Rechtsprechung durch wichtige Entscheidungen im Berichtsjahr so verfestigt, dass daraus klare Schlüsse gezogen werden können, wie er die Nutzung anonymer Daten versteht und bewertet (s. hierzu auch Roßnagel, Anonymisierung personenbezogener Daten und Nutzung anonymer Daten, Datenschutz und Datensicherheit (DuD) 2024, 513–520).

Urteil im Fall Breyer

Bereits in seinem Breyer-Urteil aus dem Jahr 2016 (EuGH vom 19. Oktober 2016, C-582/14) hatte der EuGH am Beispiel von IP-Adressen zu prüfen, ob der Verantwortliche personenbezogene oder anonyme Daten verarbeitet, wenn er selbst die Daten nicht einer betroffenen Person zuordnen kann. Ob ihm das Wissen Dritter zuzurechnen ist, prüft der EuGH aus Sicht des Verantwortlichen. Nach diesem Urteil kann das Wissen eines Dritten nicht einbezogen werden, „*wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung de facto vernachlässigbar erschiene*“ (Rn. 46). Nur wenn der Verantwortliche auf das Zusatzwissen des Dritten rechtmäßig zugreifen kann, ist dessen Wissen ein Mittel, das er zur Identifizierung der betroffenen Person nutzen kann. Außer in diesem Fall bleiben die (Re-)Identifizierungsmöglichkeiten weiterer Stellen für die Frage der Anonymität der Daten unberücksichtigt.

Urteil im Fall Gesamtverband Autoteile-Handel

In seinem Urteil zum Gesamtverband Autoteile-Handel vom 9. November 2023 (EuGH, C-319/22) ging es um den Personenbezug der Fahrzeugidentifikationsnummer (FIN). Auch in diesem Urteil stellte der EuGH für die Feststellung des Personenbezugs auf den jeweiligen Verantwortlichen ab.

Die FIN wird nur „*für denjenigen, der bei vernünftiger Betrachtung über Mittel verfügt, die es ermöglichen, sie einer bestimmten Person zuzuordnen, zu personenbezogenen Daten*“ (Rn. 46, 48). Dies ist z. B. für Reparaturbetriebe der Fall, die eine FIN eines bestimmten Kraftfahrzeugs einer Zulassungsbescheinigung für den Halter zuordnen kann. In diesem Fall stellt die FIN für den empfangenden Reparaturbetrieb „*ein personenbezogenes Datum dar, selbst wenn die FIN für sich genommen für die Fahrzeughersteller kein persönliches Datum darstellt, insbesondere dann nicht, wenn das Fahrzeug, dem sie zugewiesen wurde, nicht einer natürlichen Person gehört*“ (Rn. 49). Nach diesem Urteil kann also ein Datum je nach Verantwortlichem seinen Charakter als anonymes oder als personenbeziehbares Datum verändern. Entscheidend sind die Mittel des jeweils Verantwortlichen, nicht die irgendwelcher Dritter. Für die Feststellung der Anonymität oder Personenbeziehbarkeit ist nicht das Datum, vielmehr sind die Umstände des Einzelfalls entscheidend.

Urteil im Fall OLAF

Diese Rechtsprechungslinie hat der EuGH im Berichtsjahr fortgesetzt. In seinem Urteil vom 7. März 2024 zu einer Pressemitteilung des Europäischen Amtes für Betrugsbekämpfung (OLAF) hatte der EuGH festzustellen, wann der Öffentlichkeit in einer Pressemitteilung bekanntgegebene Daten personenbeziehbar sind. Der EuGH prüft zwei Fälle und kommt je nach Empfänger der Daten, der sie als Verantwortlicher weiterverarbeitet, zu unterschiedlichen Ergebnissen, – je nach Wahrscheinlichkeit der Identifizierung. Zum einen stellt er fest: *„Dass ein Investigativjournalist die Identität einer von einer Pressemitteilung betroffenen Person verbreitet hat, (…) lässt für sich genommen noch nicht den Schluss zu, dass die in dieser Mitteilung enthaltenen Informationen zwingend als personenbezogene Daten (…) zu qualifizieren sind*“ (Rn. 58). Dagegen hält er bezogen auf die adressierte Öffentlichkeit, auch die spezifische Forschungs-Community, fest: Empfänger der Presseerklärung, die auf demselben wissenschaftlichen Gebiet arbeiten wie die betroffene Person und ihren beruflichen Werdegang kennen, können aus Informationen über das Projekt, die fördernde und die durchführende Institution und weitere Details die betroffene Person „ohne einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskraft“ identifizieren. Daher war das „*Risiko der Identifizierung (…) nicht als unbedeutend*“ anzusehen (Rn. 60 ff.). Auch in diesem Fall stellt der EuGH auf die jeweiligen Verantwortlichen (Empfänger) ab und prüft die ihnen zugänglichen Mittel zur Identifizierung.

Urteil im Fall IAB-Europe

Beim Urteil des EuGH im Fall von IAB-Europe, ebenfalls vom 7. März 2024 (C-604/22), ging es um die massenhafte automatisierte Versteigerung von Nutzerprofilen für den Verkauf von Werbeplätzen auf Websites oder in Apps (Real Time Bidding). Ob der Nutzer in diese Datenverarbeitung eingewilligt hat, wird in einem individuellen „TC-String", einer Kombination aus Buchstaben und Zeichen, gespeichert. Der EuGH stellte fest, dass der Verband der Werbetreibenden IAB Europe zwar von dem TC-String selbst nicht auf den jeweiligen Internetnutzer schließen kann, dass er aber gegenüber seinen Mitgliedern einen Rechtsanspruch hat, ihm „*auf Anfrage alle Informationen zu übermitteln, die es ihm ermöglichen, die Nutzer zu identifizieren, deren Daten Gegenstand eines TC Strings sind*" (Rn. 48, 51). Der TC-String ermöglicht den Mitgliedern, den Anbietern von Websites oder Apps sowie Datenbrokern und Werbeplattformen durch Kombination mit anderen Daten wie der IP-Adresse des verwendeten Endgeräts auf die betroffene Person zu schließen. Aufgrund dieses Rechtsanspruchs entschied der EuGH, dass der TC-String auch für IAB Europe ein personenbezogenes Datum darstellt. Auch in diesem Urteil bezieht der EuGH die Feststellung des Personenbezugs auf den Verantwortlichen. Das Gericht nimmt einen Personenbezug der umstrittenen Daten nicht deshalb an, weil andere Personen, hier die Anbieter von Websites oder Apps sowie Datenbroker und Werbeplattformen, die Identität der betroffenen Personen feststellen können. Vielmehr ist für den Personenbezug entscheidend, dass der Verantwortliche das Wissen der anderen Personen für sich nutzen kann.

Erkenntnisse der EuGH-Rechtsprechung

Der EuGH geht immer vom Verantwortlichen aus und fragt, ob die von ihm verarbeiteten Daten für ihn personenbezogen sind. Andere Personen, deren Wissen der Verantwortliche nicht nutzen kann, spielen für diese Bewertung keine Rolle, auch wenn sie die betroffenen Personen identifizieren können. Andere Personen spielen nur dann eine Rolle, wenn sie in irgendeiner Beziehung zum Verantwortlichen stehen. Dies kann in zweifacher Weise der Fall sein. Zum einen kann es sein, dass der Verantwortliche ihr Wissen, ihre Fähigkeiten oder ihre Mittel für sich nutzen kann – entweder de facto oder de jure. Zum anderen können andere Personen eine Rolle spielen, wenn der Verantwortliche ihnen Daten offenlegt. Dann stellt sich die Frage, ob es sich um die Offenlegung personenbezogener Daten handelt. Dies ist der Fall, wenn der Empfänger nach allgemeinem Ermessen die Personen, auf die sich die Daten beziehen, identifizieren kann. Der Verantwortliche legt somit personenbezogene Daten offen, wenn sie für den Empfänger personenbezogen sind, auch wenn sie für ihn anonym sind.

In jedem Fall bestimmt der EuGH den Personenbezug oder die Anonymität nicht abstrakt am Maßstab einer Theorie, sondern, wie Erwägungsgrund 26 DS-GVO dies erfordert, nach den jeweils spezifischen Umständen des Einzelfalls, die das jeweilige Risiko einer (Re-)Identifizierung der betroffenen Person durch den jeweils Verantwortlichen bestimmen.

1.5
Settlement-Verfahren

Im Berichtsjahr führte ich das erste Mal ein Settlement-Verfahren durch, um in einem Geldbußenverfahren zu einem für alle Beteiligten zufriedenstellenden Ergebnis zu gelangen.

In einem Settlement-Verfahren wird in einem Sanktionsverfahren eine gegenseitige und einvernehmliche Verständigung gesucht. Diese besteht auf der Seite des Verantwortlichen darin, dass er seinen Verstoß gegen Datenschutzrecht von Anfang an zugesteht und in dem Verfahren zur Festsetzung einer Geldbuße durchgehend mit der Aufsichtsbehörde kooperiert. Dadurch kann die Aufsichtsbehörde das Verfahren schneller und mit geringerem Aufwand zum Abschluss bringen. Sie berücksichtigt umgekehrt das kooperative Verhalten des Verantwortlichen gemäß Art. 82 Abs. 3 Buchst. f DS-GVO bei der Zumessung der Geldbußen. Für ihn reduziert sich nicht nur die zu zahlende Geldbuße, sondern auch der Aufwand, der auf seiner Seite bei einer streitigen Durchführung des Verfahrens entstehen würde.

Im konkreten Fall (s. zu diesem Kap. 3.2) hat sich das Settlement-Verfahren als sinnvoll erwiesen. Beide Seiten hatten von der vertrauensvollen Zusammenarbeit Vorteile. Sofern Verständigungsgespräche nicht dazu missbraucht werden, die Aufsichtsbehörde hinzuhalten und das Verfahren zu verschleppen, bin ich auch in Zukunft bereit, das Instrument der Verständigung in datenschutzrechtlichen Geldbußenverfahren zu nutzen.

1.6
Verhaltensregeln für Wirtschaftsauskunfteien

Im Berichtsjahr musste ich das erste Mal eine der normativen Innovationen der DS-GVO umsetzen, nämlich die Verhaltensregeln für die Datenverarbeitung eines Verbandes für einen speziellen Wirtschaftsbereich zu genehmigen. Gut gemacht, können solche spezifischen Verhaltensregeln die Rechtssicherheit erhöhen, die Durchsetzung des Datenschutzrechts verbessern, die Verantwortlichen entlasten und die betroffenen Personen in der Durchsetzung ihrer Rechte unterstützen. Künftig dürfte mit weiteren Verhaltensregeln zu rechnen sein.

Die DS-GVO gilt für alle Mitgliedstaaten der Europäischen Union und alle Lebensbereiche. Sie enthält dementsprechend überwiegend sehr abstrakte Regelungen. Sie sieht daher in Art. 40 und 41 ausdrücklich die Möglichkeit vor, dass Verbände und andere Vereinigungen, die Verantwortliche oder Auftragsverarbeiter vertreten, für ihre Datenverarbeitung Verhaltensregeln erlassen. Diese Form der Selbstregulierung soll dazu beitragen, dass die abstrakten Regelungen den Besonderheiten der einzelnen Verarbeitungsbereiche und den besonderen Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen angepasst werden. Indem sie die Vorgaben der DS-GVO bereichsspezifisch präzisieren, sollen sie die ordnungsgemäße Anwendung der Verordnung unterstützen. Damit die Selbstregulierung aber nicht zu einer einseitigen Reduzierung von Datenschutzvorgaben führt, müssen die Verhaltensregeln zu ihrer Wirksamkeit von der zuständigen Aufsichtsbehörde genehmigt werden.

Der Verband „Die Wirtschaftsauskunfteien“ hatte Verhaltensregeln für die Datenverarbeitung von Auskunfteien ausgearbeitet, die von der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen genehmigt worden waren und zum Geltungsbeginn der DS-GVO am 25. Mai 2018 in Kraft traten. Diese enthielten die Regelung für die Prüf- und Speicherfristen von rechtmäßig gespeicherten personenbezogenen Daten. Sie galten zunächst für sechs Jahre. Sie sollten jedoch für weitere sechs Jahre fortgelten, wenn die zuständige Aufsichtsbehörde sie nicht vor Ablauf der sechs Jahre beanstandete. Nachdem der Verband seinen Sitz zum 1. Januar 2022 nach Wiesbaden verlegt hatte, wurde ich zur zuständigen Behörde für die Genehmigung der Verhaltensregeln.

Im Oktober 2023 habe ich die Verhaltensregeln beanstandet und eine Neufassung gefordert. Sie widersprachen mehreren zwischenzeitlich gefassten Beschlüssen der DSK und des EDSA. Außerdem machten zwei Urteile des EuGH vom 7. Dezember 2023 eine Neufassung der Verhaltensregeln erforderlich. Diese ergingen zur Datenverarbeitung der SCHUFA zum Bonitäts-Scoring (Rechtssache C-26 und 64/22) und zur Speicherung von Daten zur Restschuldbefreiung (Rechtssache C-634/21). Der EuGH hatte einzelne Verarbeitungsschritte als unionsrechtswidrig eingestuft, zugleich aber das grundsätzliche Geschäftsmodell der Auskunfteien nicht beanstandet. Damit hatte ich erstmals die Aufgabe, die Neufassung von Verhaltensregeln zu überprüfen und zu genehmigen.

Bei den Verhandlungen über die Bedingungen einer Genehmigung der neuen Verhaltensregeln habe ich die Aufsichtsbehörden von Baden-Württemberg, Bayern und Nordrhein-Westfalen beteiligt, weil auch sie die Aufsicht über

große Auskunfteien, die Mitglieder des Verbands sind, führen. Die Verhandlungen fanden von Januar bis Mai 2024 in mehreren Runden statt.

Im Ergebnis hat der Verband seine Verhaltensregeln stark verändert. Sie werden jetzt den Anforderungen und Erwartungen der DS-GVO besser gerecht (s. zum Verfahren, zu den Ergebnissen und ihren Auswirkungen der Verhandlungen ausführlich Kap. 11.1). Der Entwurf der Verhaltensregeln wurde der DSK vorgestellt. Die Mitglieder der DSK, die die Datenschutzaufsicht für den nichtöffentlichen Bereich ausüben, unterstützten am 14. Mai 2024 meine Absicht einstimmig, die Verhaltensregeln zu genehmigen. Am 24. Mai 2024 habe ich dann die neuen Verhaltensregeln des Verbands „Die Wirtschaftsauskunfteien“ genehmigt.

1.7
Gespräche mit Microsoft

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 steht noch immer Microsoft – vor allem mit seinem Cloud-Angebot MS 365. Für das Jahr 2024 sind jedoch hoffnungsvolle Entwicklungen zu berichten.

Bisherige Entwicklung

Im November 2022 hat die DSK nach langen Verhandlungen mit Microsoft festgestellt, dass datenschutzrechtlich Verantwortliche ihre Nachweispflicht im Zusammenhang mit der Nutzung des Angebots Microsoft 365 nicht ohne weiteres erfüllen können (DSK, Feststellung vom 24.11.2022, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf). Der Grund liegt in der Standard-Vereinbarung „Datenschutznachtrag zu den Produkten und Services“ von Microsoft (im Berichtszeitraum Stand 1.1.2024)“ (Data Protection Addendum,-abgekürzt DPA), die Microsoft seinen Kunden als Auftraggebern für den abzuschließenden Auftragsverarbeitungsvertrag vorlegt. Dieser erfüllt nicht die Anforderungen an die notwendigen Vereinbarungen zwischen Auftraggebern und Auftragsverarbeitern nach Art. 28 DS-GVO (DSK, Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf). Zu sieben

Themen sind die Regelungen des DPA unzureichend (s. ausführlich 52. Tätigkeitsbericht, Kap. 1.2).

Die Unternehmen und Behörden in Hessen, die MS 365 nutzen wollen, befinden sich im Regelfall in einem Dilemma. Sie sind von diesen Systemen abhängig, aber nicht in der Lage, mit ihnen ihrer datenschutzrechtlichen Verantwortung gerecht zu werden. Um einen Ausweg aus diesem Dilemma zu finden, forderte ich von ihnen aus Gründen der Verhältnismäßigkeit in einem ersten Schritt, dass sie von Microsoft eine Zusatzvereinbarung einfordern, in der die Festlegungen enthalten sind, die bisher im DPA fehlen. Die Datenschutzaufsichtsbehörden unterstützten dieses Vorgehen durch eine Handreichung, was genau zu fordern ist (https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/vereinbarung-zur-auftragsverarbeitung-fuer-den-einsatz-von-microsoft-365). 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.

Diese Forderungen führten dazu, dass sich Microsoft an mich wandte und vorschlug, diese vielen Forderungen zu bündeln und direkt mit mir zu verhandeln, unter welchen Bedingungen ich die datenschutzrechtlichen Anforderungen als erfüllt ansehe.

Gespräche über Microsoft Teams

Da die Hessische Ministerin für Digitalisierung und Innovation, Frau Prof. Dr. Kristina Sinemus, eruieren wollte, ob Microsoft 365, insbesondere das Dienstangebot Teams, in der hessischen Landesverwaltung datenschutzgerecht genutzt werden kann, bat sie mich, mit Microsoft Gespräche darüber zu führen, ob und wie hinsichtlich der datenschutzwidrigen Vertragsbedingungen von Microsoft Lösungen erreicht werden können. Daraufhin haben Microsoft und ich unsere Gespräche auf das Dienstangebot Teams fokussiert und für diese geprüft, unter welchen realisierbaren Bedingungen die sieben Kritikpunkte der DSK konstruktiv umgesetzt werden können. Mit dieser Zielsetzung habe ich im Juli und August 2024 mehrere Gespräche mit Microsoft geführt und eine Vielzahl von Unterlagen zu MS Teams summarisch bewertet.

Ergebnis der Gespräche

Auf Basis der gewonnenen Erkenntnisse und der von MS gegebenen Zusagen gehe ich davon aus, dass ein datenschutzkonformer Einsatz von MS Teams durch die hessische Landesverwaltung möglich ist. Dieses Ergebnis

ist ein normatives Konzept, wie beide Seiten – Microsoft und die hessische Landesverwaltung, zusammen mit ihrem Auftragnehmer Hessische Zentrale für Datenverarbeitung (HZD) – dazu beitragen können, dass die datenschutzrechtlichen Anforderungen erfüllt und insbesondere die sieben Kritikpunkte der DSK beseitigt werden können. Das Ergebnis beruht nicht auf einer datenschutzrechtlichen Prüfung von MS Teams in der Landesverwaltung. Eine solche kann erst nach der konkreten Konzipierung und Implementierung dieses Cloud-Dienstes erfolgen.

Grundlage des normativen Konzepts ist, dass nicht das Produkt MS Teams allein, sondern die Datenverarbeitungsvorgänge in der hessischen Landesverwaltung in der Anwendung von Teams betrachtet werden. Aus diesem Blickwinkel kann eine datenschutzkonforme Datenverarbeitung auch stattfinden, wenn das Land Hessen datenschutzrechtliche Defizite des Dienstangebots Teams durch eigene Anstrengungen ausgleicht und daran mitwirkt, die notwendigen Dokumentationen zu erstellen sowie die technischen und organisatorischen Maßnahmen zu ergreifen, die für einen datenschutzkonformen Betrieb von MS Teams erforderlich sind. Um dies an einem Beispiel zu erläutern: Eine datenschutzgerechte frühzeitige Löschung personenbezogener Daten, die Microsoft nicht durchführt, kann auch dadurch erreicht werden, dass die HZD auf der Grundlage eines geeigneten Löschkonzepts die notwendigen Datenlöschungen vornimmt und Microsoft dies auf seinen IT-Systemen ermöglicht.

Dieses methodische Vorgehen und die bisher gefundenen Ergebnisse sollen in weiteren Gesprächen mit Microsoft auf alle Dienstangebote von MS 365 und weitere Anwendungsfelder im öffentlichen und nicht öffentlichen Bereich zur Anwendung kommen. Aufgrund der Belastungen des DSK-Vorsitzes (s. Kap. 1.1) wurde die Fortführung der Gespräche auf das erste Halbjahr 2025 verschoben.

1.8
Landesbeauftragte für den Datenschutz in Sachsen-Anhalt

Schließlich ist noch eine Meldung aus meiner Dienststelle mitteilenswert. Die bisherige Leiterin meines Justiziariats, Leiterin der Stabsstelle Öffentlichkeitsarbeit und meine persönliche Referentin Frau Maria Christina Rost, die 12 Jahre in meiner Dienststelle beschäftigt war, ist im April 2024 vom Landtag in Sachsen-Anhalt zur Landesbeauftragten für den Datenschutz des Landes Sachsen-Anhalt gewählt worden. Sie trat ihr Amt am 1. August 2024 an. Sachsen-Anhalt hat dadurch nach sechs Jahren wieder eine demokratisch legitimierte Spitze der datenschutzrechtlichen Aufsichtsbehörde. Ich wünsche ihr für ihr Amt eine glückliche Hand.

2. Europäische und internationale Zusammenarbeit

Die Europäisierung des Datenschutzrechts erfordert eine intensive Zusammenarbeit zwischen den Aufsichtsbehörden der Mitgliedstaaten. Daher verpflichtet die DS-GVO die EWR-Datenschutzaufsichtsbehörden bei grenzüberschreitenden Datenverarbeitungen im Sinn des Art. 4 Nr. 23 DS-GVO zur Kooperation. Diese Zusammenarbeit, die für alle zu einer erheblichen Mehrarbeit führt, wird an zwei Beispielen beschrieben: der einheitlichen Bewertung großer Sprachmodelle der Künstlichen Intelligenz und der Genehmigung von verbindlichen konzerninternen Datenschutzvorschriften.

2.1 Einheitliche Bewertung großer Sprachmodelle der Künstlichen Intelligenz

Die Datenschutzaufsichtsbehörden im Europäischen Wirtschaftsraum (EWR) bearbeiten über das Binnenmarktinformationssystem Fälle grenzüberschreitender Datenverarbeitungen (Datenschutzbeschwerden nach Art. 77 DS-GVO und Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Art. 33 DS-GVO). Berichtenswert waren Verfahren mit hohen Bußgeldsummen – etwa 290 Millionen EUR gegen Uber wegen Datenübermittlungen in die USA ohne angemessene Maßnahmen zum Schutz der verarbeiteten Informationen oder 91 Millionen EUR gegen Meta wegen der Speicherung unverschlüsselter Passwörter in internen Datenbanken. Vor allem aber beschäftigte alle Datenschutzaufsichtsbehörden die weitere Verbreitung von großen Sprachmodellen (Large Language Models – LLM). Auf Antrag der irischen Datenschutzaufsichtsbehörde nach Art. 64 Abs. 2 DS-GVO mussten die europäischen Datenschutzaufsichtsbehörden im EDSA in vergleichsweise kurzer Zeit eine einheitliche Stellungnahme zu vier Rechtsfragen erarbeiten, die LLM betreffen. Vor Ausarbeitung der Stellungnahme hat der EDSA am 4. November 2024 in einem „Stakeholder Event" Vertreter von europäischen Branchenverbänden, Organisationen, Nichtregierungsorganisationen, Unternehmen, Anwaltskanzleien und Wissenschaftlern eingebunden, um die von der irischen Aufsichtsbehörde gestellten Fragen zu erörtern. Die verschiedenen Entwürfe der beteiligten Expert Subgroups wurden innerhalb der DSK intensiv diskutiert. Nach einigen Änderungen der Entwürfe konnte auch Deutschland dem endgültigen Beschluss zustimmen. Der EDSA verabschiedete seine Stellungnahme 28/2024 zu Rechtsfragen von LLM am 17. Dezember 2024. (https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_de). Zu Datenschutzfragen von Systemen Künstlicher Intelligenz, insbesondere LLM siehe auch die Kap. 5.1 und Kap. 8.1.

2.2
Genehmigung von verbindlichen konzerninternen Datenschutzvorschriften

Im zurückliegenden Berichtsjahr lag zudem erneut ein weiterer Fokus meiner Tätigkeit auf den europaweiten Kooperationsverfahren zur Genehmigung von verbindlichen internen Datenschutzvorschriften nach Art. 47 DS-GVO (sog. „Binding Corporate Rules“, kurz: BCR). So konnte im Berichtszeitraum etwa das Genehmigungsverfahren für die BCR für Verantwortliche und für die BCR für Auftragsverarbeiter der Infosys Germany Holding GmbH, für das ich europaweit federführend als sog. „BCR Lead“ zuständig bin und das ich gemeinsam mit den Co-Prüfern der italienischen und irischen Datenschutzaufsicht über die letzten Jahre sehr intensiv begleitet habe, mit positiven Stellungnahmen des EDSA (Stellungnahmen 24/2024 und 25/2024) und meinem Genehmigungsbescheid abgeschlossen werden. Umgekehrt habe ich auch in einer Vielzahl dieser europaweiten BCR-Prüfverfahren andere europäische Datenschutzaufsichtsbehörden als Co-Prüfer bei den sehr umfangreichen und komplexen Prüfungen unterstützt. Viele dieser BCRs werden im kommenden Jahr dem EDSA zur Stellungnahme nach Art. 64 Abs. 1 Buchst. f DS-GVO vorgelegt werden können, womit für weitere globale Unternehmensgruppen und Konzerne taugliche Transferinstrumente für konzerninterne Datenübermittlungen (in Drittländer) zur Verfügung stehen werden.

3. Verfahren vor Gerichten und zur Verhängung von Geldbußen

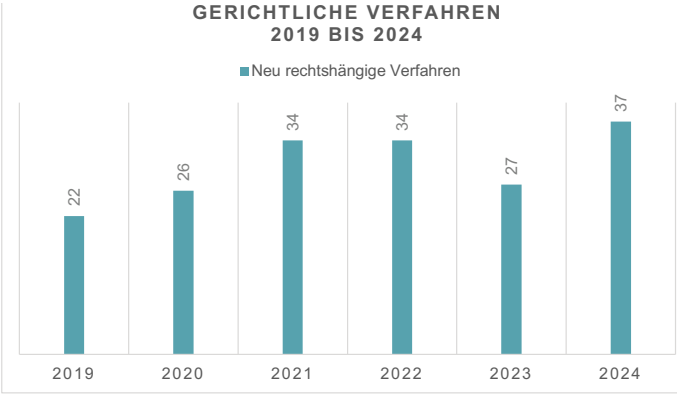
Die DS-GVO hat dazu geführt, dass Gerichts- und Sanktionsverfahren für die Tätigkeit der Datenschutzaufsichtsbehörden an Bedeutung zunehmen (s. 51. Tätigkeitsbericht Kap. 1). Auch im Berichtszeitraum ist die Zahl der Gerichtsverfahren (Kap. 3.1) und der Verfahren zur Verhängung einer Geldbuße (Kap. 3.2) jeweils weiter angestiegen. Urteile des EuGH und des Verwaltungsgerichts Wiesbaden haben die verfahrensrechtliche Stellung der Aufsichtsbehörden gestärkt und für mehr Rechtssicherheit gesorgt.

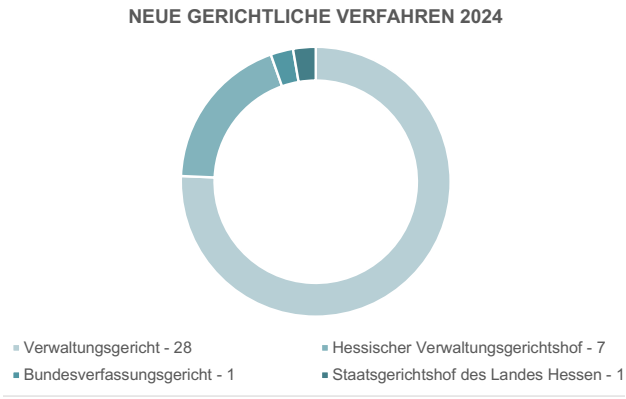
3.1 Gerichtsverfahren

Das Jahr 2024 war ein intensives Jahr im Bereich der gerichtlichen Verfahren. Im Berichtsjahr ist nicht nur die Zahl der Gerichtsverfahren wieder angestiegen, sondern auch der Umfang der Verfahren nahm zu. Zudem fällte der Europäische Gerichtshof (EuGH) in der Rechtssache C-768/21, der eine verwaltungsgerichtliche Klage gegen mich zugrunde liegt, eine bedeutende Entscheidung zum Ermessen der Aufsichtsbehörden.

In diesem Jahr war ich erstmals in 37 neue Verfahren involviert. Hierzu zählen überwiegend Klagen vor dem Verwaltungsgericht Wiesbaden sowie einige Rechtsmittel gegen Beschlüsse des Verwaltungsgerichts vor dem Hessischen Verwaltungsgerichtshof. Zudem erhielt ich erstmals im Rahmen einer Grundrechtsklage gegen eine gerichtliche Entscheidung Gelegenheit zur Stellungnahme.

Einen detaillierten Überblick bieten die nachfolgenden Übersichten:





Auch wenn die Verfahrensbelastung auf den ersten Blick zunächst überschaubar erscheint, war die Ressourcenplanung in diesem Jahr eine besondere Herausforderung. In den Verfahren vor dem Verwaltungsgericht standen überwiegend Entscheidungen oder Arbeitsweisen meiner Behörde im Streit. Aus datenschutzrechtlicher Sicht kristallisierten sich zwar keine konkreten Themenschwerpunkte heraus, jedoch stieg die Zahl der Verfahren weiter an, die durch sogenannte Vielkläger oder mit unklarem Klageziel initiiert wurden. Diese Streitigkeiten zeichneten sich im Wesentlichen durch sehr umfangreiche und weitgehend substanzlose Vorträge der jeweiligen Klägerinnen und Kläger aus.

Insgesamt konnten 20 Vorgänge im Bereich der Gerichtsverfahren abgeschlossen werden. Die Zahl der am Jahresende insgesamt noch offenen gerichtlichen Verfahren liegt bei 56. Die Gerichte haben in diesem Jahr keine meiner Abschlussentscheidungen aufgehoben oder abgeändert oder mich zum Tätigwerden verurteilt. Gleichwohl sind gerichtliche Entscheidungen nicht nur für die Arbeitsweise meiner Behörde von großer Bedeutung, denn sie haben maßgeblichen Einfluss auf die Verwaltungspraxis der Datenschutzaufsichtsbehörden insgesamt. In der folgenden Zusammenstellung findet sich eine Auswahl wichtiger Entscheidungen des Jahres 2024.

EuGH zum Ermessen der Aufsichtsbehörden

Nachdem der EuGH im Vorjahr in den verbundenen Rechtssachen C-26/22 und C-64/22 zum Charakter von Beschwerden nach Art. 77 DS-GVO bei der Datenschutzaufsichtsbehörde geurteilt hatte, hatte sich das oberste rechtsprechende Organ der Europäischen Union in diesem Jahr mit einer weiteren Vorlage zur Vorabentscheidung des Verwaltungsgerichts Wiesbaden

zu befassen, an der ich als Beklagter des Ausgangsverfahrens beteiligt war. Inhaltlich betraf die Vorlagefrage das aufsichtsbehördliche Ermessen. Mit seinem Urteil vom 26. September 2024 (C-768/21) äußerte sich der EuGH zu der umstrittenen Frage, ob die Datenschutzaufsichtsbehörde in jedem Fall verpflichtet ist, eine Geldbuße oder eine andere in Art. 58 Abs. 2 DS-GVO genannte Abhilfemaßnahme zu ergreifen, wenn sie einen Datenschutzverstoß feststellt. Im Ergebnis hat der EuGH dies verneint und so Befugnisse und Pflichten der Aufsichtsbehörden weiter konturiert.

Dem Urteil ging eine an mich gerichtete Beschwerde der betroffenen Person gegen eine Sparkasse voraus. Dieser lag zugrunde, dass eine Mitarbeiterin der Sparkasse mehrfach unberechtigt auf Personenstammdaten sowie Umsatzdaten des Klägers zugegriffen hatte. Zwar meldete das Finanzinstitut die Datenschutzvorfälle meiner Behörde gemäß Art. 33 DS-GVO, von der Benachrichtigung des Klägers nach Art. 34 DS-GVO sah die Sparkasse jedoch ab, weil nach dortiger Einschätzung kein hohes Risiko für die Rechte und Freiheiten des Klägers bestand. Die Sparkassenmitarbeiterin, gegen die auch Disziplinarmaßnahmen ergriffen wurden, hatte bestätigt und zugesichert, die eingesehenen Daten nicht weiterverarbeitet zu haben sowie ein solches Verhalten künftig zu unterlassen. Nachdem der Kläger von den unberechtigten Zugriffen durch eine Nachfrage bei der Sparkasse erfahren hatte, wandte er sich an mich und zeigte einen Verstoß gegen die Benachrichtigungspflicht aus Art. 34 DS-GVO an. Gleichzeitig monierte er auch die Speicherdauer für Zugriffsprotokolle sowie das Konzept der Zugriffsberechtigung bei der Sparkasse.

Nach eingehender Befassung und Prüfung gab mir der zu beurteilende Fall keinen Anlass, eine Geldbuße zu verhängen oder eine andere in Art. 58 Abs. 2 DS-GVO genannte Abhilfemaßnahme gegen die Sparkasse zu ergreifen. Unter anderem hatte ich im Rahmen der Beschwerdebearbeitung auf eine Anpassung der Speicherdauer für Zugriffsprotokolle hingewirkt und im Ergebnis einen Verstoß gegen Art. 34 DS-GVO verneint. Hiergegen klagte der Kläger vor dem Verwaltungsgericht Wiesbaden. Er war der Auffassung, dass ich zur Verhängung einer Geldbuße verpflichtet sei, weil mir kein Entschließungsermessen, sondern nur ein Auswahlermessen bezüglich der nach Art. 58 Abs. 2 DS-GVO zu ergreifenden Maßnahmen zustehe.

Der EuGH stellte mit seinem Urteil klar, dass weder aus Art. 58 Abs. 2 DS-GVO noch aus Art. 83 DS-GVO abgeleitet werden kann, dass Datenschutzaufsichtsbehörden verpflichtet wären, in jedem Fall, wenn sie eine Verletzung des Schutzes personenbezogener Daten feststellen, eine Abhilfemaßnahme zu ergreifen. Die Verpflichtung der Aufsichtsbehörde ist gerade darin zu sehen, in geeigneter Weise zu reagieren, um der festgestellten Unzulänglichkeit

abzuhelfen (Rn. 41). Gleichzeitig lehnt der EuGH ein subjektives Recht des Beschwerdeführers ab, von den Aufsichtsbehörden ein bestimmtes Einschreiten gegen den Verantwortlichen fordern zu können – insbesondere auch nicht die Verhängung einer Geldbuße. Insoweit schloss sich das Gericht den Schlussanträgen des Generalanwalts Priit Pikamäe an.

Folglich besteht für die Aufsichtsbehörde bei festgestellten Datenschutzverstößen nicht nur ein Auswahlermessen hinsichtlich der einzelnen Abhilfemaßnahmen („Wie"), sondern auch ein Entschließungsermessen bezüglich des „Ob" einer Maßnahme. Tätigwerden im Sinne von Art. 58 Abs. 2 DS-GVO müssen Datenschutzaufsichtsbehörden nämlich nur, wenn das Ergreifen einer oder mehrerer Abhilfemaßnahmen unter Berücksichtigung aller Umstände des konkreten Falles geeignet, erforderlich und verhältnismäßig ist, um der festgestellten Unzulänglichkeit abzuhelfen und die umfassende Einhaltung der DS-GVO zu gewährleisten (Rn. 42). Der Katalog des Art. 58 Abs. 2 DS-GVO sowie die Vorschrift des Art. 83 DS-GVO zielen darauf ab sicherzustellen, dass die Verarbeitung personenbezogener Daten entsprechend der Vorgaben der Verordnung erfolgt und etwaige Verstöße gegebenenfalls durch Abhilfemaßnahmen wieder in Einklang mit dieser gebracht werden. Nach dem EuGH kann das Ergreifen einer Abhilfemaßnahme daher „*ausnahmsweise und unter Berücksichtigung der besonderen Umstände des konkreten Falles nicht geboten sein*", *„sofern der Situation, die einen Verstoß gegen die DS-GVO begründete, bereits abgeholfen wurde, die Verarbeitung personenbezogener Daten im Einklang mit dieser Verordnung durch den hierfür Verantwortlichen gewährleistet ist"* (Rn. 46).

Die Formulierungen des Urteils legen zunächst nahe, dass die Aufsichtsbehörde, nachdem sie sich mit aller gebotenen Sorgfalt mit der betreffenden Beschwerde befasst hat, nur in Ausnahmefällen von Abhilfemaßnahmen absehen kann (Rn. 37, 43, 46). Tatsächlich treten derartige Konstellationen, in der das Ergreifen einer Maßnahme nach Art. 58 Abs. 2 DS-GVO zur Durchsetzung der DS-GVO nicht mehr sinnvoll erscheint, in der alltäglichen Arbeit meiner Behörde häufiger auf.

Es ist daher begrüßenswert, dass sich nach Auffassung des EuGH die aufsichtsbehördliche Entscheidung über das „Ob" des Ergreifens von Abhilfemaßnahmen an der konkreten Situation ausrichten lässt. Die Entscheidung gibt meiner Behörde die nötige Flexibilität, die umfassende Einhaltung der DS-GVO zu überwachen und weiterhin einzelfallbezogen auf Verstöße zu reagieren.

VG Wiesbaden zum Missbrauch prozessualer Rechte

In einem weiteren Verfahren, an dem ich als Beklagter beteiligt war, äußerte sich das Verwaltungsgericht Wiesbaden in seinem Beschluss vom 5. Februar 2024 (6 K 1/24.WI) zu einem Vielkläger und entsprechenden Kriterien für den Umgang mit missbräuchlichen oder offensichtlich sinnlosen Anträgen gegenüber Gerichten und anderen öffentlichen Stellen.

Der Kläger hatte sich in der Vergangenheit bereits mit zahlreichen Eingaben an mich gewendet, zudem ist er auch als Vielkläger nicht nur in Hessen bekannt. Ende 2023 übersandte mir der Kläger ein Schreiben zur Kenntnisnahme, in dem er auf eine Entscheidung des Bundesverfassungsgerichts (1 BvR 2368/06) aus dem Jahr 2007 verwies und dabei lediglich mitteilte, dass „*die Videoüberwachung klar unzulässig sein*“ dürfte. Seinem Anliegen fügte der Kläger zwei weitere als Klage bezeichnete Dokumente bei. Diese Klagen waren jedoch nicht gegen mich gerichtet, sondern führten als Klagegegner das Land Hessen sowie eine hessische Stadt auf. Aufgrund der Unklarheit der Schilderung stellte ich das Anliegen des Klägers zunächst zurück und verwies den Kläger darauf, dass er sich nach Abschluss der Klageverfahren im Bedarfsfall erneut am mich wenden könne. Hiergegen klagte der Kläger vor dem Verwaltungsgericht Wiesbaden. Das Verwaltungsgericht Wiesbaden stellte das Verfahren ein und führte dabei zusätzlich aus, dass die Klage sowohl unzulässig als auch unbegründet sei.

In seiner Begründung schließt sich das Gericht der Rechtsprechung der Verwaltungs-, Sozial- und Finanzgerichte sowie des Bundesgerichtshofs an, wonach die Rechtsschutzgarantie nicht den Anspruch umfasst, eine förmliche Entscheidung auf Eingaben zu erhalten, wenn diese missbräuchlich sind oder keinen substanziellen Gehalt aufweisen oder erkennbar auf die Überlastung der Behörden abzielen. Sofern der systematische Missbrauch prozessualer Rechte einer Person in einer Vielzahl von Fällen nachgewiesen ist, spricht eine Vermutung dafür, dass auch den künftigen Eingaben dieser Person Rechtsmissbrauch zugrunde liegt. Um der Verpflichtung zur Rechtsschutzgewährung nach Art. 19 Abs. 4 GG in diesen Fällen zu genügen, ist eine formlose Prüfung ausreichend, ob der Person für neu vorgebrachte Anliegen entgegen der bestehenden Missbrauchsvermutung ein Mindestmaß an berechtigtem Rechtsverfolgungsinteresse zur Seite steht (BVerfG, Beschluss vom 19. April 2021 – 1 BvR 2552/18, juris, Rn. 7). Sofern ein Mindestmaß an berechtigtem Rechtsverfolgungsinteresse erkennbar ist, wird die Eingabe als reguläres Verfahren fortgeführt. Andernfalls wird der Vorgang ohne weitere Maßnahmen geschlossen. Dies gilt auch, wenn sich zu einem späteren Zeitpunkt herausstellt, dass ein Mindestmaß an berechtigtem Rechtsverfolgungsinteresse nicht besteht.

Die Entscheidung betrifft primär das Recht auf effektiven Rechtsschutz. Dennoch ist der Beschluss des Verwaltungsgerichts auch für die behördliche Arbeit von besonderer Bedeutung, denn inhaltlich tangiert der entschiedene Fall auch das Spannungsfeld zwischen dem Recht auf Beschwerde nach Art. 77 DS-GVO und das hieraus resultierende Pflichtenprogramm für meine Behörde.

Als sogenannter Vielkläger verklagt der Kläger unter anderem auch Behörden, denen er keine Gelegenheit gibt, sich mit seinem Anliegen näher zu befassen, sofort. Aus der Entscheidung des Verwaltungsgerichts folgt, dass auch eine Behörde sich nicht uneingeschränkt mit den Wiederholungs- oder Missbrauchsanträgen auseinandersetzen muss. Hierzu führte das Verwaltungsgericht zum Verhaltensmuster des Klägers aus:

> „[…] Häufig schickt er allgemein gehaltene Äußerungen mit unklaren und oft unlogischen Inhalten, die mehr Verwirrung stiften, als dem Empfänger einen konkreten Handlungsbedarf aufzuzeigen. Die daher oft knappe Bescheidung, die in der Regel nicht über eine Eingangsbestätigung hinausgeht, nimmt der Kläger zum Anlass, mit einer Klage zu antworten. Fast alle Eilanträge und Klagen, soweit über sie in der Sache entschieden wurde, wurden wegen mangelnder behördlicher Vorbefassung abgelehnt oder abgewiesen […].
>
> Es hätte nach der Antwort der Behörde am Kläger gelegen, gegenüber der Behörde darzulegen, warum sein Verlangen nicht bis zur Entscheidung über die bereits beim Verwaltungsgericht Frankfurt am Main anhängigen Klagen in Sachen Videoüberwachung warten kann. Außergerichtliche Lösungen oder gerichtliche Konfliktbeilegungen strebt der Kläger aber weder hier noch andernorts an. Statt sich zunächst in der Sache zu erkundigen, den Standpunkt der Gegenseite zu erfragen, zu prüfen, ob die eigene Rechtsauffassung zutrifft oder möglicherweise rechtsirrig ist, ist er allein darauf aus, eine Streitlage zu konstruieren, die er sofort vor Gericht bringt. […]“

In der Sache stellte das Gericht klar, dass kein Anspruch des Klägers dahingehend besteht, dass meine Behörde eine Großstadt systematisch „begeht“. Eine solche Tätigkeit wäre mit vertretbarem Aufwand auch weder möglich noch verhältnismäßig. Diese Klarstellung ist sehr zu begrüßen, denn sie erlaubt mir, offensichtlich missbräuchliche und unsubstantiierte Eingaben zurückzustellen, die ein hinreichendes Maß an Geordnetheit und Bestimmtheit vermissen lassen, um die mir zur Verfügung stehenden Ressourcen sinnvoll einzusetzen und mich auf meine eigentlichen Aufgaben zu konzentrieren.

Daneben hatte der Kläger einen gleichlautenden Eilantrag gestellt, der mit Beschluss vom 5. Februar 2024 (6 L 2/24.WI) durch das Verwaltungsgericht ebenfalls abgelehnt wurde. Flankiert wurden die vom Kläger initiierten Verfahren von zahlreichen Befangenheitsgesuchen sowie gesetzlich nicht vorgesehenen „Rechtsmitteln“. Auch der Hessische Verwaltungsgerichtshof sah

in dem Verhalten des Klägers ein Desinteresse am Klageziel und erkannte, dass es dem Kläger vielmehr darum gehe, seinen Verfahrensgegnern durch die Überhäufung mit ohne jede prozessuale Sorgfalt geführten Verfahren einen Schaden durch Verschwendung von Arbeitskapazitäten zuzufügen. Zuletzt hatte der Kläger den Staatsgerichtshof des Landes Hessen mit einer Grundrechtsklage angerufen.

3.2
Verfahren über die Verhängung von Geldbußen

Die Palette der im Rahmen von Geldbußenverfahren von mir verfolgten datenschutzrechtlichen Verstöße war im Berichtsjahr erneut sehr bunt und vielfältig. Im Mittelpunkt der Bearbeitung standen insbesondere Zuwiderhandlungen im Gesundheitsbereich, Verstöße im Zusammenhang mit unrechtmäßiger Werbung sowie erhebliche Verletzungen von Betroffenenrechten.

Geldbußenverfahren in Zahlen

Insgesamt leitete ich im Berichtsjahr 46 neue Geldbußenverfahren ein. Damit bewegt sich die Zahl der neuen Fälle etwa auf dem Niveau der letzten beiden Jahre. Der Großteil der eingeleiteten Verfahren beruht auf den zuvor geführten Verwaltungsverfahren, die durch Individualbeschwerden initiiert wurden. Ein weiterer Teil der Vorgänge erhielt ich von einer Staatsanwaltschaft oder einer Polizeibehörde, nachdem diese die zuvor geführten strafrechtlichen Ermittlungen eingestellt und den Vorgang an mich zur Verfolgung in eigener Zuständigkeit abgegeben hatten.

Anlässlich der festgestellten Verstöße verhängte ich 2024 insgesamt 47 einzelne Geldbußen. Das unten abgebildete Balkendiagramm zeigt, wie die verhängten Sanktionen sich über die verschiedenen Branchen verteilen. Der Gesamtbetrag der festgesetzten Geldbußen belief sich im Berichtsjahr auf einen Betrag von 544.986 € und erreichte damit ein Rekordhoch.

Verstöße im Gesundheitswesen

Wie auch schon in den Vorjahren bildete die Verfolgung von Datenschutzverstößen im Gesundheitsbereich einen der Schwerpunkte meiner Sanktionstätigkeit. Im Berichtsjahr habe ich mehrere Arztpraxen wegen verschiedener Datenschutzverstöße sanktioniert. Zwei Beispiele:

In zwei Verfahren gegen Arztpraxen habe ich mehrere datenschutzrechtliche Verstöße im Zusammenhang mit der Veröffentlichung von Patientendaten im Rahmen von Google-Rezensionen festgestellt. Dabei haben die jewei-

ligen Praxisinhaber in zahlreichen Fällen auf negative Bewertungen zur Praxis auf www.google.com öffentlich reagiert und dabei Patienten- bzw. Behandlungsdaten offenbart. In manchen Fällen wurden Patientinnen und Patienten mit Klarnamen angesprochen, obwohl sie ihre Bewertung zuvor unter einem Pseudonym abgegeben hatten. In anderen Fällen wurden Behandlungsdetails, Diagnosen, Krankheitsepisoden, Befunde, Medikationen, Verordnungen sowie weitere Angaben zur Behandlung, die über die seitens der Patientinnen und Patienten selbst genannten Daten hinausgingen, veröffentlicht. Ein solches Verhalten der Ärzte verstößt gegen den Grundsatz der Rechtmäßigkeit nach Art. 5 Abs. 1 Buchst. a i. V. m. Art. 6 Abs. 1 und Art. 9 Abs. 1 DS-GVO.

Die festgestellten Zuwiderhandlungen habe ich in einem Fall mit einer Geldbuße in Höhe von insgesamt 3.700 € sanktioniert. In einem weiteren Verfahren habe ich einen Bescheid über eine Geldbuße in Höhe von insgesamt 3.300 € erlassen. Beide Entscheidungen sind rechtskräftig geworden.

Im Rahmen der Zumessung der Geldbußen habe ich in beiden Fällen unter anderem schärfend berücksichtigt, dass umfangreiche gesundheitsbezogene Informationen einem unbegrenzten Adressatenkreis im Internet öffentlich gemacht wurden. Dabei ist jedem Arzt bereits durch seine Eigenschaft als Berufsgeheimnisträger bekannt, dass Angaben zu Patientinnen und Patienten vertraulich zu behandeln sind. Dennoch wurden die Verstöße vorsätzlich begangen. Mildernd habe ich dagegen berücksichtigt, dass die Ärzte den Vorfall jeweils vollständig eingeräumt, mit mir kooperativ zusammengearbeitet und den Verstoß umgehend abgestellt haben, indem sie die Kommentare gelöscht haben.

In einem weiteren Fall bewahrte eine Ärztin Patientenunterlagen unsachgemäß auf, so dass es zu einer Offenlegung von Patientendaten gegenüber Dritten kam. Die Ärztin beschäftigte einen Praxismanager, der für die wesentlichen administrativen Aufgaben zuständig war. Unter anderem erstellte er Rechnungen und hatte hierfür Zugang zu Patientenakten. Seit der Corona-Pandemie erledigte der Praxismanager diese Aufgaben auch im Homeoffice. Hierfür durfte er die Ordner mit den Patientenunterlagen in seinem Heimbüro aufbewahren. Durch einen externen Hinweis hatte ich Kenntnis davon erlangt, dass diese Dokumente in offenen Regalen verwahrt wurden und das Arbeitszimmer nicht durchgehend abgeschlossen war. Beispielsweise legten Gäste während einer Feier die Jacken und Handtaschen dort ab, so dass die Möglichkeit bestand, dass auch unbefugte Dritte Zugang zu den Patientenakten hatten. Ich konnte ermitteln, dass die Akten u. a. Informationen zu Vorerkrankungen, Medikation und Allergien enthielten.

Darüber hinaus bat der Praxismanager seine Lebensgefährtin, mit ihrem privaten Smartphone Aufnahmen von Ausgangsrechnungen aus den Patientenunterlagen zu erstellen und per WhatsApp an ihn zu senden. Hintergrund dessen war, dass die Lebensgefährtin spontan mit dem Pkw, in dem sich die Patientenunterlagen befanden, eine längere Reise angetreten hatte. Da der Praxismanager die Unterlagen jedoch für einen am darauffolgenden Tag geplanten Termin mit dem Steuerberater benötigte, wurden ihm die Dokumente auf diese Weise zugesandt.

Die festgestellten Verstöße gegen den Grundsatz der Vertraulichkeit gemäß Art. 5 Abs. 1 Buchst. f i. V. m. Art. 32 DS-GVO sowie gegen den Grundsatz der Rechtmäßigkeit gemäß Art. 5 Abs. 1 Buchst. a i. V. m. Art. 9 Abs. 1 i. V. m. Art. 6 Abs. 1 DS-GVO waren der Ärztin zuzurechnen. Da zahlreiche Gesundheitsdaten betroffen waren, die dem besonderen Schutzbereich des Art. 9 Abs. 1 DS-GVO unterfallen, war von größeren Beeinträchtigungen für betroffene Personen auszugehen. Die Praxisinhaberin, als Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO, stellte keine hinreichenden erforderlichen technischen und organisatorischen Maßnahmen sicher und konnte die Vertraulichkeit der Datenverarbeitung nicht gewährleisten.

Gegen die Praxisinhaberin habe ich eine Geldbuße in Höhe von 2.500 € verhängt. Bei der Zumessung der Geldbuße habe ich unter anderem die fahrlässige Begehungsweise der Zuwiderhandlung sowie die im Nachgang des Verstoßes ergriffenen Maßnahmen, wie die Anschaffung von abschließbaren Aktenschränken und einem Tresor sowie erneute datenschutzrechtliche Sensibilisierung, mildernd berücksichtigt. Erschwerend habe ich dagegen insbesondere den Umfang der rechtswidrigen Datenverarbeitung und die Sensitivität der betroffenen Daten gewertet.

Verstöße im Zusammenhang mit Werbung

Auch im Berichtszeitraum 2024 waren einige Verstöße im Zusammenhang mit unrechtmäßiger Werbung Gegenstand von Geldbußenverfahren. Insbesondere habe ich Sanktionen wegen Verarbeitung von Daten zu Werbezwecken ohne Rechtsgrundlage, Nichtberücksichtigung von Werbewidersprüchen und fehlenden Hinweise auf das Werbewiderspruchsrecht der betroffenen Personen verhängt.

In einem Verfahren gegen ein Unternehmen aus der IT-Branche erhielt der Beschwerdeführer, ohne dass er jemals Kunde des Unternehmens war oder sich für Werbe-E-Mails oder Newsletter angemeldet hatte, mehrere E-Mails mit werblichem Inhalt. Für Akquisemaßnahmen wurden durch Auswertung und Zusammenführen öffentlich zugänglicher und im Internet verfügbarer Informationen geeignete Empfängerunternehmen ausgewählt. Insgesamt

wurden im Rahmen der einmalig durchgeführten E-Mail-Kampagne über 2.700 Personen angeschrieben, wobei ein Teil der E-Mail-Adressen nicht personenbezogen war. Für die beschriebene Akquisemaßnahme hatte das Unternehmen einen Auftragsverarbeiter engagiert, der die datenschutzrechtliche Zulässigkeit der Werbemaßnahme zusicherte. Eine eigene datenschutzrechtliche Prüfung der geplanten Kampagne führte der Verantwortliche nicht durch. Da der Auftragsverarbeiter sich an seinen Auftrag gehalten hatte, waren seine Handlungen dem Verantwortlichen zuzurechnen (vgl. EuGH, Urteil vom 5.Dezember 2023, C-683/21).

Das Vorgehen des Unternehmens war nicht rechtmäßig, da für die Verarbeitung von personenbezogenen Daten keine Rechtsgrundlage vorlag. Die per E-Mail angeschriebenen Personen hatten für die Kontaktaufnahme zu Werbezwecken keine Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 DS-GVO erteilt. Die Verarbeitung konnte auch nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden, da die Voraussetzungen zur Zulässigkeit von E-Mail-Werbung gemäß § 7 Abs. 2 Nr. 2 UWG nicht erfüllt waren und die wirtschaftlichen Interessen des Unternehmens nicht als berechtigte Interessen herangezogen werden konnten (s. hierzu auch 52. Tätigkeitsbericht 2023, Kap. 9.2, S. 144 ff.).

Zur Sanktion des Verstoßes habe ich eine Geldbuße in Höhe von 10.000 € gegen das Unternehmen verhängt. Bei der Zumessung habe ich entsprechend der Leitlinien des EDSA für die Berechnung von Geldbußen unter Zugrundelegung des Jahresumsatzes des Unternehmens sämtliche weiteren Umstände des Falls in die Bewertung einbezogen. Mildernd habe ich insbesondere berücksichtigt, dass das Unternehmen zum ersten Mal datenschutzrechtlich auffällig geworden war, wenige Daten der jeweiligen Personen betroffen waren und diesen Personen bis auf die Unannehmlichkeiten und den Zeitaufwand kein Schaden entstanden ist. Darüber hinaus habe ich zu Gunsten des Unternehmens gewertet, dass es die Zuwiderhandlung fahrlässig begangen und konstruktiv mit mir zusammengearbeitet hatte.

Nichtbefolgung der Anweisung der Datenschutzaufsichtsbehörde

Bereits im 52. Tätigkeitsbericht 2023 informierte ich über die Sanktionierung von Verstößen gegen die Mitwirkungspflicht von Verantwortlichen gemäß Art. 31 DS-GVO (s. 52. Tätigkeitsbericht 2023, Kap. 3.3, S. 37 ff.). In diesem Jahr erreichte das nichtkooperative Verhalten eines Websitebetreibers eine neue Eskalationsstufe, indem er meine förmliche Anweisung nach Art. 58 Abs. 2 Buchst. d DS-GVO ignorierte.

Bei einer Überprüfung der Internetpräsenz eines freiberuflichen Websitebetreibers stellte ich fest, dass im Rahmen des Online-Angebots keine Unterrichtung der Seitennutzenden über die bei den betroffenen Personen erhobenen personenbezogenen Daten stattfindet. Die Website enthielt überhaupt keinen Datenschutzhinweis mit den Informationen, die nach Art. 13 DS-GVO für die Seitennutzenden angeboten werden müssen. Dabei hielt der Verantwortliche innerhalb des Online-Angebots mehrere Formulare bereit, mit denen er personenbezogene Daten erhebt sowie anschließend speichert und verwendet.

Nach erfolgloser Kontaktaufnahme des Verantwortlichen im Rahmen des Aufsichtsverfahrens wies ich diesen gemäß Art. 58 Abs. 2 Buchst. d DS-GVO förmlich an, detaillierte Datenschutzhinweise zur Verfügung zu stellen. Zeitgleich drohte ich für den Fall der Nichtbefolgung dieser Anweisung ein Zwangsgeld in Höhe von 2.000 € an. Obwohl die Anweisung bestandskräftig wurde, befolgte der Verantwortliche diese nicht. Daran änderten auch die Festsetzung und anschließende Beitreibung von weiteren zwei Zwangsgeldern in Höhe von jeweils 2.000 € nichts. Die Aufsichtsbehörde wurde vom Websitebetreiber weiterhin anhaltend ignoriert. Dieses Verhalten stellt einen geldbußenbewehrten Verstoß nach Art. 83 Abs. 5 Buchst. e DS-GVO i. V. m. Art. 58 Abs. 2 Buchst. d DS-GVO dar. Die festgestellten Verstöße sowie die nachhaltige nichtkooperative Haltung des Websiteanbieters nahm ich zum Anlass, zusätzlich zu den bereits verhängten Zwangsgeldern von insgesamt 6.000 € eine Geldbuße in Höhe von 10.000 € gegen den Verantwortlichen zu verhängen. Ein solch außerordentlich tiefgreifendes, unkooperatives Verhalten eines Verantwortlichen kommt zwar nur in wenigen Ausnahmefällen vor, kann jedoch nicht ohne spürbare Konsequenzen bleiben. Der Bescheid über die Festsetzung von Geldbußen ist inzwischen rechtskräftig.

Settlement-Verfahren

Ein umfangreiches Geldbußenverfahren gegen ein großes Unternehmen aus der Finanzbranche zeichnete sich dagegen durch ein einsichtiges und durchgehend kooperatives Verhalten der verantwortlichen Stelle aus und konnte letztendlich im Rahmen einer einvernehmlichen Verständigung beendet werden.

Dem Geldbußenverfahren lagen einige Individualbeschwerden zugrunde. Unter anderem konnte ich in mehreren Fällen Verstöße gegen Art. 15 i. V. m. Art. 12 Abs. 3 DS-GVO durch verspätete Erteilung von Datenauskünften an betroffene Personen feststellen. Darüber hinaus waren Verstöße gegen die Grundsätze (Art. 5 DS-GVO) sowie gegen die Rechtmäßigkeit (Art. 6 DS-GVO) der Verarbeitung Gegenstand des Verfahrens. So wurden beispielsweise

zum Teil sensible Kundenunterlagen an falsche Empfänger übermittelt oder Kunden telefonisch zu Werbezwecken angesprochen, obwohl diese keine erforderliche Einwilligung erteilt hatten.

Das Unternehmen signalisierte von Beginn an volle Kooperationsbereitschaft. Im Verlauf des Verfahrens erfolgte eine umfangreiche Korrespondenz und es fanden mehrere Gespräche statt. Nachdem der Sachverhalt vollständig aufgeklärt und das Verfahren entscheidungsreif war, gab ich der Gegenseite im Rahmen eines persönlichen Termins die beabsichtigte Entscheidung bekannt. Gleichzeitig unterbreitete ich dem Unternehmen auf seinen Wunsch hin einen Settlement-Vorschlag. Dieser sah vor, dass ich der verantwortlichen Stelle im Falle einer geständigen Einlassung einen geldbußenmindernden Abschlag gewähre und das Verfahren zu zwei Verstößen aus Opportunitätsgründen einstelle. Das Unternehmen nahm den Vorschlag an. Es räumte die zu beurteilenden Verstöße ein und akzeptierte die beabsichtigte Festsetzung der Geldbußen. Das Geldbußenverfahren beendete ich anschließend mit einem Bescheid über die Festsetzung von Geldbußen in Höhe von insgesamt 496.000 € zuzüglich Gebühren. Die Abgabe der Settlement-Erklärung war nicht mit einem Rechtsmittelverzicht verbunden, so dass für das Unternehmen trotz der Verständigung die Möglichkeit bestand, Einspruch einzulegen. Der Bescheid über die festgesetzten Geldbußen wurde rechtskräftig.

Die Möglichkeit, das Geldbußenverfahren durch eine einvernehmliche Verständigung zu beenden, bot im vorliegenden Fall mehrere Vorteile wie die eingetretene Beschleunigung und Verkürzung des Verfahrens sowie die eingesparten Ressourcen meiner Behörde. Für die verantwortliche Stelle führte das Settlement insbesondere zu einem mindernden Abschlag der verhängten Sanktionen. Aus diesen Gründen wird das Instrument der Verständigung in datenschutzrechtlichen Geldbußenverfahren aktuell und voraussichtlich künftig häufiger von Aufsichtsbehörden und Verfahrensbeteiligten in Anspruch genommen.

An dieser Stelle ist es mir wichtig zu betonen, dass ein Settlement-Verfahren von Einsicht, Kooperation und einer vertrauensvollen Zusammenarbeit zwischen der verantwortlichen Stelle und der Aufsichtsbehörde abhängt, bei der die Positionen offen ausgetauscht und die Zusagen der Parteien jeweils eingehalten werden. Verständigungsgespräche dürfen nicht dazu führen, dass diese von Betroffenen als Hinhaltetaktik genutzt und zur Verfahrensverschleppung missbraucht werden.

Zusammenfassend ist festzuhalten, dass es sich in jedem Stadium des behördlichen Verfahrens – sowohl des Aufsichts- als auch des Geldbußenverfahrens – als lohnenswert erwiesen hat, mit mir zusammenzuarbeiten. Die Kooperation der verantwortlichen Stellen mit der Aufsichtsbehörde wird

gemäß Art. 82 Abs. 3 Buchst. f DS-GVO bei der Zumessung der Geldbußen mildernd berücksichtigt. Darüber hinaus ist es auch möglich, ein Verfahren über die Verhängung von Geldbußen im Rahmen einer Verständigung einvernehmlich zu beenden, was sowohl für die verantwortliche Stelle als auch für die Aufsichtsbehörde mit erheblichen Vorteilen und Erleichterungen verbunden ist.

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. Neuere Entwicklungen im Sicherheitsbereich führen dazu, dass diese Eingriffe umfangreicher und tiefgehender werden (Kap. 4.1). Diese Befugnisse sind jedoch gerade 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 zum Hessischen Verfassungsschutzgesetz (Kap. 4.2). Die Einhaltung der Voraussetzungen und Grenzen dieser Befugnisse war Gegenstand von Prüfungen bei Staatsanwaltschaften (Kap. 4.3) sowie bei Polizeibehörden und dem Landesamt für Verfassungsschutz (Kap. 4.5). Bei einem staatsanwaltschaftlichen Einstellungsbescheid war die Offenlegung personenbezogener Daten zu kritisieren (Kap. 4.4). Typosquatting bei der Hessischen Polizei führte zu Meldungen wegen Datenschutzverletzungen (Kap. 4.6).

4.1 Aktuelle Entwicklungen im Sicherheitsbereich

Zu den aktuellen datenschutzrechtlichen Entwicklungen im Sicherheitsbereich gehören verschiedene Gesetzgebungsverfahren auf Bundes- und Landesebene, die Entscheidung des Bundesverfassungsgerichts zur teilweisen Verfassungswidrigkeit des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) sowie die erneute Verfassungsbeschwerde gegen § 25a des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG), die Entschließung der DSK zur Gesichtserkennung sowie das Inkrafttreten der KI-Verordnung mit spezifischen Regelungen für Polizei- und Strafverfolgungsbehörden. Einen Schwerpunkt bildet die Novellierung des HSOG, die insbesondere die Ausweitung der Videoüberwachung im öffentlichen Raum, die Implementierung von gesetzlichen Möglichkeiten zum Einsatz von KI-Technologien und die Erweiterung der elektronischen Aufenthaltsüberwachung beinhaltet.

Überblick über die Entwicklungen im Berichtsjahr

Im Bereich der nationalen Gesetzgebung gab es sowohl auf Bundes- als auch auf Landesebene verschiedene Gesetzgebungsverfahren. Hierzu gehören der Entwurf der Bundesregierung zu einem Gesetz zur Verbesserung der Terrorismusbekämpfung (BT-Drs. 20/12806) sowie die Novellierung des HSOG durch den Gesetzentwurf für ein Gesetz zur Stärkung der Inneren Sicherheit in Hessen LT-Drs. 21/1151.

Das Bundesverfassungsgericht entschied mit Urteil vom 1. Oktober 2024 (1 BvR 1160/19), dass § 18 Abs. 1 Nr. 2 i. V. m. Abs. 2 Nr. 1 BKAG, soweit diese Vorschrift i. V. m. §§ 13 Abs. 3, 29 BKAG die Speicherung von Daten im polizeilichen Informationsverbund erlaubt, und § 45 Abs. 1 Satz 1 Nr. 4 BKAG nicht vereinbar mit dem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) sind. Aus dem Urteil ergibt sich folglich Anpassungsbedarf in den entsprechenden polizeirechtlichen Vorschriften.

Nach dem Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 zu automatisierten Datenanalyse (1 BvR 1547/19, 1 BvR 2634/20) hatte der hessische Gesetzgeber Anpassungen des § 25a HSOG unter Berücksichtigung der Vorgaben aus dem Urteil des Bundesverfassungsgerichts vorgenommen. Gegen diese Fassung wurde zwischenzeitlich erneut Verfassungsbeschwerde eingelegt.

Die DSK äußerte in ihrer Entschließung vom 20. September 2024 „Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden“ Zweifel an der Vereinbarkeit einiger bereits im Einsatz befindlicher Gesichtserkennungssysteme mit den einschlägigen rechtlichen Vorgaben und dem bestehenden engen gesetzgeberischen Spielraum. Verwiesen wird dabei auch auf die am 1. August 2024 in Kraft getretene KI-VO, die ihrerseits Grenzen für den Einsatz von Gesichtserkennungssystemen im öffentlichen Raum setzt.

Darüber hinaus beinhaltet die KI-VO eine Reihe an Vorschriften für den Einsatz von Künstlicher Intelligenz (KI) im Sicherheitsbereich, die von den Polizei- und Strafverfolgungsbehörden und dem Gesetzgeber zukünftig zu beachten sind. In Art. 113 KI-VO sind verschiedene Zeitpunkte für die Geltung der Verordnung vorgesehen: Grundsätzlich soll die KI-VO ab dem 2. August 2026 gelten, jedoch gelten einzelne Kapitel und Vorschriften schon ab dem 2. Februar 2025 und dem 2. August 2025 sowie Art. 6 Abs. 1 KI-VO erst ab dem 2. August 2027.

Novellierung des HSOG

Die o. g. Novellierung des HSOG erfolgte auf Grundlage eines Gesetzentwurfs der Fraktionen von CDU und SPD für ein Gesetz zur Stärkung der Inneren Sicherheit in Hessen vom 1. Oktober 2024 (LT-Drs. 21/1151) sowie eines Änderungsantrags der Fraktionen vom 5. Dezember 2024 (LT-Drs. 21/1448) und wurde im Berichtsjahr abgeschlossen.

Die Änderungen betreffen die §§ 1, 10, 12a, 14, 15d, 15e, 18, 21, 25a, 27, 31, 31a, 32, 35, 43b, 43c HSOG und sind am 19. Dezember 2024 sowie am 2. Februar 2025 in Kraft getreten. Ich konnte im Rahmen einer öffentlichen Anhörung im Innenausschuss des Hessischen Landtags lediglich zum ursprünglichen Gesetzentwurf und den darin enthaltenen Novellierungen Stellung nehmen (Ausschussvorlage INA 21/6 öffentlich vom 8. November 2024 Teil 1), da eine öffentliche Anhörung zum Änderungsantrag nicht durchgeführt wurde. Die von mir in meiner Stellungnahme geäußerten Bedenken wurden vom Gesetzgeber überwiegend nicht aufgegriffen. Die Neuregelungen, die auf Grundlage des Änderungsantrags erfolgt sind, beinhalten teilweise weitreichende Änderungen in den §§ 1, 10, 14, 15e, 21, 18, 25a, 27, 31a, 43b, 43c HSOG.

Die datenschutzrechtlich relevanten Novellierungen betreffen im Wesentlichen die Erweiterung der Videoüberwachung in § 14 HSOG, einschließlich der Schaffung einer Rechtsgrundlage für den Einsatz von biometrischer Echtzeit-Fernidentifizierung, die Einführung von Rechtsgrundlagen zum Einsatz von unbemannten Luftfahrtsystemen und zum Einsatz technischer Mittel gegen unbemannte Fahrzeugsysteme in §§ 15d und 15e HSOG, bei der Identitätsfeststellung in § 18 HSOG die Schaffung einer Rechtsgrundlage für Kontrollen in Bereichen, in denen per Gefahrenabwehrverordnung nach § 71 HSOG das Führen gefährlicher Gegenstände verboten oder beschränkt ist, den Einsatz von KI-Systemen bei der automatisierten Anwendung zur Datenanalyse in § 25a HSOG und die Erweiterung der elektronischen Aufenthaltsüberwachung in § 31a HSOG.

Bei der Darstellung der Novellierungen beschränke ich mich im Folgenden auf die kritischen und wichtigsten Änderungen in den §§ 14, 25a und 31a HSOG.

Videoüberwachung

Durch die Novellierung von § 14 HSOG wurden Änderungen in den Absätzen 1, 3, 3a und 4 vorgenommen sowie die Absätze 7 bis 11 neu hinzugefügt. Dadurch haben sich einige erhebliche Neuregelungen im Bereich der Videoüberwachung ergeben.

Erweiterung um sog. Angsträume und den unmittelbaren Nahbereich von Flughäfen

Durch die in § 14 Abs. 3 Satz 1 HSOG neu eingefügte Nr. 3 können nun auch öffentlich zugängliche Orte, sofern diese Orte aufgrund ihrer konkreten Lage, Einsehbarkeit und Frequentierung günstige Tatgelegenheiten für Straftaten bieten und deshalb anzunehmen ist, dass sie gemieden werden, sog. Angsträume, mittels Bildüberwachung offen beobachtet und aufgezeichnet werden. In meiner Stellungnahme hatte ich mit Hinweis auf die Verhältnismäßigkeit das Fehlen einer gesetzlich vorgeschriebenen Kriminalitätsanalyse zur Feststellung eines Kriminalitätsschwerpunktes für die Videoüberwachung von Angsträumen kritisiert und auf die Möglichkeit von zunächst weniger invasiven Maßnahmen, wie baulichen Veränderungen und die Schaffung von Lichtquellen, hingewiesen. Weiterhin habe ich angemerkt, dass der präventive Zweck einer Videoüberwachung zur Gefahrenabwehr nur erfüllt werden kann, wenn ausreichend Personal zur Verfügung steht, das die Bildübertragung konsequent im Auge behält und entsprechend reagieren kann. In Frage gestellt habe ich zudem, ob eine derartige in das Recht auf informationelle Selbstbestimmung eingreifende Maßnahme lediglich auf eine individuell empfundene Stärkung des Sicherheitsgefühls gestützt werden kann. Die Stärkung des Sicherheitsgefühls, der die Regelung laut Gesetzesbegründung dienen soll, zählt – auch in Verbindung mit Tatgelegenheitsstrukturen wie Lage, Einsehbarkeit und Frequentierung – nicht zu den Schutzgütern des Gefahrenabwehrrechts. Diese Bedenken wurden vom Gesetzgeber nicht aufgegriffen.

Der neue § 14 Abs. 3a Satz 2 HSOG erweitert die Vermutungsregelung in Absatz 3, dass die Voraussetzungen für eine Videoüberwachung in den im Gesetz genannten öffentlich zugänglichen Bereichen vorliegen, auf den unmittelbaren Nahbereich von Flughäfen. Bereits in meinen Stellungnahmen (vom 30. Juni 2022 und 27. April 2023) im Rahmen des Gesetzgebungsverfahrens zur letzten Novellierung des HSOG hatte ich den Begriff des „öffentlich zugänglichen Bereichs“ im Zusammenhang mit dem Flughafengelände als zu unbestimmt kritisiert, insbesondere im Hinblick auf die räumlichen Abgrenzungsprobleme des Flughafenbereichs. Die Verwendung der Formulierung „in unmittelbarer Nähe“ als weiterer unbestimmter Rechtsbegriff verstärkt diese Problematik nun. Problematisch ist darüber hinaus, dass durch den Verweis in Absatz 3a auf die Voraussetzungen in Absatz 3 Satz 1 für eine Videoüberwachung an öffentlich zugänglichen Bereichen in unmittelbarer Nähe von Flughäfen – als Vermutungsregelung/Beweislastumkehr mit kursorischer Prüfung – ebenfalls ein Kriminalitätsschwerpunkt oder eine konkrete Gefahr vorausgesetzt wird, was regelmäßig schwer zu begründen sein dürfte.

Erweiterung um besonders gefährdete Religionsstätten

§ 14 Abs. 4 wurde um den Begriff „besonders gefährdete Religionsstätten“ erweitert. Gerade bei Glaubenseinrichtungen kann es zu bestimmten Zeiten, bspw. bei Gottesdiensten und Gebeten, zu einer erhöhten Zahl von Besuchern kommen, die dann videoüberwacht werden. Hierzu hatte ich in meiner Stellungnahme darauf hingewiesen, dass im Zusammenhang mit der Religionsausübung besondere Kategorien personenbezogener Daten i. S. v. § 41 Nr. 15 Buchst. a) HDSIG von der Videoüberwachung betroffen sein können, weshalb bei der Datenverarbeitung spezifische Vorgaben zu beachten sind. Nach § 43 Abs. 1 HDSIG muss die Datenverarbeitung zur Aufgabenerfüllung unbedingt erforderlich sein und nach § 43 Abs. 2 HDSIG sind geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorzusehen.

Einsatz von Bodycams in Wohnungen, Absatz 6

§ 14 Abs. 6 Satz 3 HSOG ermöglicht den Einsatz von Bodycams nun auch in Wohnungen. Die neue Regelung ist mit erheblichen verfassungsrechtlichen Risiken verbunden, da umstritten ist, ob ein solcher Eingriff in die Unverletzlichkeit der Wohnung überhaupt gerechtfertigt werden kann (Problematik der Anwendbarkeit von Art. 13 Abs. 4 und 5 oder Abs. 7 GG), und der Einsatz von Bodycams in Wohnungen aktuell Gegenstand anhängiger Verfassungsklagen vor dem Bundesverfassungsgericht in Karlsruhe sowie dem Bayerischen Verfassungsgerichtshofs ist (s. die Stellungnahme von Zöller vom 2. Januar 2024, Vorlage 18/5076, S. 2, zu LT-Drs. 18/6909 und LT-Drs. 18/7881 in Rheinland-Pfalz).

Vor diesem Hintergrund hatte ich in meiner Stellungnahme angeregt, eine Regelung zur Evaluierung zu schaffen, wonach die Vorschrift nach einem gewissen Zeitraum auf die praktische Anwendung und ihre Auswirkungen geprüft werden sollte, so wie dies in anderen Landespolizeigesetzen der Fall ist (s. z. B. die Regelung zur Evaluierung in § 57 Abs. 9 SächsPVDG).

Mustererkennung und biometrische Echtzeit-Fernidentifizierung bei Überwachungsmaßnahmen

Die infolge des Änderungsantrags in § 14 HSOG neu eingefügten Absätze 8 bis 11 ermöglichen nunmehr Videoüberwachungsmaßnahmen u. a. durch Mustererkennung und intelligente Gesichtserkennungstechnik, die sog. biometrische Echtzeit-Fernidentifizierung. Die Erweiterung der Videoüberwachung erstreckt sich auf die Anwendungsalternativen in den Absätzen 1, 3, 3a und 4. Diese undifferenzierte Bezugnahme auf alle möglichen Videoüberwa-

chungsmaßnahmen des § 14 HSOG wird weder dem Eingriffsgewicht einer solchen Maßnahme noch den verfassungsrechtlichen Anforderungen an die Verhältnismäßigkeit einer derartigen Eingriffsnorm gerecht.

Der neu eingefügte § 14 Abs. 8 Satz 1 Nr. 1 und Nr. 2 erlaubt künftig den Einsatz von automatisierten Anwendungen zur Datenverarbeitung zur Erkennung und Auswertung von Bewegungsmustern, die auf die Begehung einer Straftat hindeuten, und Mustern bezogen auf Waffen i. S. d. § 1 Abs. 2 des Waffengesetzes, Messer oder gefährliche Gegenstände. Hier stellt sich die Frage, welche konkreten Bewegungs- oder Verhaltensmuster der automatisierten Auswertung und dem zum Einsatz kommenden Algorithmus zugrunde gelegt werden sollen, da die Norm dazu keine Regelungen enthält.

Durch den neu eingefügten § 14 Abs. 8 Satz 4 und Abs. 9 HSOG ermöglicht der Gesetzgeber neben der Mustererkennung auch den Einsatz biometrischer Echtzeit-Fernidentifizierung zur gezielten Suche oder Nachverfolgung von Personen zur Gefahrenabwehr. Grundsätzlich stellen Verfahren, bei denen biometrische Echtzeit-Fernerkennungssysteme dazu eingesetzt werden, Personen oder ihr Verhalten zu erkennen, um ihre Identifizierung ohne ihre aktive Mitwirkung wesentlich zu erleichtern, einen tiefgreifenden Grundrechtseingriff dar. Dieser Eingriff wird durch die Betroffenheit besonderer Kategorien personenbezogener Daten und eines Datenabgleichs in Echtzeit noch intensiviert. Zu berücksichtigen ist in diesem Zusammenhang bereits jetzt die KI-VO, wobei gemäß Art. 5 Abs. 1 Buchst. h) der Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken nur unter engen Voraussetzungen zugelassen wird und ansonsten zu den verbotenen Praktiken im KI-Bereich zählt.

Für den Einsatz nach § 14 Abs. 9 Satz 3 HSOG sieht das Gesetz vor, diesen auf das zeitlich und örtlich unbedingt erforderliche Maß zu beschränken. Aus datenschutzrechtlicher Sicht ist problematisch, dass im Gesetz nicht näher definiert wird, was unter einer zeitlichen und örtlichen Begrenzung konkret zu verstehen ist. Der Regelung mangelt es an dieser Stelle an der erforderlichen Bestimmtheit und Verhältnismäßigkeit.

Zudem sind in den neuen Regelungen keine spezifischen Löschfristen oder Vorgaben dafür enthalten, dass ein Mensch vor Ergreifen von Folgemaßnahmen die gewonnenen Ergebnisse noch einmal prüft und bewertet. Dies ist jedoch für die Nachvollziehbarkeit, Transparenz und spätere Kontrolle der Maßnahme unabdingbar. Ungeregelt ist daher die Frage, wie nach Abschluss der Maßnahmen mit den Ergebnissen, ggf. auch falsch-positiven Ergebnissen, verfahren werden soll.

§ 14 Abs. 10 normiert Protokollierungs- und Begründungspflichten, die bei der Durchführung einer biometrischen Echtzeit-Fernidentifizierung zu

berücksichtigen sind. Der neue Absatz 11 enthält Verfahrensregelungen, die im Wesentlichen die Anordnung der Maßnahme betreffen, wobei die Einzelheiten durch eine Verwaltungsvorschrift geregelt werden sollen. Hier ergibt sich vor dem Hintergrund der Wesentlichkeitstheorie die Problematik, inwieweit wesentliche Entscheidungen an die Exekutive delegiert werden können oder vom Gesetzgeber selbst zu regeln sind.

Im Ergebnis ist fraglich, ob die die von der KI-VO geforderten notwendigen und verhältnismäßigen Schutzvorkehrungen und Bedingungen für die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in ausreichendem Maße aufgreifen.

§ 14 HSOG

(1) Die Polizeibehörden können personenbezogene Daten, insbesondere durch den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen, auch über andere als die in den §§ 6 und 7 genannten Personen, bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass bei oder im Zusammenhang mit der Veranstaltung oder Ansammlung Straftaten oder nicht geringfügige Ordnungswidrigkeiten drohen. Die Unterlagen und die personenbezogenen Daten sind spätestens zwei Monate nach Beendigung der Veranstaltung oder Ansammlung zu vernichten oder zu löschen, soweit sie nicht zur Abwehr einer Gefahr, zur Verfolgung einer Straftat oder Ordnungswidrigkeit oder zur Strafvollstreckung benötigt werden. Eine Verarbeitung für andere Zwecke ist unzulässig. § 20 Abs. 8 bleibt unberührt. (…)

(3) Die Gefahrenabwehr- und die Polizeibehörden können öffentlich zugängliche Orte

1. *zur Abwehr einer Gefahr,*
2. *wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen, oder*
3. *sofern diese Orte aufgrund ihrer konkreten Lage, Einsehbarkeit und Frequentierung günstige Tatgelegenheiten für Straftaten mit erheblicher Bedeutung im Sinne des § 13 Abs. 3 Satz 1 bieten und deshalb anzunehmen ist, dass sie gemieden werden,*

mittels Bildübertragung offen beobachten und aufzeichnen. Ob die Voraussetzungen nach Satz 1 vorliegen, haben die Gefahrenabwehr- und die Polizeibehörden auf der Grundlage einer ortsbezogenen Lagebeurteilung unter besonderer Berücksichtigung der Verhältnismäßigkeit zu ermitteln und zu dokumentieren. 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. Diese Vermutung gilt auch für öffentlich zugängliche Bereiche in unmittelbarer Nähe von Flughäfen. Abs. 1 Satz 2 und 3 und Abs. 3 Satz 3 und 4 gelten entsprechend.

(4) Die Gefahrenabwehr- und die Polizeibehörden können mittels Bildübertragung offen beobachten und aufzeichnen

1. *zum Schutz besonders gefährdeter öffentlicher Einrichtungen oder Räumlichkeiten oder besonders gefährdeter Religionsstätten,*
2. *zur Steuerung von Anlagen zur Lenkung oder Regelung des Straßenverkehrs, soweit Bestimmungen des Straßenverkehrsrechts nicht entgegenstehen.*

Soweit der Inhaber des Hausrechts nicht Gefahrenabwehr- oder Polizeibehörde ist, gilt er im Fall des Satz 1 Nr. 1 als Gefahrenabwehrbehörde. Abs. 1 Satz 2 und 3 und Abs. 3 Satz 3 und 4 gelten entsprechend. (…)

(6) Die Gefahrenabwehr- und die Polizeibehörden können eine Person mittels Bild- und Tonübertragung durch den Einsatz körpernah getragener technischer Mittel

1. *kurzfristig offen technisch erfassen, wenn dies nach den Umständen zum Schutz von Beschäftigten der Gefahrenabwehr- und der Polizeibehörden oder von Dritten gegen eine Gefahr für Leib, Leben oder Freiheit erforderlich erscheint,*
2. *offen beobachten und dies aufzeichnen, wenn dies nach den Umständen zum Schutz von Beschäftigten der Gefahrenabwehr- und der Polizeibehörden oder von Dritten gegen eine Gefahr für Leib, Leben oder Freiheit erforderlich ist.*

Soweit es für die Durchführung von Maßnahmen nach Satz 1 unerlässlich ist, können personenbezogene Daten auch über dritte Personen erhoben werden. In Wohnungen sind Maßnahmen nach Satz 1 nur durch die Polizeibehörden und nur zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person zulässig. (…)

(7) Auf Maßnahmen nach Abs. 1 oder 6 ist in geeigneter Weise hinzuweisen, soweit diese nicht offenkundig sind oder Gefahr im Verzug besteht.

(8) Bei den Maßnahmen nach Abs. 1, 3, 3a und 4 dürfen automatisierte Anwendungen zur Datenverarbeitung zur Erkennung und Auswertung von

1. *Bewegungsmustern, die auf die Begehung einer Straftat hindeuten, oder*
2. *Mustern bezogen auf Waffen im Sinne des § 1 Abs. 2 des Waffengesetzes, Messer und gefährliche Gegenstände*

verwendet werden.

Sofern Muster nach Satz 1 erkannt werden, prüfen die Polizeibehörden unverzüglich, ob mit Straftaten mit erheblicher Bedeutung nach § 13 Abs. 3 Satz 1 in absehbarer Zeit mit hinreichender Wahrscheinlichkeit gerechnet werden kann. Liegen die Voraussetzungen nach Satz 2 vor, können die Polizeibehörden eine automatisierte Nachverfolgung der für das Vorliegen der Voraussetzungen nach Satz 2 verantwortlichen Personen durch ihre Kennzeichnung in den vorliegenden Bildübertragungen und -aufzeichnungen vornehmen.

Die Polizeibehörden können in Bezug auf die jeweils nachverfolgten Personen nach Satz 3 eine biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen anhand des Datenbestandes der polizeilichen Auskunfts- und Fahndungssysteme durchführen, wenn eine erhebliche gegenwärtige Gefahr für das Leben oder die körperliche Unversehrtheit einer Person vorliegt, sofern die Abwehr dieser Gefahr auf diese Weise unbedingt erforderlich ist.

(9) Die Polizeibehörden können zur Abwehr einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr einer terroristischen Straftat bei den Maßnahmen nach Abs. 1, 3, 3a und 4 die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zur gezielten Suche nach Personen, die diese Gefahr verursachen, durchführen, soweit die Abwehr dieser Gefahr auf diese Weise unbedingt erforderlich ist. Die Polizeibehörden können bei den Maßnahmen nach Abs. 1, 3, 3a und 4 die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen auch zur gezielten Suche nach im Datenbestand der polizeilichen Auskunfts- und Fahndungssysteme gespeicherten bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung und vermissten Personen durchführen, soweit die Suche auf diese Weise unbedingt erforderlich ist. Die biometrische Echtzeit-Fernidentifizierung nach Satz 1 und 2 darf nur zeitlich und örtlich auf das unbedingt erforderliche Maß begrenzt erfolgen.

(10) Die Durchführung der biometrischen Echtzeit-Fernidentifizierung unterliegt der ständigen Protokollierung, die die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, den Zeitpunkt ihres Einsatzes sowie die Organisationseinheit, einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, enthalten muss. Jeder Fall der biometrischen Echtzeit-Fernidentifizierung ist von der Anwenderin oder dem Anwender zu begründen. Die Einzelheiten des notwendigen Inhalts der Begründung werden in einer Verwaltungsvorschrift geregelt, die zu veröffentlichen ist. Für die Maßnahmen nach Abs. 8 und 9 gilt Abs. 3 Satz 3 entsprechend.

(11) Maßnahmen nach Abs. 8 Satz 4 und Abs. 9 Satz 1 und 2 dürfen nur nach richterlicher Anordnung nach Maßgabe des Art. 5 Abs. 3 UAbs. 2 der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 (KI-VO) auf Antrag der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten durchgeführt werden. Bei Gefahr im Verzug dürfen die Maßnahmen nach Abs. 8 Satz 4 und Abs. 9 Satz 1 und 2 durch die Polizeibehörden angeordnet werden, mit der Maßgabe, dass die Anordnung der Maßnahmen nach Abs. 9 Satz 1 und 2 durch die Behördenleitung oder eine von dieser beauftragte Bedienstete oder einen von dieser beauftragten Bediensteten erfolgt. Hat die Polizeibehörde bei Gefahr im Verzug die Anordnung getroffen, so beantragt die Behördenleitung oder eine von dieser beauftragte Bedienstete oder ein von dieser beauftragter Bediensteter unverzüglich, spätestens innerhalb von 24 Stunden, die richterliche Bestätigung der Anordnung.

Die Anordnung tritt außer Kraft, soweit sie nicht binnen drei Tagen richterlich bestätigt wird. Wird die Anordnung nicht richterlich bestätigt, werden die Maßnahmen nach Abs. 8 Satz 4 und Abs. 9 Satz 1 und 2 mit sofortiger Wirkung eingestellt und alle Daten sowie die Ergebnisse und Ausgaben dieser Maßnahmen unverzüglich gelöscht. In der Begründung des Antrags auf Erlass einer richterlichen Anordnung sind die Voraussetzungen für die Maßnahmen nach Abs. 8 Satz 4 und Abs. 9 Satz 1 und 2 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die das Vorliegen der Voraussetzungen nach Abs. 8 Satz 4 und Abs. 9 Satz 1 und 2 begründen, und die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme darzustellen. Im Übrigen gilt für das Verfahren § 39 Abs. 1 Satz 2 und 3 mit der Maßgabe, dass das Amtsgericht zuständig ist, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Das Nähere zu dem technischen Verfahren wird in einer Verwaltungsvorschrift geregelt.

Automatisierte Anwendung zur Datenanalyse, § 25a HSOG

Die Änderungen in § 25a HSOG sind ebenfalls auf Grundlage des Änderungsantrags erfolgt und betreffen die Absätze 1 und 2 sowie einen neuen Absatz 6. In § 25a Abs. 1 Satz 5 HSOG wurde die Einschränkung, dass eine regelbasierte und von Menschen definierte Abfolge von Analyse- und Verarbeitungsschritten erforderlich ist, gestrichen. Der Gesetzgeber begründet dies damit, den Einsatz von KI-Systemen auch im Rahmen von § 25a HSOG, folglich insbesondere bei hessenDATA, unter Berücksichtigung der Einschränkungen der unmittelbar geltenden KI-VO zu ermöglichen (LT-Drs. 21/1448, S. 11). Nach dem neuen Absatz 6 haben die Polizeibehörden sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden.

Das Bundesverfassungsgericht führt in seinem Urteil vom 16. Februar 2023 (1 BvR 1547/19 und 1 BvR 2634/20) zur automatisierten Datenanalyse aus, dass die Verwendung lernfähiger Systeme, d. h. KI-Systeme, je nach Einsatzart ein besonderes Eingriffsgewicht aufweisen kann und diese Systeme daher nur unter besonderen verfahrensrechtlichen Vorkehrungen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern, zur Anwendung kommen dürften (Rn. 100). Im Hinblick auf den Einsatz von Software, die komplexere Formen des automatisierten Abgleichs von Daten erlaubt, führt das Bundesverfassungsgericht aus, dass „auch Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit erforderlich [sind], was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann“ (Rn. 109). Ferner stellt das Bundesverfassungsgericht fest, dass der Gesetzgeber beim Einsatz von eingriffsintensiven Methoden der Datenauswertung, insbesondere bei komplexen Formen des Datenabgleichs, für schützende Regelungen sorgen muss (Rn. 101). Beim Einsatz von KI-Systemen dürfte dies vor allem die Nachvollziehbarkeit und Erklärbarkeit der Datenverarbeitung sowie die Gewährleistung der notwendigen Kennzeichnung der Quelldaten betreffen.

Im novellierten § 25a HSOG wird weder der Begriff der KI oder des KI-Systems erwähnt, noch finden sich besondere verfahrensrechtliche Vorkehrungen oder schützende Regelungen in der Norm. Mithin ist fraglich, ob die dargestellten Maßgaben des Bundesverfassungsgerichts zum Einsatz von KI-Systemen im Zusammenhang mit der automatisierten Anwendung zur Datenanalyse auf der Ebene eines förmlichen Gesetzes umgesetzt werden.

§ 25a HSOG

(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. Eine direkte Anbindung an Internetdienste ist ausgeschlossen.

(2) (…) Bei einer Maßnahme nach Satz 1 Nr. 3 dürfen Verkehrs- sowie Telekommunikationsdaten nicht in die Analyse einbezogen werden. (…)

(6) Die Polizeibehörden haben sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden.

Elektronische Aufenthaltsüberwachung

§ 31a Abs. 1 Satz 1 HSOG wurde u. a. um die Formulierung „zur Gefahrenabwehr“ ergänzt und durch eine Nr. 3 um eine weitere Anwendungsmöglichkeit erweitert, die laut Gesetzesbegründung den Einsatz der elektronischen Aufenthaltsüberwachung bei von den Sicherheitsbehörden als gefährlich eingestuften Personen und in Hochrisikofällen häuslicher Gewalt ermöglicht soll (LT-Drs 21/1151), S. 10 f). In Abs. 3 wird die Möglichkeit der Anordnung der elektronischen Aufenthaltsüberwachung in zeitlicher Hinsicht von drei auf jeweils vier Monate erweitert.

In meiner Stellungnahme hatte ich im Hinblick auf den neu gefassten § 31a Abs. 5 HSOG, der die Verbindung der erhobenen Daten zu einem Bewegungsbild aufgrund richterlicher Anordnung ermöglicht, auf die Problematik hingewiesen, dass die Erstellung des Bewegungsprofils allein von dem Erfordernis der Erfüllung des Überwachungszwecks abhängig gemacht wird. Auch wenn die Überwachung offen erfolgt und einem Richtervorbehalt unterliegt, stellt sie einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar, weil sie gerade die Erstellung eines Bewegungsprofils ermöglichen und (verbunden mit anderen Maßnahmen) zur Erstellung umfassender Persönlichkeitsprofile beitragen kann. Zwar finden sich in der Gesetzesbegründung einige Hinweise, was die Polizeibehörden in einem entsprechenden Antrag für das Gericht darlegen müssen: welches bedeutende Rechtsgut durch den konkreten Störer gefährdet ist, dass die Gefahr durch die elektronische Überwachung des Aufenthalts des Störers abgewehrt werden kann, die Notwendigkeit dieser polizeilichen Eingriffs-

maßnahme (LT-Drs. 21/1151, S. 12). Die Norm selbst enthält jedoch keine konkreten Vorgaben, an denen sich die Behörden im Zusammenhang mit der Bewertung der Verhältnismäßigkeit der Maßnahme orientieren können.

Des Weiteren wurde in Absatz 5 Satz 4 auf Grundlage des Änderungsantrags das sog. Zwei-Komponenten-Model eingeführt, wonach gefährdete Personen mit deren Einwilligung ebenfalls mit einem technischen Mittel ausgestattet und ihre Aufenthaltsdaten verarbeitet und abgeglichen werden können, um so die zu ihrem Schutz angeordneten Kontakt- und Näherungsverbote zu kontrollieren (LT-Drs. 21/1151, S. 12).

§ 31a HSOG

Die Polizeibehörden können zur Verhütung von terroristischen Straftaten oder zur Gefahrenabwehr eine Person dazu verpflichten, ein technisches Mittel, mit dem der Aufenthaltsort dieser Person elektronisch überwacht werden kann, ständig in betriebsbereitem Zustand am Körper bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen, wenn

1. *bestimmte Tatsachen die Annahme rechtfertigen, dass diese Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird,*
2. *deren individuelles Verhalten eine konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen wird, oder*
3. *im Einzelfall bestimmte Tatsachen die Annahme rechtfertigen, dass diese Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise Leben, Leib oder Freiheit einer Person erheblich gefährden oder eine Straftat gegen die sexuelle Selbstbestimmung, die im Mindestmaß mit wenigstens drei Monaten Freiheitsstrafe bedroht ist, begehen wird, um diese Person durch die Überwachung und die Datenverarbeitung von der Begehung terroristischer Straftaten abzuhalten oder die Effektivität der Gefahrenabwehr zu steigern. Die Verpflichtung nach Satz 1 umfasst auch die Verpflichtung, ein zur Verfügung gestelltes Mobiltelefon ständig in betriebsbereitem Zustand bei sich zu führen und dessen Funktionsfähigkeit nicht zu beeinträchtigen. (…)*

(3) Die Maßnahme nach Abs. 1 und die Verlängerung der Maßnahmen nach Abs. 2 dürfen nur aufgrund richterlicher Anordnung auf Antrag der Behördenleitung getroffen werden. Bei Gefahr im Verzug kann die Anordnung nach Satz 1 durch eine von der Behördenleitung beauftragte Person getroffen werden. In diesem Fall ist die richterliche Anordnung unverzüglich nachzuholen. Die Anordnung ist auf höchstens vier Monate zu befristen. Eine Verlängerung um jeweils bis zu vier Monate ist möglich, soweit die Anordnungsvoraussetzungen fortbestehen. Liegen die Voraussetzungen nicht mehr vor, ist die Maßnahme unverzüglich zu beenden. Zuständig ist das Amtsgericht, in dessen Bezirk die Polizeibehörde ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. (…)

(5) Die Polizeibehörden können mithilfe der von der betroffenen Person mitgeführten technischen Mittel automatisiert Daten über deren Aufenthaltsort sowie über etwaige Beeinträchtigungen der Datenerhebung verarbeiten. Soweit dies zur Erfüllung des Über-

wachungszwecks erforderlich ist, dürfen die erhobenen Daten aufgrund richterlicher Anordnung zu einem Bewegungsbild verbunden werden. Durch Rechtsverordnung der Ministerin oder des Ministers des Innern, für Sicherheit und Heimatschutz kann bestimmt werden, dass eine andere öffentliche Stelle als die Polizeibehörde die in Satz 1 genannten Daten verarbeitet. Die Polizeibehörden können mit Einwilligung einer Person, zu deren Schutz gegenüber der betroffenen Person eine Anordnung nach Abs. 2 oder § 1 des Gewaltschutzgesetzes besteht, Daten über deren Aufenthaltsort durch ein von dieser mitzuführendes technisches Mittel automatisiert verarbeiten und mit den nach Abs. 1 Satz 1 erhobenen Daten automatisiert abgleichen. Soweit es technisch möglich ist, ist sicherzustellen, dass innerhalb der Wohnung der Person keine über den Umstand ihrer Anwesenheit hinausgehenden Aufenthaltsdaten erhoben werden. Die Daten dürfen ohne Einwilligung der betroffenen Person nur verarbeitet werden, soweit dies erforderlich ist für folgende Zwecke:

1. *zur Verhütung zu erwartender Straftaten sowie zur Verfolgung von Straftaten im Sinne des Abs. 1 Satz 1 Nr. 1 und 2,*
2. *zur Abwehr einer Gefahr für Leib, Leben, Freiheit oder sexuelle Selbstbestimmung einer Person im Sinne des Abs. 1 Satz 1 Nr. 3,*
3. *zur Feststellung von Verstößen gegen Maßnahmen nach Abs. 2 oder § 1 des Gewaltschutzgesetzes,*
4. *zur Abwehr einer erheblichen gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer dritten Person oder*
5. *zur Aufrechterhaltung der Funktionsfähigkeit der technischen Mittel.*

Zur Einhaltung der Zweckbindung nach Satz 4 hat die Verarbeitung der Daten automatisiert zu erfolgen und es sind die Daten gegen unbefugte Kenntnisnahme besonders zu sichern. Die in Satz 1 genannten Daten sind spätestens zwei Monate nach ihrer Erhebung zu löschen, soweit sie nicht für die in Satz 4 genannten Zwecke verarbeitet werden. Jeder Abruf der Daten ist zu protokollieren. Die Protokolldaten sind nach zwölf Monaten zu löschen. Werden innerhalb der Wohnung der betroffenen Person über den Umstand ihrer Anwesenheit hinausgehende Aufenthaltsdaten erhoben, dürfen diese nicht verwendet werden und sind unverzüglich nach Kenntnisnahme zu löschen. Die Tatsache ihrer Kenntnisnahme und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach Abschluss der Datenschutzkontrolle zu löschen.

4.2
Entscheidung des BVerfG zum Hessischen Verfassungsschutzgesetz

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 17. Juli 2024 (1 BvR 2133/22) mehrere Datenerhebungs- und Übermittlungsbefugnisse des HVSG wegen Verstoßes gegen das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG für verfassungswidrig erklärt. Die Entscheidung knüpft an die 2023 abgeschlossene Novellierung des HVSG an (s. 52. Tätigkeitsbericht, Kap. 4.2, S. 48 ff.). Zu einem Großteil der Regelungen habe ich im Gesetzgebungsverfahren sowie im Beschwerdeverfahren vor dem BVerfG als Sachverständiger kritisch Stellung genommen.

Der hessische Gesetzgeber ist nun aufgerufen, die notwendigen Änderungen im HVSG vorzunehmen.

Mit der Entscheidung konkretisiert das BVerfG seine Rechtsprechung aus dem Jahr 2022 zum Bayerischen Verfassungsschutzgesetz (Urteil vom 26. April 2022, 1 BvR 1619/17, „Bayerisches Verfassungsschutzgesetz“) und zum Bundesverfassungsschutzgesetz (Beschluss vom 28. September 2022, 1 BvR 2354/13). Im Kern rügt es die unverhältnismäßigen Überwachungsbefugnisse des Hessischen Landesamtes für Verfassungsschutz (LfV Hessen) sowie die Befugnisse zur Übermittlung von mit nachrichtendienstlichen Mitteln erhobenen personenbezogenen Daten an andere Behörden, da das Gesetz hierfür keine hinreichenden rechtlichen Hürden vorsieht. Das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ist daher durch die Befugnisse zur heimlichen Erhebung und Übermittlung personenbezogener Daten regelmäßig intensiv betroffen.

Bei den Überwachungsbefugnissen fokussiert sich das BVerfG auf die Regelungen, die das LfV Hessen gemäß § 9 HVSG zur Ortung von Mobilfunkendgeräten und zum Einsatz verdeckter Mitarbeiter gemäß § 12 HVSG ermächtigen. Diese Maßnahmen ermöglichen eine intensive Überwachung, die tief in die Grundrechte der Betroffenen eingreift. Nachfolgend werden die Kernaussagen des BVerfG zu den aufgeführten Normen kurz dargestellt.

Ortung von Mobilfunkendgeräten, § 9 HVSG

§ 9 Abs. 1 Nr. 2 HVSG ist laut Gericht verfassungswidrig, weil er eine engmaschige langandauernde Überwachung der Bewegungen im Raum erlaubt, ohne hierfür eine hinreichende Eingriffsschwelle vorzusehen. Dies gilt insbesondere deshalb, weil die Norm keine ausreichenden Vorgaben zur zeitlichen Taktung und Dauer der Standortbestimmung enthält, so dass der Aufenthaltsort einer Person in kurzen Zeitabständen und über einen längeren Zeitraum ermittelt werden kann, was die Erstellung von Bewegungsprofilen ermöglicht. Im Hinblick auf § 9 Abs. 2 HVSG kritisiert das BVerfG ebenso fehlende Eingriffsschwellen. Insbesondere werden nicht alle Fälle mit hohem Eingriffsgewicht erfasst, wie z. B. punktuelle Ortungen über mehrere Tage hinweg. Selbst wenn eine Ortung nur an drei aufeinanderfolgenden Tagen stattfindet und danach für einen Tag oder mehrere Tage unterbrochen wird, kann sie einen ebenso schwerwiegenden Eingriff darstellen, da auch auf diese Weise Bewegungsprofile erstellt werden können.

§ 9 HVSG

(1) Das Landesamt darf im Einzelfall, soweit dies zur Erfüllung seiner Aufgaben nach § 2 erforderlich ist, technische Mittel einsetzen

1. *zur Ermittlung der Geräte- oder Kartennummer und*
2. *zur Ermittlung des Standorts eines aktiv geschalteten Mobilfunkendgeräts.*

(2) Technische Mittel nach Abs. 1 Nr. 2, die

1. *nicht lediglich im Zusammenhang mit anderen operativen Maßnahmen zu deren Ermöglichung eingesetzt werden, insbesondere für Zwecke von Observationsmaßnahmen nach § 11 zur Bestimmung des Standorts der eingeloggten Funkzelle, sondern um anhand der Standortdaten die Bewegungen des Mobiltelefons nachzuverfolgen (Bewegungsprofil) und*
2. *zu diesem Zweck an mehr als drei aufeinanderfolgenden Tagen mehrfach täglich eingesetzt werden,*

dürfen nur eingesetzt werden, soweit dies zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit gemäß § 3 Abs. 2 im Einzelfall geboten ist.

Einsatz von verdeckten Mitarbeiterinnen und Mitarbeitern, § 12 HVSG

§ 12 Abs. 1 Satz 1 HVSG ist verfassungswidrig, weil die Befugnis auch eingriffsintensive Einsätze verdeckter Mitarbeitender erlaubt, ohne einen erhöhten Beobachtungsbedarf und Aufklärungsgewinn zu fordern. Somit wird keine ausreichende Eingriffsschwelle vorausgesetzt. Laut BVerfG ergibt sich aus Satz 1 insbesondere nicht, dass tatsächliche Anhaltspunkte sowohl für die Annahme einer beobachtungsbedürftigen Bestrebung als auch für die Erforderlichkeit der Aufklärung vorliegen müssen. Durch die Formulierung des § 12 Abs. 1 Satz 2 HVSG, der erhöhte Voraussetzungen für den Einsatz verdeckter Mitarbeitender über sechs Monate hinaus vorsieht, werden nach Auffassung des Gerichts zudem nicht alle einriffsintensiven Einsätze erfasst. Neben der Dauer der Maßnahme hängt die Eingriffsintensität u. a. auch von der Intensität der Beziehung zwischen den Mitarbeitenden und den Betroffenen ab, wonach sich die erhöhten Anforderungen bestimmen müssen.

§ 12 HVSG

(1) Das Landesamt darf eigene Mitarbeiterinnen und Mitarbeiter unter einer ihnen verliehenen und auf Dauer angelegten Legende (Verdeckte Mitarbeiterinnen und Verdeckte Mitarbeiter) einsetzen, wenn dies zur Aufklärung einer bestimmten nachrichtendienstlich beobachtungsbedürftigen Bestrebung oder Tätigkeit im Einzelfall geboten ist. Der Einsatz Verdeckter Mitarbeiterinnen und Verdeckter Mitarbeiter für eine Dauer von länger als sechs Monaten ist nur zulässig, wenn dieser zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit gemäß § 3 Abs. 2 unerlässlich ist.

Auch die derzeitigen Regelungen zur Übermittlung nachrichtendienstlich erhobener personenbezogener Daten an andere Behörden und öffentliche Stellen hält das BVerfG in einigen Teilen für verfassungswidrig und beanstandet insbesondere die mangelnde Bestimmtheit der Normen. Dabei ist zu berücksichtigen, dass die Übermittlung personenbezogener Daten an andere Stellen einen eigenständigen Grundrechtseingriff darstellt, der sich am jeweiligen Grundrecht orientieren muss, in das bei der ursprünglichen Datenerhebung eingegriffen wurde.

Informationsübermittlung durch das Landesamt an Strafverfolgungsbehörden, § 20a HVSG

§ 20a Satz 1 HVSG ist nach Ansicht des BVerfG verfassungswidrig, soweit § 20a Satz 2 Buchst. b und Satz 3 HVSG an nicht hinreichend gewichtige Straftaten anknüpfen. Die Qualifizierung einer Straftat als besonders schwer und der Umstand, dass Schutzgüter der Verfassung betroffen sind, muss bereits im Tatbestand der Strafnorm zum Ausdruck kommen. Dem wird § 20a Satz 1 HVSG bei Übermittlungen nach § 20a Satz 2 Buchst. b HVSG nicht gerecht. Laut Gericht knüpft die Norm nicht an bestimmte Begehungsformen oder Tatfolgen an, die die besondere Schwere der Tat begründen würden. Zudem ist nicht sichergestellt, dass sich die Betroffenheit von Verfassungsschutzgütern auch objektiv im Tatbestand des jeweiligen Straftatbestandes niederschlägt.

§ 20a HVSG

Begründen bestimmte Tatsachen den Verdacht, dass jemand eine besonders schwere Straftat begangen (§ 25 des Strafgesetzbuchs), an der Begehung teilgenommen (§§ 26, 27 des Strafgesetzbuchs) oder die Beteiligung versucht (§§ 22, 23, 30 des Strafgesetzbuchs) hat, darf die Verfassungsschutzbehörde mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an die Strafverfolgungsbehörden übermitteln, soweit dies zur Verfolgung der Tat erforderlich ist. Besonders schwere Straftaten sind solche, die mit einer Höchststrafe bedroht sind von mindestens

a) zehn Jahren Freiheitsstrafe oder

b) fünf Jahren Freiheitsstrafe, wenn sie im Zusammenhang mit der Beteiligung an einer beobachtungsbedürftigen Bestrebung i. S. d. § 2 Abs. 2 Nr. 1, 3, 4 oder 5 oder in Ausübung einer beobachtungsbedürftigen Tätigkeit i. S. d. § 2 Abs. 2 Nr. 2 begangen werden.

Besonders schwere Straftaten sind ferner sonstige gegen Leib, Leben, Gesundheit, sexuelle Selbstbestimmung, Freiheit oder Sachen von bedeutendem Wert, deren Erhaltung im besonderen öffentlichen Interesse geboten ist, gerichtete Straftaten, soweit im Einzelfall tatsächliche Anhaltspunkte dafür vorliegen, dass der Tatentschluss auf einem rassistischen, fremdenfeindlichen, antisemitischen oder sonstigen menschenverachtenden Beweggrund oder Ziel beruht, und die Tat geeignet ist,

1. Personen zu instrumentalisieren, indem ihnen wiederkehrend oder in beträchtlichem Ausmaß körperliches oder seelisches Leid oder wirtschaftlicher Schaden zugefügt wird,
2. Personen von der Teilhabe an der demokratischen Willensbildung auszuschließen oder nachhaltig zu hindern oder
3. das Vertrauen von Teilen der Bevölkerung in die Unverbrüchlichkeit des Rechts zu erschüttern.

Informationsübermittlung an sonstige inländische öffentliche Stellen, § 20b HVSG

§ 20b Abs. 2 HVSG erklärt das BVerfG für verfassungswidrig, da die Befugnis auch die Übermittlung an inländische öffentliche Stellen mit operativen Anschlussbefugnissen erlaubt und dafür keine hinreichende Übermittlungsschwelle vorsieht. Die erhöhten Eingriffsschwellen für die Datenübermittlung müssen bereits dann gelten, wenn die empfangende Stelle überhaupt über operative Anschlussbefugnisse verfügt. Laut Gericht ist eine solche Datenübermittlung daher nur zulässig, wenn eine mindestens konkretisierte Gefahr vorliegt.

§ 20b HVSG

(2) Das Landesamt darf von sich aus mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an sonstige inländische öffentliche Stellen zum Schutz eines der in § 20 genannten Rechtsgüter übermitteln, wenn hinreichende tatsächliche Anhaltspunkte dafür vorliegen, dass dies im Einzelfall zur Erfüllung der Aufgaben des Empfängers erforderlich ist.

Für die derzeitigen Regelungen gilt eine Übergangsfrist bis zum 31. Dezember 2025, innerhalb derer der hessische Gesetzgeber nun aufgerufen ist, die verfassungswidrigen Regelungen zu überarbeiten und vor dem Hintergrund tiefgreifender Grundrechtseingriffe mit hoher Persönlichkeitsrelevanz für die Betroffenen an die verfassungsrechtlichen Anforderungen anzupassen.

Diesen Prozess werde ich aufmerksam und kritisch begleiten.

4.3
Datenschutzkontrollen bei einer Staatsanwaltschaft

Im Herbst 2024 habe ich erneut eine Datenschutzkontrolle bei einer hessischen Staatsanwaltschaft durchgeführt. Der Schwerpunkt lag hierbei wieder auf der Telekommunikationsüberwachung nach § 100a StPO. Infolge der bereits in den beiden Vorjahren durchgeführten Kontrollen hatte die Generalstaats-

anwaltschaft das Vordruckformular für Anträge für verdeckte Maßnahmen angepasst; der Umgang mit diesem überarbeiteten Formular war ebenfalls Gegenstand meiner Kontrolle.

Im Berichtsjahr 2023 hatte ich eine Datenschutzkontrolle bei einer hessischen Staatsanwaltschaft durchgeführt, deren Schwerpunkt auf der Einhaltung der gesetzlichen Anforderungen an die Benachrichtigung der Beteiligten einer überwachten Telekommunikation nach §§ 101 Abs. 4 Satz 1 Nr. 3 und Abs. 1 sowie § 100a StPO lag. Nach meiner Überprüfung hatte die Generalstaatsanwaltschaft eine Anpassung am Vordruckformular für Anträge für verdeckte Maßnahmen vorgenommen. Das Formular wurde mit entsprechenden Hinweisen der Generalstaatsanwaltschaft den hessischen Staatsanwaltschaften zur Verfügung gestellt. Dies habe ich zum Anlass genommen, im Herbst 2024 eine weitere hessische Staatsanwaltschaft auf die Einhaltung der gesetzlichen Benachrichtigungspflicht nach § 101 Abs. 4 Satz 1 Nr. 3 und Abs. 1 StPO zu überprüfen.

Im Folgenden gebe ich einen Überblick über die gesetzlichen Anforderungen an die Benachrichtigung der Beteiligten einer überwachten Telekommunikation und Ergebnisse meiner Datenschutzkontrolle.

Eine Telekommunikationsüberwachung gemäß § 100a StPO stellt eine besonders eingriffsintensive Maßnahme der Strafverfolgung dar. Neben den gespeicherten Umständen der Kommunikation dürfen nach § 100a Abs. 1 Satz 3 StPO auch Inhalte der Gespräche ohne Wissen des Betroffenen überwacht und aufgezeichnet werden. Folglich werden im Zuge einer Überwachungsmaßnahme personenbezogene Daten regelmäßig im größeren Umfang verarbeitet.

Aufgrund des besonderen Eingriffscharakters der Telekommunikationsüberwachung sind die Beteiligten nach Beendigung der Maßnahme gemäß § 101 Abs. 4 Satz 1 Nr. 3 und Abs. 1 StPO zu benachrichtigen. Eine Zurückstellung der Benachrichtigung ist nur unter den Voraussetzungen des § 101 Abs. 6 StPO möglich. Der Grund für die zurückgestellte Benachrichtigung ist 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. In Ausnahmefällen kann eine Benachrichtigung betroffener Personen gemäß § 101 Abs. 4 Satz 3 und 4 StPO unterbleiben, etwa wenn ihr überwiegend schutzwürdige Belange einer betroffenen Person entgegenstehen oder die betroffene Person von der Maßnahme nur unerheblich betroffen wurde und anzunehmen ist, dass sie kein Interesse an der Benachrichtigung hat. Zuständig für die Durchführung

der Benachrichtigung über Maßnahmen nach § 100a StPO ist die jeweilige Staatsanwaltschaft.

Für meine Datenschutzkontrolle habe ich elf Verfahrensakten aus den Jahren 2022/2023 bei einer hessischen Staatsanwaltschaft angefordert. Bei der Auswahl der Akten habe ich darauf geachtet, unterschiedliche Dezernate abzudecken. Alle angeforderten Verfahrensakten betrafen Maßnahmen zur Telekommunikationsüberwachung nach § 100a StPO und konnten mir für meine Überprüfung vollständig bereitgestellt werden.

Im Ergebnis waren die richterlichen Beschlüsse als Rechtsgrundlage der verdeckten Maßnahmen vollumfänglich in den Akten vorhanden und ordnungsgemäß dokumentiert.

Aus einer der überprüften Akten konnte entnommen werden, dass das überarbeitete Formblatt der Generalstaatsanwaltschaft verwendet wurde. Hier wurden die Beteiligten der überwachten Telekommunikation nach Beendigung der Maßnahme ordnungsgemäß benachrichtigt und die Benachrichtigungen nachvollziehbar dokumentiert.

Gleichwohl konnte nicht in allen Akten nachvollzogen werden, ob die Benachrichtigungen nach § 101 Abs. 4 Satz 1 Nr. 3 und Abs. 1 StPO erfolgt sind. Auch die Zurückstellungen nach § 101 Abs. 5 StPO sowie deren Begründung durch die Staatsanwaltschaft waren nicht immer und nicht in Bezug auf alle Beteiligten der überwachten Telekommunikation eindeutig nachzuvollziehen. In einer der überprüften Akten wurden die erstmaligen Zurückstellungen der Benachrichtigungen der Beteiligten im Anordnungsbeschluss zur Maßnahme durch das Gericht angeordnet. Für diese Akte fehlte es im Umkehrschluss an einer Zurückstellung durch die Staatsanwaltschaft, die trotz des gerichtlichen Beschlusses für die erstmalige Zurückstellung zuständig bleibt.

Das Ergebnis meiner Überprüfung zeigt, dass die Verwendung des abgeänderten Formblatts der Generalstaatsanwaltschaft wesentlich dazu beitragen kann, die Benachrichtigungspflicht nach § 101 Abs. 4 Satz 1 Nr. 3 und Abs. 1 StPO einzuhalten und das staatsanwaltschaftliche Handeln bei der Durchführung der Benachrichtigung und das Verfahren zur Telekommunikationsüberwachung nachvollziehbar zu dokumentieren. Dass das geänderte Formblatt in nur einem der überprüften Verfahrensakten vorgefunden wurde, wird dem Umstand geschuldet sein, dass das Formblatt erst ab dem vierten Quartal des Jahres 2023 zur Verfügung stand.

Ein vorläufiges Ergebnis und Handlungsbedarfe wurden der Leitung der geprüften Staatsanwaltschaft im Anschluss an meine Datenschutzkontrolle mitgeteilt. Auch wurde auf das Formblatt der Generalstaatsanwaltschaft noch einmal hingewiesen.

§ 100a StPo

(1) Auch ohne Wissen der Betroffenen darf die Telekommunikation überwacht und aufgezeichnet werden, wenn

1. *bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat,*
2. *die Tat auch im Einzelfall schwer wiegt und*
3. *die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.*

Die Überwachung und Aufzeichnung der Telekommunikation darf auch in der Weise erfolgen, dass mit technischen Mitteln in von dem Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn dies notwendig ist, um die Überwachung und Aufzeichnung insbesondere in unverschlüsselter Form zu ermöglichen. Auf dem informationstechnischen System des Betroffenen gespeicherte Inhalte und Umstände der Kommunikation dürfen überwacht und aufgezeichnet werden, wenn sie auch während des laufenden Übertragungsvorgangs im öffentlichen Telekommunikationsnetz in verschlüsselter Form hätten überwacht und aufgezeichnet werden können.

(2) Schwere Straftaten im Sinne des Absatzes 1 Nr. 1 sind: (…)

(3) Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt.

§ 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.

4.4
Offenlegung personenbezogener Daten im staatsanwaltschaftlichen Einstellungsbescheid

Im Wege einer Beschwerde wurde mir mitgeteilt, dass personenbezogene Daten eines Anzeigenerstatters in einem staatsanwaltschaftlichen Einstellungsbescheid gegenüber Dritten offengelegt worden sind. Die verantwortliche Staatsanwaltschaft habe ich daraufhin sensibilisiert, künftig Daten Dritter, die für die Begründung der Einstellung nicht erforderlich sind, zu entfernen. Die Generalstaatsanwaltschaft hat dies zum Anlass genommen, die hessischen Staatsanwaltschaften für die Thematik zu sensibilisieren und die Vordrucke für Einstellungsbescheide datenschutzkonform anpassen zu lassen.

Im Rahmen eines Beschwerdeverfahrens rügte der Beschwerdeführer, dass die Staatsanwaltschaft in einem Einstellungsbescheid, der ihm als Anzeigender und Geschädigter einer mutmaßlichen Straftat durch ein Unternehmen zugestellt worden war, seine personenbezogenen Daten gegenüber dritten Personen offengelegt hatte. Weitere sechs Personen, die dem Beschwer-

deführer unbekannt waren, hatten aufgrund desselben Tatvorwurfes und ähnlicher Sachverhalte Anzeige gegen das Unternehmen gestellt, so dass dies in einem Verfahren von der Staatsanwaltschaft bearbeitet wurde.

Die Staatsanwaltschaft stellte das Ermittlungsverfahren mangels Tatverdachts gemäß § 170 Abs. 2 Satz 1 StPO ein und hat die Anzeigenerstatter, darunter auch den Beschwerdeführer, beschieden. Der Einstellungsbescheid enthielt Angaben zum Vor- und Zunamen und zum Wohnort des Beschwerdeführers und den weiteren Anzeigenerstattern. Die Staatsanwaltschaft teilte dem Beschwerdeführer auf Nachfrage mit, dass der Einstellungsbescheid inhaltsgleich auch den übrigen Anzeigenden in dem Ermittlungsverfahren zugestellt worden war.

Bei der Offenlegung der personenbezogenen Daten gegenüber Dritten handelt es sich um eine Datenverarbeitung, die auf einer Rechtsgrundlage beruhen muss.

Gemäß § 171 StPO besteht bei Einstellung des Ermittlungsverfahrens und Vorliegen der gesetzlichen Voraussetzungen eine Bescheidungspflicht der Staatsanwaltschaft gegenüber Anzeigeerstattern einer möglichen Straftat. Der Bescheid ist jedem Anzeigenden zu erteilen. Von mehreren Anzeigeerstattern hat jeder Einzelne Anspruch auf einen gesonderten Bescheid. In diesem sind die tragenden tatsächlichen und rechtlichen Gründe für die Einstellung in einer verständlichen Weise mitzuteilen. Die namentliche Nennung und Angaben zum Wohnort der anderen Anzeigeerstatter ist gesetzlich nicht vorgeschrieben. Hierauf ist somit zu verzichten, sofern die Darstellung der Einstellungsentscheidung weiterhin nachvollziehbar bleibt.

Ich habe mich mit der Staatsanwaltschaft in Verbindung gesetzt, um die Erforderlichkeit der Angaben in den Bescheiden überprüfen zu lassen. Die Staatsanwaltschaft erklärte, dass für die Erstellung der staatsanwaltschaftlichen Einstellungsbescheide ein Vordruck der Generalstaatsanwaltschaft genutzt werde. Dieser diene insbesondere der Arbeitserleichterung in Massenverfahren. Die Reinschrift im Vordruck könne individuell angepasst und somit können auch Daten Dritter gelöscht werden. Im konkreten Ermittlungsverfahren sei die nachvollziehbare Darstellung der Einstellungsbescheidung auch ohne die Nennung der Namen und Wohnorte gegenüber den anderen Anzeigenerstattern möglich gewesen.

Ich habe die verantwortliche Staatsanwaltschaft wegen des im konkreten Fall als geringfügig einzustufenden Verstoßes sensibilisiert, künftig personenbezogene Daten im Bescheid, die für die Begründung der Einstellungsentscheidung nicht erforderlich sind, zu entfernen und so eine verzichtbare Offenlegung gegenüber Dritten zu vermeiden.

Die Generalstaatsanwaltschaft hat meine Sensibilisierung zum Anlass genommen, die hessischen Staatsanwaltschaften per Rundschreiben erneut auf den sorgfältigen Umgang mit personenbezogenen Daten und den Grundsatz der Datensparsamkeit hinzuweisen. Zudem wurde das Einstellungsformular um eine Ergänzung des Hinweisfeldes und eine Ankreuzmöglichkeit zur Einzelbescheidung ergänzt, wonach bei der Bescheidung mehrerer Anzeigeerstatter zu prüfen ist, ob nur der jeweilige Adressat namentlich aufzuführen ist.

Im Ergebnis hat die Staatsanwaltschaft zu prüfen, ob die Offenlegung der personenbezogenen Daten der Anzeigensteller zur Darlegung der Einstellungsbegründung erforderlich ist. Der jeweilige Einstellungsvordruck ist im Einzelfall insoweit datenschutzkonform anzupassen.

§ 170 StPo

(1) Bieten die Ermittlungen genügenden Anlass zur Erhebung der öffentlichen Klage, so erhebt die Staatsanwaltschaft sie durch Einreichung einer Anklageschrift bei dem zuständigen Gericht.

(2) Andernfalls stellt die Staatsanwaltschaft das Verfahren ein. Hiervon setzt sie den Beschuldigten in Kenntnis, wenn er als solcher vernommen worden ist oder ein Haftbefehl gegen ihn erlassen war; dasselbe gilt, wenn er um einen Bescheid gebeten hat oder wenn ein besonderes Interesse an der Bekanntgabe ersichtlich ist.

§ 171 StPo

Gibt die Staatsanwaltschaft einem Antrag auf Erhebung der öffentlichen Klage keine Folge oder verfügt sie nach dem Abschluss der Ermittlungen die Einstellung des Verfahrens, so hat sie den Antragsteller unter Angabe der Gründe zu bescheiden. In dem Bescheid ist der Antragsteller, der zugleich der Verletzte ist, über die Möglichkeit der Anfechtung und die dafür vorgesehene Frist (§ 172 Abs. 1) zu belehren. § 187 Absatz 1 Satz 1 und Absatz 2 des Gerichtsverfassungsgesetzes gilt entsprechend für Verletzte, die nach § 395 der Strafprozessordnung berechtigt wären, sich der öffentlichen Klage mit der Nebenklage anzuschließen, soweit sie einen Antrag auf Übersetzung stellen.

4.5
Datenschutzkontrollen bei Polizeibehörden und Verfassungsschutz

In verschiedenen Bereichen sind gesetzliche Pflichten zu Datenschutzkontrollen für meine Behörde geregelt. Im Berichtsjahr 2024 wurde turnusmäßig die Antiterrordatei (ATD) geprüft. Zudem habe ich die regelmäßige Kontrolle zu verdeckten Maßnahmen begonnen. Des Weiteren wurden die Datenschutzkontrollen zu vergebenen personengebundenen Hinweisen und Zeugenschutz im Bundeszentralregister bei der Hessischen Polizei abgeschlossen.

Kontrolle der Antiterrordatei

Gemäß § 10 Abs. 2 ATDG fand eine Datenschutzkontrolle zu Neuspeicherungen im Zeitraum 2022 bis Mai 2024 in die ATD beim Hessischen Landeskriminalamt statt. Durch das Hessische Landesamt für Verfassungsschutz wurden im entsprechenden Zeitraum keine Neuspeicherungen in die Datei vorgenommen, deren Rechtmäßigkeit hätte geprüft werden können.

Schwerpunkt meiner Kontrolle lag auf Speicherungen gemäß § 2 ATDG. Es wurden stichprobenartig die Speicherungen von 15 Personen überprüft. Nicht bei allen Personen konnten die Speichervoraussetzungen ohne ergänzende Erklärungen seitens der speicherverantwortlichen Stelle ausreichend nachvollzogen werden. Über das abschließende Ergebnis der Kontrolle werde ich im nächsten Tätigkeitsbericht informieren.

§ 2 ATDG

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

1. *Personen, die*

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

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

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

§ 10 ATDG

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

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

Datenschutzkontrolle von verdeckten Maßnahmen

Im Berichtszeitraum habe ich mit der Datenschutzkontrolle von verdeckten Maßnahmen – konkret die Anordnungen des Einsatzes verdeckter Ermittler (VE) oder verdeckt ermittelnder Personen (VP) – der Hessischen Polizei gemäß § 29a HSOG begonnen. Gegenstand der Prüfung sind die formellen Voraussetzungen der jeweiligen Anordnungen und das Vorliegen entsprechender richterlicher Beschlüsse gemäß § 16 Abs. 9 HSOG. Bis zur Fertigstellung dieses Tätigkeitsberichts war die Kontrolle noch nicht abgeschlossen. Über das Ergebnis wird im nächsten Jahr berichtet.

§ 16 HSOG

(9) Eine Anordnung über den Einsatz von V-Personen oder VE-Personen erfolgt außer bei Gefahr im Verzug schriftlich durch die Behördenleitung oder eine von dieser beauftragte Bedienstete oder einen von dieser beauftragten Bediensteten. Abweichend von Satz 1 bedarf der Einsatz von V-Personen, der sich gegen eine bestimmte Person richtet, und von VE-Personen mit einer auf Dauer angelegten Legende einer richterlichen Anordnung. Bei Gefahr im Verzug kann die Anordnung nach Satz 2 auch durch die Behördenleitung oder eine von dieser beauftragte Bedienstete oder einen von dieser beauftragten Bediensteten schriftlich getroffen werden. Ist eine Anordnung nach Satz 3 ergangen, so ist unverzüglich die richterliche Bestätigung der Anordnung zu beantragen; die Anordnung tritt außer Kraft, soweit sie nicht binnen drei Tagen richterlich bestätigt wird. Eine Anordnung muss die Personen, gegen die sich der Einsatz richten soll, so genau bezeichnen, wie dies nach den zur Zeit der Anordnung vorhandenen Erkenntnissen möglich ist. Art, Umfang und Dauer des Einsatzes sind festzulegen und die wesentlichen Gründe anzugeben. Eine Verlängerung ist zulässig, soweit die Voraussetzungen fortbestehen. Für eine richterliche Anordnung ist das Amtsgericht zuständig, in dessen Bezirk die Polizeibehörde ihren Sitz hat; für das Verfahren gilt § 39 Abs. 1 Satz 3. Die Staatsanwaltschaft ist unverzüglich über eine Anordnung nach Satz 2 zu unterrichten.

§ 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.

Datenschutzkontrolle polizeilich vergebener personengebundener Hinweise

Die im Jahr 2023 begonnene Datenschutzkontrolle zu polizeilich vergebenen personengebundenen Hinweisen „Betäubungsmittelkonsument (BTMK)“ wurde abgeschlossen. Gemäß § 20 Abs. 12 Satz 3 HSOG, § 16 Abs. 6 Nr. 1 i. V. m. § 29 Abs. 3 BKAG dürfen Polizeibehörden zum Schutz dieser Person oder zum Schutz der Bediensteten der Gefahrenabwehr- und der Polizeibe-

hörden in polizeilichen Auskunftssystemen personengebundene Hinweise weiterverarbeiten. Die Vergabe erfolgt nach bundesweit einheitlichen Kriterien. Im Rahmen meiner Datenschutzkontrolle habe ich 35 Speicherungen des personengebundenen Hinweises BTMK anhand der mir zur Verfügung gestellten Kriminalakten geprüft. Gegenstand meiner Kontrolle waren die Speichervoraussetzungen und deren Dokumentation sowie die Durchführung der einzelnen Speicherung.

Ergebnis der Prüfung war insbesondere, dass innerhalb Hessens unterschiedliche Formulare für die Zulieferung an und Erfassung durch die entsprechenden speicherverantwortlichen Dienststellen verwendet werden. Unterschiede gab es auch im Hinblick auf den Zeitpunkt der Speicherung und den Umgang mit Altfällen, die aufgrund geänderter Kriterien die Speichervoraussetzungen nicht mehr erfüllten.

Im Nachgang der Datenschutzkontrolle wurden Gespräche mit allen speicherverantwortlichen Dienststellen geführt. Dabei berichteten die Polizeibehörden, dass bereits eine Arbeitsgruppe eingerichtet wurde, die sich für die hessenweit einheitliche Erfassung dieser „Personengebundenen Hinweise“ (PHW) einsetzt.

§ 20 HSOG

(12) § 13 Abs. 9 gilt bei der Weiterverarbeitung personenbezogener Daten entsprechend. Bei Bewertungen ist § 68 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes zu beachten. In den Fällen, in denen bereits Daten zu einer Person vorhanden sind, können zu dieser Person auch personengebundene Hinweise, die zum Schutz dieser Person oder zum Schutz der Bediensteten der Gefahrenabwehr- und der Polizeibehörden erforderlich sind, und weitere Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen, weiterverarbeitet werden.

§ 16 BKAG

(6) Das Bundeskriminalamt kann in den Fällen, in denen bereits Daten zu einer Person vorhanden sind, zu dieser Person auch weiterverarbeiten:

1. *personengebundene Hinweise, die zum Schutz dieser Person oder zur Eigensicherung von Beamten erforderlich sind, oder*
2. *weitere Hinweise, die geeignet sind, dem Schutz Dritter oder der Gewinnung von Ermittlungsansätzen zu dienen.*

§ 29 BKAG

(3) Außer dem Bundeskriminalamt und den Landeskriminalämtern sind zur Teilnahme am polizeilichen Informationsverbund berechtigt:

1. sonstige Polizeibehörden der Länder,
2. die Bundespolizei,
3. die Polizei beim Deutschen Bundestag,
4. mit der Wahrnehmung grenzpolizeilicher Aufgaben betraute Behörden der Zollverwaltung,
5. die Zollfahndungsämter,
6. das Zollkriminalamt und
7. die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden.

Die am polizeilichen Informationsverbund teilnehmenden Stellen haben das Recht, Daten zur Erfüllung der Verpflichtung nach § 32 im automatisierten Verfahren einzugeben und, soweit dies zur jeweiligen Aufgabenerfüllung erforderlich ist, abzurufen.

Prüfung zum Zeugenschutz im Bundeszentralregister

Im Jahr 2024 konnte die Datenschutzkontrolle zum Zeugenschutz im Bundeszentralregister (BZR) gemäß § 44a Bundeszentralregistergesetz, die im Vorjahr begonnen wurde, beendet werden. Inhalt meiner Prüfung waren die Kennzeichnung zusammengehöriger Echtpersonalien-Datensätze und Pseudo-Datensätze in Zeugenschutzvorgängen, Veränderungen und Einträge über strafrechtliche Verurteilungen im BZR sowie Postfachadressen von Zeugenschutzstellen ohne Polizeibezug. Für meine Datenschutzkontrolle kam nur ein konkreter Fall der Hessischen Polizei in Betracht, der einen Bezug zum BZR aufwies. Im Rahmen der Prüfung konnte ich Einsicht in die Fallakte nehmen.

Verstöße gegen Datenschutzvorschriften wurden im vorliegenden Fall nicht festgestellt.

§ 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.

4.6
Typosquatting bei der Hessischen Polizei

Gemäß § 60 HDSIG hat mir die verantwortliche Stelle Verletzungen des Schutzes personenbezogener Daten zu melden, wenn diese voraussichtlich zu einem Risiko für Rechte und Freiheiten natürlicher Personen führen. Grund einer großen Anzahl von Meldungen waren im Jahr 2024 Tippfehler in E-Mails, die dazu führten, dass zunächst unbemerkt Inhalte an unbekannte Dritte versendet wurden. Zu Fehladressierung von E-Mails aus der Hessischen Landesverwaltung s. Kap. 14.9.

Im Jahr 2024 meldete die Hessische Polizei insgesamt 105 gleichartige Datenschutzverletzungen. Konkret haben unbekannte Dritte die Domains „hesssen.de“ und „hesen.de“ im nichteuropäischen Ausland registrieren lassen, um so aufgrund von versehentlichen Tippfehlern bei der Eingabe von E-Mail-Adressen Informationen erlangen zu können. Diese Art von Angriff wird als „Typosquatting“ (von engl. „typo“ = Tippfehler und „squatting“ = etwas besetzen oder in Beschlag nehmen) bezeichnet. Infolgedessen kam es zu einem Risiko für die Rechte und Freiheiten der innerhalb der E-Mails benannten Personen.

„Typosquatting“ stellt eine Verletzung des Schutzes personenbezogener Daten dar, wenn zuvor nicht ausreichend technische und organisatorische Maßnahmen getroffen wurden, um zu verhindern, dass Unbefugte die Domains haben übernehmen können.

Nach den ersten Meldungen habe ich Kontakt mit den Datenschutzbeauftragten der Polizeibehörden aufgenommen und in der Folge die verantwortlichen Stellen zu dieser Problematik im Sinne des § 13 Abs. 2 Nr. 4 HDSIG sensibilisiert. Zudem wurden polizeiintern Sensibilisierungen der Beschäftigten zum „Typosquatting“ vorgenommen sowie technische und organisatorische Maßnahmen getroffen. Diese bestehen darin, dass im E-Mail-System Sperren und Fehlermeldungen eingerichtet sowie die Domains „hesssen.de“ und „hesen.de“ durch die Hessische Zentrale für Datenverarbeitung gesperrt wurden.

Neben der Meldepflicht kamen die verantwortlichen Stellen auch ihrer Benachrichtigungspflicht gegenüber den betroffenen Personen nach und informierten diese in den Fällen, in denen eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hatte.

Ergänzend verweise ich auf einen Onlineartikel auf meiner Homepage (https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/typosquat-

ting-wenn-internetadressen-und-e-mails-durch-tippfehler-gefaehrlich-werden) verwiesen.

§ 60 Abs. 1 HDSIG

Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Hessischen Datenschutzbeauftragten zu melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

§ 61 Abs. 1 HDSIG

Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen.

§ 13 Abs. 2 HDSIG

Neben den Aufgaben nach Art. 57 der Verordnung (EU) Nr. 2016/679 hat die oder der Hessische Datenschutzbeauftragte die Aufgaben, (…)

4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten bei der Verarbeitung personenbezogener Daten zu sensibilisieren, (…).

Art. 6 Abs. 1 DS-GVO

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

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

5. Allgemeine Verwaltung, Kommunen

Die Arbeit der Landesverwaltung sowie der Verwaltungen der Landkreise, Städte und Gemeinden in Hessen besteht überwiegend in der Verarbeitung personenbezogener Daten. Diese betrifft alle Bürgerinnen und Bürger Hessens. Daher ist es besonders wichtig, dass die Verwaltungstätigkeiten datenschutzrechtlichen Vorgaben entsprechen. Dies ist im weit überwiegenden Umfang der Fall. Im Berichtsjahr hat der Drang, Systeme Künstlicher Intelligenz für Verwaltungstätigkeiten einzusetzen, zu neuen Datenschutzfragen geführt (Kap. 5.1). Aber für die konventionelle Datenverarbeitung ergeben sich immer wieder grundlegende Fragen zum Datenschutz (Kap. 5.2). Zur Benennung und zur Stellung von kommunalen Datenschutzbeauftragten habe ich eine Fragebogenaktion durchgeführt, die zu interessanten Ergebnissen geführt hat (Kap. 5.3). Besondere Fragen entstanden zum Datenschutz bei politischen Informationssystemen (Kap. 5.4). Zum Datenschutz in der Rehabilitation und Teilhabe (SGB IX) konnte ein bundesweites Projekt, an dem ich beteiligt war, abgeschlossen werden (Kap. 5.5).

5.1
Datenschutz als Vertrauensbasis für Künstliche Intelligenz in der Verwaltung

Mit dem Einsatz von Künstlicher Intelligenz (KI) in der öffentlichen Verwaltung gehen viele Hoffnungen einher: Sie soll Dienstleistungen effizienter gestalten, Ressourcen sparen und Wissen besser nutzbar machen. Gleichzeitig soll KI helfen, den wachsenden Personalmangel einzudämmen. Auch ich sehe die Möglichkeiten, die sich durch den Einsatz von KI für eine moderne Verwaltung ergeben. Gleichwohl gibt es datenschutzrechtliche Herausforderungen, die es zu lösen gilt. KI kann ihr volles Potenzial nur entfalten, wenn Bürgerinnen und Bürger ihr vertrauen. Hierbei leistet die DS-GVO einen wichtigen Beitrag, indem sie einen einheitlichen Rechtsrahmen im Bereich des Datenschutzes in der Union setzt und für die Verarbeitung personenbezogener Daten eine Vertrauensbasis schafft. S. zu Datenschutz und Künstlicher Intelligenz auch Kap. 8.1 (aktuelle Entwicklungen) und Kap. 2 (EDSA-Beschluss zu Sprachmodellen).

Ich sehe es als meine Aufgabe an, den Einsatz von KI-Systemen in der öffentlichen Verwaltung in Hessen unter Berücksichtigung des Schutzes personenbezogener Daten zielführend und konstruktiv zu begleiten. Hierzu fasse ich einige grundsätzliche Erwägungen und erste Praxiserfahrungen zusammen.

Ist das KI? Notwendigkeit der Standortbestimmung im Technologiedschungel

Der Auseinandersetzung mit datenschutzrechtlichen Fragestellungen im KI-Kontext vorgelagert ist die Frage eines einheitlichen Verständnisses des Begriffs „Künstliche Intelligenz“.

Art. 3 Nr. 1 der Verordnung (EU) 2024/1689 vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung mehrerer Verordnungen und Richtlinien (Verordnung über künstliche Intelligenz – KI-VO) enthält eine Definition. Danach ist ein

> „‚KI-System‘ ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können.“

Etwas ausführlicher und verständlicher ist die Definition des Fraunhofer Instituts für kognitive Systeme:

> „Künstliche Intelligenz (KI) imitiert menschliche kognitive Fähigkeiten, indem sie Informationen aus Eingabedaten erkennt und sortiert. Diese Intelligenz kann auf programmierten Abläufen basieren oder durch maschinelles Lernen erzeugt werden. Bei maschinellen Lernverfahren erlernt ein Algorithmus durch Wiederholung, selbstständig eine Aufgabe zu erfüllen. Die Maschine orientiert sich dabei an einem vorgegebenen Gütekriterium und dem Informationsgehalt der Daten. Anders als bei herkömmlichen Algorithmen wird kein Lösungsweg modelliert. Der Computer lernt selbstständig die Struktur der Daten zu erkennen.
>
> Ein Untergebiet von maschinellem Lernen sind neuronale Netze. Diese Lernalgorithmen sind von Nervenzellenverbindungen im menschlichen Gehirn inspiriert. Das Gehirn verarbeitet Informationen über Neuronen und Synapsen. Analog dazu bestehen künstliche neuronale Netze aus mehreren Reihen von Datenknoten, die mit gewichteten Verbindungen untereinander vernetzt sind. Das neuronale Netz wird trainiert, indem ihm immer wieder Daten vorgelegt werden. Durch diese Wiederholung lernt das neuronale Netz die Daten jedes Mal exakter einzuordnen. Das funktioniert, indem die Gewichtung für die einzelnen Verbindungen zwischen den Neuronen-Schichten immer wieder angepasst werden. Das in den Lerndurchläufen erzeugte Modell kann dann auch auf Daten angewandt werden, die die Künstliche Intelligenz im Training noch nicht kennengelernt hat. Haben neuronale Netze verdeckte Neuronen-Schichten, die nicht direkt an die Eingabe- oder Ausgabe-Schicht gekoppelt sind, werden sie ‚Deep Neural Networks‘ genannt. Deep Neural Networks können Hunderttausend oder Millionen Neuronen-Schichten aufweisen. Damit können beim sogenannten ‚Deep Learning‘ immer komplexere Probleme gelöst werden.“

Ein wesentlicher Unterschied zu klassischen, deterministischen Systemen liegt in der Entscheidungsfindung: Während herkömmliche Algorithmen feste Regeln befolgen (z. B.: Wenn A, dann B), arbeitet KI probabilistisch. Das bedeutet, dass sie Wahrscheinlichkeiten berechnet, z. B. „Wenn A, dann mit einer Wahrscheinlichkeit von 70 % B, von 20 % C und von 10 % D".

Meine Empfehlung für Verantwortliche lautet daher, genau zu prüfen, ob das System, das zum Einsatz kommen soll, sich tatsächlich probabilistisch verhält und damit als KI zu bewerten ist, oder ob es sich „nur" um ein innovatives, gleichwohl deterministisch geprägtes Entscheidungssystem handelt.

Auch bei KI-Systemen gilt: Entscheidend ist der Personenbezug!

Gemäß Art. 8 Abs. 1 GRCh hat jede Person das Recht auf den Schutz der sie betreffenden personenbezogenen Daten. Dementsprechend ist der Anwendungsbereich der DS-GVO nach ihrem Art. 2 Abs. 1 auf die Verarbeitung personenbezogener Daten beschränkt. Daher gilt auch bei KI-Systemen: Maßgebend für die Anwendung des Datenschutzrechts ist die Verarbeitung personenbezogener Daten. Verantwortliche sollten daher genau prüfen, ob ein KI-System personenbezogene Daten verarbeitet oder nicht. Denn die Frage des Personenbezugs ist maßgebend für die Anwendbarkeit des Datenschutzrechts und sich daraus ergebender Pflichten seitens der Verantwortlichen. Häufig wird unterschätzt, dass bereits wenige indirekte Informationen ausreichen können, um eine Person zu identifizieren. Zudem muss der Personenbezug bei KI-Systemen aus verschiedenen Perspektiven betrachtet werden – etwa von jenen, deren Daten für das Training genutzt wurden, und jenen, deren Daten beim Betrieb verarbeitet werden.

KI verändert die Verwirklichungsbedingungen des Datenschutzrechts

Die DS-GVO basiert auf einem deterministisch geprägten IT-Verständnis. Dies lässt sich etwa an den datenschutzrechtlichen Gestaltungsrechten veranschaulichen: In deterministisch geprägten IT-Systemen kann die Wahrnehmung der datenschutzrechtlichen Gestaltungsrechte vergleichsweise einfach umgesetzt werden, indem einzelne Parameter verändert oder gelöscht werden. Bei probabilistischen Systemen ist dies nicht ohne weiteres möglich. Denn hier genügt es nicht, einfach nur einen Parameter abzuändern oder zu löschen, damit das gewünschte Ergebnis erzielt wird. Der Einsatz von KI ändert daher die Verwirklichungsbedingungen des Datenschutzrechts. Es gilt somit, die Ziele der DS-GVO bei der Entwicklung und dem Einsatz von KI-Systemen bestmöglich zu gewährleisten, hierbei aber die geänderten

Rahmenbedingungen durch den technologischen Fortschritt zu berücksichtigen (s. hierzu auch Kap. 8.1).

Mögliche Einsatzszenarien von KI in der Verwaltung

Die Unterstützung der Verwaltung durch KI ist in vielen unterschiedlichen Szenarien und Fallgestaltungen denkbar. Im Kontext des Datenschutzrechts sind Verfahren unter Einsatz von KI denkbar, die intensiv in die Rechte und Freiheiten der hiervon betroffenen Personen eingreifen (z. B. KI-Einsatz im Beschäftigungsverhältnis). Möglich ist aber auch, dass Verfahren unter Nutzung von KI in der Verwaltung zum Einsatz kommen, die überhaupt keine Verarbeitung personenbezogener Daten zum Gegenstand haben (z. B. KI-unterstützte Auswertung von Luftmessnetzdaten). Kurzum: Die Bandbreite möglicher Einsatzszenarien ist groß. Hier einige Beispiele, die aktuell diskutiert werden: Hilfestellung bei der Vorgangsbearbeitung durch automatisierte Dokumentenverarbeitung (Analyse, Kategorisierung und Extraktion relevanter Informationen), Unterstützung bei Bürgeranfragen durch Chatbots und virtuelle Assistenten, automatische Bearbeitung wiederkehrender Verwaltungsaufgaben (Prozessautomatisierung), Datenanalyse und Prognosen, Texterstellung und Textbearbeitung, Spracherkennung und Übersetzung. In der hessischen Verwaltung werden teilweise bereits KI-Technologien aus diesen Bereichen eingesetzt, z. B.:

In der Justiz:

– „Codefy“ soll Richterinnen und Richter bei der Strukturierung und Durchsuchung umfangreicher Verfahrensakten unterstützen.
– „FraUKe“ unterstützt bei Massenverfahren, wie Fluggastrechteverfahren. Es handelt sich um ein Richterassistenzsystem, bei dem eine Künstliche Intelligenz in der Urteilfindung assistiert.
– KI-Anonymisierungstool soll bei der Anonymisierung von Urteilen unterstützen und dadurch dazu beitragen, dass Gerichtsentscheidungen schnell und effizient für eine Veröffentlichung vorbereitet werden können.

Bei der Polizei:

– KI-Einsatz zur forensischen Analyse großer Datenmengen, z. B. zur Bekämpfung von Kinderpornografie.

Bei der Stadt Frankfurt am Main

– Verkehrsmanagement: Mithilfe von Echtzeitdaten und KI-Algorithmen werden Verkehrsflüsse analysiert und optimiert.

Beim Landeswohlfahrtsverband Hessen:

– KI-basierter virtueller Assistent (Chatbot), um Kundenanfragen zu beantworten.

Neue Technologie – bekanntes Datenschutzrecht

Auch wenn es sich bei KI um eine neue Art von Technologie handelt: Verantwortliche müssen die Bestimmungen der DS-GVO bereits seit 2018 beachten. Ich rate Verantwortlichen daher, sich auf ihr erlerntes Rüstzeug zu verlassen und hiervon ausgehend den Einsatz von KI-Technologien in Datenverarbeitungsverfahren zu beurteilen. Basierend auf den bisher vorliegenden Erfahrungen empfehle ich, bei der Prüfung, ob die Bestimmungen des Datenschutzrechts eingehalten sind, insbesondere die folgenden Gesichtspunkte ausreichend zu berücksichtigen:

– Zwecke und Rechtsgrundlagen für die Verarbeitung personenbezogener Daten
– Transparenz
– Gewährleistung von Betroffenenrechten
– Datenschutzrechtliche Verantwortlichkeit
– Notwendigkeit der Durchführung einer Datenschutz-Folgenabschätzung
– Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
– Datensicherheit

Die DSK und der EDSA haben bereits erste Empfehlungen zum KI-Einsatz und Datenschutz herausgegeben, die sich u. a. mit den zuvor genannten Themen beschäftigen:

– Stellungnahme des EDSA zu KI-Modellen vom 17. Dezember 2024: https://www.edpb.europa.eu/news/news/2024/edpb-opinion-ai-models-gdpr-principles-support-responsible-ai_de (s. hierzu auch Kap. 2),
– DSK Orientierungshilfe „Künstliche Intelligenz und Datenschutz“ der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. Mai 2024: https://www.datenschutzkonferenz-online.de/orientierungshilfen.html,

– Bayerisches Landesamt für Datenschutzaufsicht „Datenschutzkonforme Künstliche Intelligenz, Checkliste“: https://www.lda.bayern.de/media/ki_checkliste.pdf,
– Hamburgischer Beauftragten für Datenschutz und Informationsfreiheit „Checkliste zum Einsatz LLM-basierter Chatbots“: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/20231113_Checkliste_LLM_Chatbots_DE.pdf,
– Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Diskussionspapier „Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz“: https://www.baden-wuerttemberg.datenschutz.de/rechtsgrundlagen-datenschutz-ki/.

Neue Technologie – neuer EU-Rechtsakt: die KI-Verordnung

Verantwortliche stehen vor der Herausforderung, neben den Bestimmungen des Datenschutzrechts, insbesondere der DS-GVO, auch die Bestimmungen der KI-Verordnung beachten zu müssen. Neben dem Datenschutzrecht gibt es also neue regulatorische Anforderungen (z. B. bezogen auf Transparenz und Erklärbarkeit, Bias und Diskriminierung und Dokumentationspflichten) die erfüllt werden müssen. Zudem gibt es komplexe Zuständigkeits- und Abgrenzungsfragen, die noch geklärt werden müssen.

Eigene Aktivitäten zum Thema KI-Einsatz und Datenschutz

Auf Ebene der DSK beteilige ich mich in dem neu gegründeten Arbeitskreis „Künstliche Intelligenz“. Auf Landesebene wirke ich im Arbeitskreis „KI und Innovation“ mit. Außerdem waren KI-Themen ein Schwerpunktthema des „3. Datenschutztags für behördliche, kommunale und betriebliche Datenschutzbeauftragte Hessen und Rheinland-Pfalz“, den ich gemeinsam mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. einmal jährlich veranstalte (s. Kap. 15).

Für die Zukunft beabsichtige ich, meine Aktivitäten im öffentlichen Bereich weiter zu verstärken und dies auch in der Organisationsstruktur meiner Behörde sowie durch Beiträge auf meiner Internetpräsenz nach außen sichtbar zu machen. Zudem beabsichtige ich, für hessische Kommunen Fortbildungsmöglichkeiten zum Thema „KI-Einsatz in der Verwaltung und Datenschutz“ anzubieten.

„Es ist nicht genug, zu wissen, man muss auch anwenden. Es ist nicht genug, zu wollen, man muss auch tun.“ (Goethe)

Verwaltungsmodernisierung durch KI bietet Chancen, braucht aber eine Vertrauensbasis, damit sie ihre Potenziale entfalten kann. Mit der DS-GVO und KI-VO hat der europäische Gesetzgeber zwei Rechtsakte verabschiedet, die diese Vertrauensbasis schaffen. Wie für jedes andere IT-Projekt gilt auch hier: Verantwortliche sollten sich frühzeitig, schon in der Planungsphase neuer KI-Anwendungen mit den Anforderungen der DS-GVO und der KI-VO auseinandersetzen, damit etwaigen Herausforderungen frühzeitig begegnet werden kann und diese sich nicht zu einem Projektrisiko entwickeln.

5.2
Rechtsgrundlagen für Datenverarbeitungen in Kommunen

Für kommunale Stellen bestehen verschiedene Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Wenngleich sich Kommunen in aller Regel an die datenschutzrechtlichen Vorgaben halten, sind in der Praxis mitunter Unklarheiten hinsichtlich der einschlägigen Rechtsgrundlage festzustellen. Im Folgenden werden daher die relevantesten Rechtsgrundlagen und ihre wesentlichen Anforderungen aufgezeigt (s. zu einzelnen Fallkonstellationen 51. Tätigkeitsbericht, Kap. 7.2).

Allgemeine Anforderungen an eine Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfordert entsprechend Art. 5 Abs. 1 Buchst. a und Art. 6 DS-GVO eine Rechtsgrundlage.

Art. 5 DS-GVO

(1) Personenbezogene Daten müssen

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

Art. 6 DS-GVO

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

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

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

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

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

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

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

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

(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.

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

Für kommunale Stellen kommen insbesondere die Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO sowie die Erfüllung der in ihrer Zuständigkeit liegenden Aufgabe gemäß Art. 6 Abs. 1

UAbs. 1 Buchst. e DS-GVO in Betracht. In diesen Fällen muss zudem eine Rechtsgrundlage des Unionsrechts oder des mitgliedstaatlichen Rechts entsprechend Abs. 3 Satz 1 einschlägig sein. Neben formellen Gesetzen sind ausweislich des Erwägungsgrunds 41 DS-GVO auch Rechtsverordnungen und Satzungen erfasst.

Rechtsgrundlagen können häufig dem Fachrecht entnommen werden. Detaillierte Regelungen enthält zum Beispiel das Melderecht insbesondere zu Datenübermittlungen zwischen öffentlichen Stellen gemäß §§ 33 ff. BMG sowie Melderegisterauskünften nach §§ 44 ff. BMG (s. 51. Tätigkeitsbericht, Kap. 7.2; sowie HDBI, Rechte der Betroffenen bei Meldebehörden, https://datenschutz.hessen.de/datenschutz/kommunen/rechte-der-betroffenen-bei-meldebehoerden; s. zu Melderegisterauskünften bei Wahlen und Abstimmungen 52. Tätigkeitsbericht, Kap. 5.5; HBDI, Datenschutz bei Wahl- und Abstimmungswerbung, https://datenschutz.hessen.de/datenschutz/kommunen/datenschutz-bei-wahl-und-abstimmungswerbung; sowie Rapp/Roßnagel/Franke, ZD 2023, 247 ff.). Weitere Rechtsgrundlagen beinhalten etwa §§ 86 ff. AufenthG, §§ 67a ff. SGB X, § 8a OZG sowie § 36 GVG (s. 52. Tätigkeitsbericht, Kap. 5.6). Auch finden sich im hessischen Kommunalrecht entsprechende Tatbestände (s. zu Bürgerbegehren HBDI, Datenschutz bei Bürgerbegehren, https://datenschutz.hessen.de/datenschutz/kommunen/datenschutz-bei-buergerbegehren; sowie ausführlich Rapp, KommJur 2023, 361 ff.; 401 ff.), bei politischen Informationssystemen kann auf Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 DS-GVO in Verbindung mit § 52 HGO zurückgegriffen werden (s. Kap. 5.4 sowie HBDI, Datenschutz bei politischen Informationssystemen, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2024-07/handreichuing_datenschutz_bei_politischen_informationssystemen_240724.pdf).

Soweit keine fachrechtliche Rechtsgrundlage einschlägig ist, kann gemäß § 1 Abs. 2 HDSIG ggf. auf das HDSIG zurückgegriffen werden.

§ 1 HDSIG

(2) Andere Rechtsvorschriften über den Datenschutz gehen vorbehaltlich des Abs. 3 den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

Dieses enthält u. a. Rechtsgrundlagen gemäß § 22 Abs. 1 in Verbindung mit § 21 HDSIG für die Übermittlung personenbezogener Daten an öffentliche

Stellen sowie nach § 22 Abs. 2 HDSIG für die Übermittlung personenbezogener Daten an nicht öffentliche Stellen. Die subsidiäre Generalklausel des § 3 Abs. 1 HDSIG sollte wegen ihrer mangelnden Bestimmtheit und hohen Abstraktheit sowie umstrittenen Europarechtskonformität nur ausnahmsweise bei Datenverarbeitungen mit sehr geringer Eingriffsintensität angewendet werden (s. zu der inhaltsgleichen Regelung des § 3 BDSG BVerwG, Urt. vom 20.3.2024, 6 C 8.22). § 23 HDSIG enthält (s. zur Personaldatenverarbeitung die vorrangigen Regelungen der §§ 86 ff. HBG) Maßgaben für die Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses (s. EuGH, Urt. vom 30.3.2023, C-34/21; HBDI, Handreichung zur Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023, C-34/21, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-05/handreichung_beschaeftigtendatenschutz_eugh-urteil.pdf sowie Roßnagel/Wetzstein/Horlbeck, DuD 2023, 429 ff.).

§ 4 HDSIG beinhaltet eine Rechtsgrundlage für die Videoüberwachung öffentlich zugänglicher Räume. Die Vorschrift kann jedoch keine Ermächtigungsgrundlage für grundrechtsintensive Datenverarbeitungen sein, da sie gemäß § 1 Abs. 2 HDSIG von zahlreichen spezialgesetzlichen Regelungen verdrängt wird und es ihr an Bestimmtheit mangelt (s. Rapp, in: Ronellenfitsch, HDSIG, 19. Nl. 2024, § 4 Rn. 8 ff., 24; Spiecker gen. Döhmann, in: Roßnagel, HDSIG, 2021, § 4 Rn. 41 ff.).

Die Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DS-GVO stellt ausweislich des Erwägungsgrunds 43 Satz 1 DS-GVO gegenüber kommunalen Stellen keine geeignete Rechtsgrundlage dar, da es infolge des Über- und Unterordnungsverhältnisses zwischen Staat und Bürger in der Regel an der Freiwilligkeit der Einwilligung fehlt. Soweit kein „klares Ungleichgewicht“ zwischen Behörde und Bürgerin oder Bürger besteht (etwa bei optional digital verfügbaren Verwaltungsleistungen), kann die Einwilligung dagegen – unter Wahrung der weiteren Voraussetzungen – grundsätzlich eine Datenverarbeitung erlauben. Aufgrund der jederzeitigen Widerrufbarkeit der Einwilligung und der damit einhergehenden fehlenden Rechtmäßigkeit der Verarbeitung für die Zukunft entsprechend Art. 7 Abs. 3 DS-GVO sollte die Einwilligung jedoch stets kritisch auf ihre Praxistauglichkeit hin überprüft werden.

Kommunale Stellen können sich entsprechend des Unterabsatzes 2 in aller Regel nicht auf ein „berechtigtes Interesse“ im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO berufen. Ausweislich des Erwägungsgrunds 47 Satz 5 DS-GVO obliegt es dem Gesetzgeber, per Rechtsvorschrift die Rechtsgrundlage für die Datenverarbeitung durch die Behörden zu schaffen, so dass diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten sollte, welche diese in Erfüllung ihrer Aufgaben vornehmen. Im Falle

der Teilnahme von kommunalen Stellen am Privatrechtsverkehr oder für nichthoheitliches Handeln auf der Ebene der Gleichberechtigung kommt die Verarbeitungsbefugnis dagegen in Betracht.

Besondere Anforderungen bei sensiblen Daten und Drittlandübermittlungen

Für bestimmte Verarbeitungssituationen sind neben den Vorgaben der Art. 5 Abs. 1 Buchst. a und Art. 6 DS-GVO weitere Maßgaben zu berücksichtigen.

Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO (etwa politische Meinungen oder Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO) ist grundsätzlich untersagt. Sie ist zulässig, sofern – neben einem Tatbestand des Art. 6 Abs. 1 DS-GVO – auch eine Ausnahme nach Absatz 2 (s. auch § 20 HDSIG) einschlägig ist (s. EuGH, Urt. vom 21.12.2023, C-667/21). Dies kann etwa nach Buchstabe a eine „ausdrückliche Einwilligung", gemäß Buchstabe e eine „offensichtliche Veröffentlichung" seitens der betroffenen Person oder nach Buchstabe g ein „erhebliches öffentliches Interesse" sein.

Bei der Übermittlung von personenbezogenen Daten an Drittländer (Staaten außerhalb des EWR) oder an internationale Organisationen im Sinne des Art. 4 Nr. 26 DS-GVO sind zudem die Anforderungen der Art. 44 ff. DS-GVO zu berücksichtigen. Es kommen eine Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses der Europäischen Kommission gemäß Art. 45 DS-GVO (s. EuGH, Urt. vom 16.7.2020, C-311/18; sowie HBDI, Angemessenheitsbeschluss zum EU-US Data Privacy Framework, https://datenschutz.hessen.de/datenschutz/internationaler-datentransfer/eu-us-data-privacy-framework), eine Datenübermittlung vorbehaltlich geeigneter Garantien nach Art. 46 DS-GVO (etwa Standarddatenschutzklauseln) sowie Ausnahmen für bestimmte Fälle nach Art. 49 DS-GVO (etwa eine ausdrückliche Einwilligung) in Betracht.

Fazit

Die Ausführungen zeigen, dass kommunalen Stellen vielfältige Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zur Verfügung stehen. Je nach Verarbeitungssituation sind die Anforderungen mitunter sehr unterschiedlich. Aufgrund der Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO sind die Rechtsgrundlagen zu dokumentieren und etwa bei den Betroffenenrechten der Art. 12 ff. DS-GVO sowie in dem Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO entsprechend abzubilden.

Art. 5 DS-GVO

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Auf meiner Website (s. https://datenschutz.hessen.de/datenschutz/kommunen/datenschutz-in-kommunen) biete ich kommunalen Stellen eine erste Übersicht auch über die weiteren Anforderungen des Datenschutzes (s. vertiefend Rapp, KommJur 2024, 401 ff.).

5.3
Fragebogen zu kommunalen Datenschutzbeauftragten

Datenschutzbeauftragte erfüllen wichtige Aufgaben bei der Kontrolle und Einhaltung des Datenschutzes in den hessischen Kommunen. Daher habe ich mir mittels eines an 80 Kommunen versendeten Fragebogens einen Überblick hinsichtlich der Umsetzung der Art. 37 bis 39 DS-GVO und §§ 5 bis 7 HDSIG verschafft. Es zeigte sich, dass die Maßgaben zwar überwiegend eingehalten werden, in einzelnen Bereichen jedoch Mängel bestehen. Diese betreffen insbesondere die fehlende Benennung einer Vertretung sowie eine unzureichende Ausstattung mit Ressourcen.

Ablauf der Prüfung

Der Fragebogen wurde mit E-Mail vom 11. Juni 2024 (mit Frist bis zum 2. Juli 2024) an 80 über ganz Hessen verteilte kleine und mittelgroße Kommunen versendet. Dieser enthielt folgende Fragen:

1. Haben Sie eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benannt?
2. Haben Sie eine Vertreterin oder einen Vertreter der oder des Datenschutzbeauftragten benannt?
3. Seit wann ist die Datenschutzbeauftragte oder der Datenschutzbeauftragte benannt?
4. Seit wann ist die Vertreterin oder der Vertreter der oder des Datenschutzbeauftragten benannt?
5. Bitte teilen Sie mir Name und Erreichbarkeit (etwa Telefonnummer, Postanschrift, E-Mail-Adresse) der oder des Datenschutzbeauftragten mit.
6. Bitte teilen Sie mir Name und Erreichbarkeit (etwa Telefonnummer, Postanschrift, E-Mail-Adresse) der Vertreterin oder des Vertreters mit.

7. Haben Sie die oder den Datenschutzbeauftragten sowie die Vertreterin oder den Vertreter bei meiner Behörde gemeldet? Sofern dies nicht geschehen ist, bitte ich Sie, dies – möglichst über meine Website (https://datenschutz.hessen.de/service/meldung-eines-datenschutzbeauftragten) – nachzuholen.
8. Welche Ressourcen werden der oder dem Datenschutzbeauftragten zu der Aufrechterhaltung der Fachkunde (etwa Teilnahme an Schulungen oder Konferenzen, Fachbücher) zur Verfügung gestellt?
9. Bitte legen Sie mir die letzten drei Fortbildungsnachweise der oder des Datenschutzbeauftragten in Kopie vor.
10. Welcher Stellenanteil steht für den Datenschutz zur Verfügung?

Die Auswahl der Kommunen erfolgte zufällig. Insbesondere waren damit keine Verstöße, Versäumnisse oder Ähnliches der behördlichen Datenschutzbeauftragten verbunden.

Auf meine E-Mail vom 11. Juni 2024 haben 49 Kommunen geantwortet. Die übrigen 31 Kommunen habe ich mit E-Mail vom 9. Juli 2024 (Frist bis zum 19. Juli 2024) an die Beantwortung meiner Fragen erinnert. Daraufhin haben weitere 22 Kommunen geantwortet. Die verbleibenden neun Kommunen habe ich per Briefpost mit Schreiben vom 1. August 2024 (Frist bis zum 15. August 2024) erneut erinnert und weitere aufsichtsrechtliche Maßnahmen angedroht. Daraufhin haben weitere acht Kommunen geantwortet.

Mit E-Mail vom 22. August 2024 habe ich alle Kommunen über die Auswertung des Fragebogens informiert sowie praktische und rechtliche Empfehlungen gegeben.

Gegenüber der Kommune, die nicht auf meine Nachrichten geantwortet hat, habe ich mit Schreiben vom 22. August 2024 wegen mangelnder Zusammenarbeit mit der Aufsichtsbehörde gemäß Art. 31 DS-GVO eine Verwarnung nach Art. 58 Abs. 2 Buchst. b DS-GVO erteilt. Die Ausübung meiner Befugnis nach Art. 58 Abs. 2 Buchst. b DS-GVO habe ich gemäß § 14 Abs. 1 Satz 5 HDSIG der nach § 136 Abs. 3 HGO zuständigen Rechts- und Fachaufsichtsbehörde (der Landrat als Behörde der Landesverwaltung) mitgeteilt. Daraufhin hat auch diese Kommune am 30. August 2024 auf den Fragebogen geantwortet.

Art. 31 DS-GVO

Der Verantwortliche und der Auftragsverarbeiter und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Art. 58 DS-GVO

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten, (…)

b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat, (…).

§ 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 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. (…).

§ 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.

(5) Ist in einer vom Landrat als Behörde der Landesverwaltung als Aufsichtsbehörde zu entscheidenden Angelegenheit der Landkreis zugleich als Gemeindeverband beteiligt, entscheidet die obere Aufsichtsbehörde. Sind an Angelegenheiten, die nach diesem Gesetz der Genehmigung oder der Entscheidung der Aufsichtsbehörde bedürfen, Gemeinden mehrerer Landkreise oder Regierungsbezirke beteiligt, ist die gemeinsame nächst höhere Aufsichtsbehörde oder die von dieser bestimmte Aufsichtsbehörde zuständig.

Ergebnisse der Prüfung

Nachfolgend möchte ich relevante Erkenntnisse der Prüfung beleuchten.

Eine Benennung der oder des Datenschutzbeauftragten ist fast ausnahmslos erfolgt. In wenigen Einzelfällen bestanden lediglich kurzfristige Vakanzen infolge personeller Neubesetzungen. Demgegenüber ist in etwa einem Drittel der Kommunen eine Vertreterin oder ein Vertreter der oder des Datenschutzbeauftragten nicht benannt worden. Diese Benennung ist gemäß § 5 Abs. 1 HDSIG verpflichtend. Bei der Vertretung handelt es sich aufgrund der gestiegenen Anforderungen an die Aufgaben nach der DS-GVO nicht um eine bloße Abwesenheitsvertretung für Situationen, in denen die oder der Datenschutzbeauftragte (etwa durch Urlaub, Krankheit oder Ähnliches) verhindert oder abwesend ist (s. Rapp, in: Ronellenfitsch, HDSIG, 19. Nl. 2024, § 5 Rn. 18 f.; Wilmer, in: Roßnagel, HDSIG, § 5 Rn. 16).

Mitunter ist die gemäß Art. 37 Abs. 7 DS-GVO, § 5 Abs. 5 HDSIG verpflichtende Mitteilung der Kontaktdaten der oder des Datenschutzbeauftragten an meine Behörde nicht oder nicht vollständig erfolgt. Diese sollte möglichst (ggf. als Änderungsmitteilung) mittels des Formulars auf meiner Website erfolgen (s. HBDI, https://datenschutz.hessen.de/service/meldung-eines-datenschutzbeauftragten).

Die Angaben zu den zu der Aufrechterhaltung der Fachkunde zur Verfügung gestellten Ressourcen sind teilweise sehr vage. Der Stellenanteil der internen Datenschutzbeauftragten ist mitunter sehr gering. Art. 38 Abs. 2 DS-GVO, § 6 Abs. 2 HDSIG bedingen eine Ausstattung mit den erforderlichen Ressourcen durch die Kommune. Eine konkrete Stundenzahl des für den Datenschutz erforderlichen Zeitaufwandes ist schwierig zu benennen. Diese ist insbesondere von der Größe der Kommune und von dem Reifegrad der Datenschutzorganisation abhängig. Überdies müssen sich die Ressourcen an Umfang, Komplexität und Sensibilität der verarbeiteten personenbezogenen Daten, der Anzahl der betroffenen Personen sowie der Risiken für die Rechte und Freiheiten betroffener Personen orientieren (s. Rapp, in: Ronellenfitsch, HDSIG, 19. Nl. 2024, § 6 Rn. 12 f.; Wilmer, in: Roßnagel, HDSIG, § 6 Rn. 15f.). Losgelöst von der konkreten Stundenzahl sollte der oder dem Datenschutzbeauftragten jedenfalls ein festes Zeitkontingent für die Erfüllung datenschutzrechtlicher Aufgaben zur Verfügung stehen. Denkbar ist zudem die Benennung einer oder eines gemeinsamen Datenschutzbeauftragten etwa im Rahmen der interkommunalen Zusammenarbeit entsprechend Art. 37 Abs. 3 DS-GVO, § 5 Abs. 2 HDSIG. Hinsichtlich des einzuräumenden Zeitaufwandes stehe ich gerne beratend zur Verfügung.

Stellenweise ist die Teilnahme an Schulungen (spezifisch zum Datenschutzrecht) unzureichend. Neben einer „Grundausbildung“ vor der Benennung

zum Datenschutzbeauftragten sollten fortwährend mindestens zwei Tage im Jahr für Fortbildungen (Seminare, Schulungen oder ähnliches) aufgewendet werden. Das Fachwissen muss auf dem Niveau, das für die Aufgabenerfüllung erforderlich ist, gehalten werden, so dass erhöhte Anforderungen (etwa durch Veränderungen bei der Verarbeitung personenbezogener Daten oder der Risiken) eine Verbesserung des Fachwissens bedingen können (s. Rapp, in: Ronellenfitsch, HDSIG, 19. Nl. 2024, § 6 Rn. 15.; Wilmer, in: Roßnagel, HDSIG, § 6 Rn. 15). Auch Beschäftigte meiner Behörde bieten Schulungen zu verschiedenen Themen des Datenschutzes an (s. HBDI, https://datenschutz.hessen.de/service/schulungen-0). Überdies empfiehlt sich die Teilnahme an dem einmal jährlich stattfindenden Datenschutztag Hessen und Rheinland-Pfalz (s. HBDI, https://datenschutz.hessen.de/presse/grosses-interesse-am-3-datenschutztag-hessen-rheinland-pfalz), der neben praxisrelevanten Vorträgen auch Möglichkeiten zum „Netzwerken“ bietet. Des Weiteren sollten die Kenntnisse mittels Selbststudiums kontinuierlich vertieft und erweitert werden. Dafür finden sich auch auf meiner Website verschiedene Unterlagen und Verweise auf weiterführende Informationen.

Wenn auch nicht ausdrücklich im Fragebogen adressiert, waren bei einzelnen Kommunen Interessenkonflikte der Datenschutzbeauftragten gemäß Art. 38 Abs. 6 DS-GVO und § 7 Abs. 2 HDSIG ersichtlich (s. 51. Tätigkeitsbericht, Kap. 7.6; sowie ausführlich Rapp, ZD 2024, 193 ff.). In einer Kommune war etwa die Bürgermeisterin zugleich als Datenschutzbeauftragte benannt, in anderen hatten Datenschutzbeauftragte zugleich herausgehobene Leitungstätigkeiten inne (etwa die Leitung der Personalverwaltung). Wenngleich die Vermeidung jedweden Interessenkonflikts insbesondere angesichts knapper personeller und finanzieller Ressourcen in kleineren Kommunen äußerst schwierig ist, lassen sich etwa mittels der Benennung einer oder eines gemeinsamen Datenschutzbeauftragten oder einer oder eines externen Datenschutzbeauftragten in aller Regel Lösungen finden.

Fazit

Ausweislich der Rückmeldungen besteht insgesamt trotz der aufgezeigten Mängel ein jedenfalls grundlegendes Verständnis für die Stellung und die Aufgaben der Datenschutzbeauftragten in den hessischen Kommunen. Es ist ausdrücklich darauf hinzuweisen, dass für die Einhaltung der Maßgaben der Art. 37 bis 39 DS-GVO und §§ 5 bis 7 HDSIG die Kommune gemäß Art. 4 Nr. 7 DS-GVO und nicht die oder der Datenschutzbeauftragte verantwortlich ist.

Art. 4 Nr. 7 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

7. „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; (…)

Zwecks Erreichung weiterer Verbesserungen werde ich auch zukünftig die Umsetzung der Anforderungen an die behördlichen Datenschutzbeauftragten beratend (etwa durch einzelne persönliche Gespräche mit Datenschutzbeauftragten) begleiten und diese (ggf. auch mittels Vor-Ort-Terminen) näher überprüfen.

Weiterführende Informationen können überdies meinem Arbeitspapier „Behördliche und betriebliche Datenschutzbeauftragte" entnommen werden (s. HBDI, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-10/behoerdliche_und_betriebliche_datenschutzbeauftragte_231009_1.pdf).

5.4
Datenschutz bei politischen Informationssystemen

Politische Informationssysteme (auch Gremieninformationssysteme / Ratsinformationssysteme genannt) dienen dem Informationsinteresse der Bürgerinnen und Bürger und einem transparenten politischen Willensbildungsprozess. Zugleich muss das Recht auf informationelle Selbstbestimmung der betroffenen Personen geschützt werden. Im Berichtszeitraum erreichten mich erneut mehrere diesbezügliche Anfragen und Beschwerden (s. zuletzt 52. Tätigkeitsbericht, Kap. 5.3; 50. Tätigkeitsbericht, Kap. 8.2).

Unterlagen von Stadtverordneten

Im Rahmen einer Beschwerde wurde mir folgender Sachverhalt mitgeteilt: In einer öffentlichen Sitzung der Stadtverordnetenversammlung einer hessischen Stadt erfolgte eine Diskussion über die Vereinbarkeit des Mandats als Stadtverordnete mit einem Beschäftigungsverhältnis. Der Vorgang wurde zudem in der städtischen Öffentlichkeit und in der Presse ausführlich erörtert. Die Stadtverwaltung stellte sodann Unterlagen der Stadtverordneten (anwaltliche Schreiben, Entgeltunterlagen und persönliche Dokumente) in den öffentlich einsehbaren Bereich des politischen Informationssystems ein. Diese enthielten diverse personenbezogene Daten der Stadtverordneten (u. a. private Anschrift, Geburtsdatum und Beurteilungen). Infolge der Aufforderung des Fraktionsvorsitzenden und unter Beteiligung des behörd-

lichen Datenschutzbeauftragten wurden die Unterlagen aus dem öffentlich zugänglichen Bereich des politischen Informationssystems entfernt und in den nicht öffentlichen Bereich eingestellt, wobei die personenbezogenen Daten auf den betreffenden Unterlagen unkenntlich gemacht wurden.

Die Stadtverordnete reichte später Beschwerde bei mir ein. Zudem erfolgte seitens der Stadt eine Meldung hinsichtlich der Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO (eine Benachrichtigung der betroffenen Person nach Art. 34 DS-GVO erfolgte nicht, da diese bereits Kenntnis von dem Vorgang hatte). Im Rahmen der von mir eingeholten Stellungnahme wurde der Sachverhalt seitens der Stadt bestätigt.

Den Vorgang bewerte ich datenschutzrechtlich wie folgt:

Die Erörterung der Thematik in öffentlicher Sitzung der Stadtverordnetenversammlung ist datenschutzrechtlich nicht zu beanstanden. Vielmehr war es auch im Interesse der Mandatsträgerin und der Stadtverordnetenversammlung, dass die Öffentlichkeit darüber aufgeklärt wird und eine transparente Aufarbeitung erfolgt. Dies folgt aus dem Öffentlichkeitsgrundsatz gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 DS-GVO in Verbindung mit § 52 HGO (s. zu Rechtsgrundlagen für kommunale Stellen Rapp, KommJur 2024, 401, 404 f.).

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; (…)

§ 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.

Die Offenlegung der personenbezogenen Daten im politischen Informationssystem war jedoch nicht erforderlich. Vielmehr hätten diese vorab unkenntlich gemacht werden müssen. Aufgrund der Offenlegung lag ein Verstoß gegen die Rechtmäßigkeit der Verarbeitung gemäß Art. 5 Abs. 1 Buchst. a, Art. 6

DS-GVO sowie gegen den Grundsatz der Datenminimierung im Sinne des Art. 5 Abs. 1 Buchst. c DS-GVO vor.

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"); (…)

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung"); (…)

Aufgrund der plausiblen Darstellung der Stadt, dass es sich – insbesondere aufgrund der medial „aufgeheizten" Lage – um eine besondere Ausnahmesituation gehandelt habe, des kooperativen Verhaltens und der umgehenden Einleitung von erneuten Schulungs- und Sensibilisierungsmaßnahmen (insbesondere betreffend Datenschutzverletzungen und Risikobewertungen) sowie der Erstellung von Merkblättern für die beteiligten Personen durch den behördlichen Datenschutzbeauftragten verzichtete ich auf weitere aufsichtsrechtliche Maßnahmen gegenüber der Stadt (s. zu aufsichtsrechtlichen Maßnahmen gegenüber öffentlichen Stellen Friedrichsen/Rapp, ZD 2023, 535 ff.).

Der Vorgang zeigt überdies, dass eine Unterteilung des politischen Informationssystems in einen öffentlichen Bereich (etwa Sitzungstermine, Niederschriften der öffentlichen Tagesordnungspunkte sowie Angaben zu den Mandatsträgern) und einen geschlossenen Bereich mit weiteren Unterlagen (etwa Niederschriften der nicht öffentlichen Tagesordnungspunkte), auf den lediglich registrierte Nutzerinnen und Nutzer (zugehörige Mandatsträger) Zugriff erhalten, in aller Regel geboten ist.

Unterlagen der Bauleitplanung

Eine weitere Beschwerde hatte folgenden Sachverhalt zum Gegenstand: Anfang des Jahres 2020 wurde der Entwurf eines Bebauungsplans durch eine hessische Stadt öffentlich ausgelegt. Die Bürgerinnen und Bürger reichten in der Folgezeit Einwände und Anmerkungen zu diesem ein. Im September 2024 wurde zu der Sitzung des Bauausschusses ein Dokument mit Einwänden und Anmerkungen von Bürgerinnen und Bürgern in das politische Informationssystem eingestellt. Auf dem Dokument wurden die Namen der Bürgerinnen und Bürger unkenntlich gemacht. Deren Anschriften waren jedoch vollständig lesbar. Zu der Vorlage bei der Sitzung der Stadtverordnetenversammlung im September 2024 wurde das Dokument aktualisiert in

das politische Informationssystem hochgeladen. Auf dem Dokument waren diesmal sowohl die Namen als auch die Anschriften der Bürgerinnen und Bürger teilweise vollständig lesbar.

Der Beschwerdeführer wandte sich selbst an die Datenschutzbeauftragte der Stadt. Diese entschuldigte sich für den Sachverhalt und kündigte die Sensibilisierung der verantwortlichen Bereiche an. Der Beschwerdeführer legte zudem Beschwerde bei mir ein. Ich fragte bei der Stadt insbesondere nach, ob weiterhin personenbezogene Daten wie etwa Namen und Anschriften im politischen Informationssystem veröffentlicht oder auf den Dokumenten geschwärzt worden sind.

Daraufhin teilte mir die Stadt mit, dass in den nunmehr hochgeladenen Dokumenten die personenbezogenen Daten vollständig unkenntlich gemacht worden sind und damit die Offenlegung personenbezogener Daten vollständig behoben worden ist. Die beteiligten Beschäftigten der Stadt wurden für die Belange des Datenschutzes sensibilisiert. Diese werden zukünftig das Verfahren bei der Einstellung von Dokumenten im politischen Informationssystem entsprechend anpassen.

Mangels Rechtsgrundlage für die Offenlegung der personenbezogenen Daten im politischen Informationssystem gemäß Art. 5 Abs. 1 Buchst. a, Art. 6 DS-GVO lag ein datenschutzwidriges Verhalten der Stadt vor. Da die Stadt die Verstöße gegen den Datenschutz jedoch umgehend beseitigte und mir keine weiteren Offenlegungen personenbezogener Daten bekannt wurden, verzichtete ich auf weitergehende aufsichtsrechtliche Maßnahmen gegenüber der Stadt.

Der Vorfall zeigt, dass Dokumente vor der Veröffentlichung im politischen Informationssystem stets umfassend hinsichtlich der Bereinigung personenbezogener Daten zu überprüfen sind. Dies war vorliegend nur teilweise geschehen.

Unterlagen von Grundstücken

In einer anderen Beschwerde wurde die Veröffentlichung von Unterlagen, die auch Grundstücksinformationen und Rückkaufswerte von veräußerten Grundstücken enthielten, im politischen Informationssystem einer hessischen Stadt bemängelt. Aufgrund der detaillierten Darstellung der betroffenen Gebiete war es für Personen, die sich in der Gegend auskennen, möglich, Rückschlüsse auf die Eigentümerinnen und Eigentümer der Grundstücke zu ziehen.

In der von mir eingeholten Stellungnahme teilte die Stadt mit, dass der Verkauf und der Ankauf der Grundstücke die städtischen Gremien und die lokale

Öffentlichkeit (mitsamt Akteneinsichtsausschüssen sowie Bürgerinitiativen) über mehrere Jahre erheblich beschäftigt hat. Mit der Veröffentlichung der Unterlagen wollte die Stadt die Bürgerinnen und Bürger informieren und Transparenz herstellen.

Die Ausführungen der Stadt erachte ich datenschutzrechtlich für vertretbar. Die Offenlegung der personenbezogenen Daten (personenbeziehbare Grundstücksinformationen und Rückkaufswerte von veräußerten Grundstücken) in dem städtischen Gremieninformationssystem kann in diesem Fall auf Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und Abs. 3 DS-GVO in Verbindung mit dem Öffentlichkeitsprinzip gemäß § 52 HGO gestützt werden. Die Abwägung des individuellen Rechts auf informationelle Selbstbestimmung mit der kommunalpolitischen Transparenz und dem Informationsbedürfnis der Bürgerinnen und Bürger seitens der Stadt ist aufgrund der erheblichen kommunalpolitischen Bedeutung des Vorganges nicht zu bemängeln.

An dieser Stelle ist darauf hinzuweisen, dass der Begriff der „personenbezogenen Daten“ gemäß Art. 4 Nr. 1 DS-GVO, also „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (…) beziehen“, weit auszulegen ist und auch eine nur mittelbare Personenbeziehbarkeit ausreichen kann.

Art. 4 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

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

Namensnennung in Protokollen

Mich erreichte eine Anfrage hinsichtlich der Zulässigkeit der Offenlegung des Namens von Bürgerinnen und Bürgern in Protokollen von öffentlichen Sitzungen der Gemeindevertretung im Internet. Wenn Bürgerinnen und Bürger im Rahmen einer Gemeindevertretung (etwa bei einer „Fragestunde“) eine Frage stellen, ist die Nennung des Namens auch in öffentlichen Sitzungen in aller Regel datenschutzrechtlich unproblematisch. Dies folgt aus dem Öffentlichkeitsgrundsatz gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2, Abs. 3 DS-GVO in Verbindung mit § 52 HGO. Eine Offenlegung des Namens einer

Bürgerin oder eines Bürgers durch Veröffentlichung der Niederschrift im Sinne des § 61 HGO im politischen Informationssystem ist jedoch aufgrund der nahezu unbegrenzten Verfügbarkeit häufig unzulässig.

§ 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.

Vielmehr muss der Name in der Regel vorab etwa mittels Schwärzung unkenntlich gemacht werden. Es fehlt zumeist an der Erforderlichkeit der Veröffentlichung des Namens im Internet. Dies gilt erst recht für weitere personenbezogene Daten wie etwa die Anschrift einer Bürgerin oder eines Bürgers. In einzelnen besonderen Konstellationen kann eine Veröffentlichung des Namens im Internet zulässig sein. Zu denken ist etwa an Rechtsstreitigkeiten oder den Fall, dass die betreffende Person eine spezielle Funktion (etwa Vorsitz in einem Sportverein) innehat, die mit dem Gegenstand der Sitzung (Bau eines neuen Fußballplatzes) im Zusammenhang steht. Dies muss dann seitens der Gemeinde nachweisbar dokumentiert werden.

Die Erteilung einer den Maßgaben des Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7 DS-GVO entsprechenden Einwilligung der Bürgerin oder des Bürgers, mit der Veröffentlichung des Namens im Internet einverstanden zu sein, stellt grundsätzlich eine zulässige Rechtsgrundlage für die Verarbeitung dar. Die Freiwilligkeit der Einwilligung gegenüber öffentlichen Stellen begegnet jedoch ausweislich des Erwägungsgrunds 43 DS-GVO infolge des Über- und Unterordnungsverhältnisses zwischen Behörde und Bürger bzw. Bürgerin hohen Anforderungen. Überdies ist die Einwilligung aufgrund der jederzeitigen Widerrufbarkeit gemäß Art. 7 Abs. 3 DS-GVO und der daraus folgenden Verpflichtung zur Löschung der personenbezogenen Daten in der Praxis kaum tauglich.

Art. 6 DS-GVO

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

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

Art. 7 DS-GVO

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

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

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

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

ErwGr 43 DS-GVO

Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. (…)

Zugriffsberechtigungen auf Unterlagen des Gemeindevorstands

Eine weitere Anfrage betraf die Zugriffsberechtigungen auf Unterlagen von nicht öffentlichen Sitzungen des Gemeindevorstands in einem politischen Informationssystem. Gemäß § 67 Abs. 1 HGO sind die Sitzungen des Gemeindevorstands im Gegensatz zu denjenigen der Gemeindevertretung in der Regel nicht öffentlich.

§ 67 HGO

(1) Der Gemeindevorstand fasst seine Beschlüsse in Sitzungen, die in der Regel nicht öffentlich sind. Der Vorsitzende kann Gemeindebedienstete zu den Sitzungen beiziehen. In einfachen Angelegenheiten können die Beschlüsse im Umlaufverfahren gefasst werden, wenn niemand widerspricht. (…).

In der Anfrage wurde mitgeteilt, dass das politische Informationssystem selektive Zugriffsberechtigungen auf die Unterlagen der Sitzungen des Gemeindevorstands für die Fachbereichsleitungen sowie die Sachbearbeiterinnen und Sachbearbeiter der Gemeinde ermöglicht. Es besteht auch die Möglichkeit, Beschäftigten der Kommunalverwaltung die entsprechende Rolle (Gremium Gemeindevorstand) zuzuweisen, so dass diese dann einen Zugriff auf alle Unterlagen erhalten. Die Gemeinde wollte wissen, ob eine grundsätzliche Freischaltung aller Unterlagen der Sitzungen des Gemeindevorstands für den Leiter des Rechnungsprüfungsamtes und die Fachbereichsleitung des Fachbereichs Finanzen datenschutzrechtlich zulässig ist.

Ich habe die Gemeinde darauf hingewiesen, dass Zugriffsberechtigungen entsprechend des Grundsatzes der „Integrität und Vertraulichkeit" des Art. 5 Abs. 1 Buchst. f in Verbindung mit Art. 32 DS-GVO nach dem „Need-to-know"-Prinzip ausgestaltet werden müssen.

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; (…)

Eine voraussetzungslose Freischaltung aller Unterlagen der Sitzungen des Gemeindevorstands für den Leiter des Rechnungsprüfungsamtes und die

Fachbereichsleitung des Fachbereichs Finanzen ist damit nicht vereinbar. Vielmehr sind die Zugriffsberechtigungen grundsätzlich auf die Mitglieder des Gemeindevorstands gemäß § 65 HGO zu beschränken.

§ 65 HGO

(1) Der Gemeindevorstand besteht aus dem Bürgermeister als Vorsitzenden, dem Ersten Beigeordneten und weiteren Beigeordneten.

Die Übermittlung personenbezogener Daten an den Leiter des Rechnungsprüfungsamtes und die Fachbereichsleitung des Fachbereichs Finanzen bedarf vielmehr einer Rechtsgrundlage in dem jeweiligen Einzelfall, die nachweisbar zu dokumentieren ist. Diese kann etwa die Wahrnehmung von Aufsichts- und Kontrollbefugnissen oder die Rechnungsprüfung gemäß § 22 Abs. 1 in Verbindung mit § 21 Abs. 1 Nr. 6 HDSIG sein.

§ 22 HDSIG

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

§ 21 HDSIG

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

6. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

Fazit & Handreichung

Die dargestellten Fallkonstellationen zeigen, dass die datenschutzrechtlichen Maßgaben auch im Rahmen von politischen Informationssystemen große Praxisrelevanz aufweisen. Mit meiner Handreichung „Datenschutz bei politischen Informationssystemen“ (s. HBDI, https://datenschutz.hessen.de/sites/

datenschutz.hessen.de/files/2024-07/handreichuing_datenschutz_bei_politischen_informationssystemen_240724.pdf) unterstütze ich die Kommunen bei der Umsetzung der wesentlichen Aspekte des Datenschutzes.

5.5
Bundesweites Projekt zum Datenschutz in der Rehabilitation und Teilhabe (SGB IX)

Alle guten Dinge sind drei? Ich bin als Vertreter der Landesdatenschutzaufsichtsbehörden aus der DSK in ein weiteres Nachfolgeprojekt auf multiinstitutioneller Ebene bei der Bundesarbeitsgemeinschaft für Rehabilitation (BAR) in Frankfurt am Main aktiv eingebunden. Nach den beiden erfolgreich abgeschlossenen Projekten „Datenschutz im trägerübergreifenden Reha-Prozess“ (im Sommer 2019) und „Datenschutz in der Rehabilitation“ (im Sommer 2021) befasste sich die seit 2018 bestehende Arbeitsgruppe nunmehr in einem dritten Projekt mit einem deutschlandweit einsetzbaren „gemeinsamen Grundantrag für Reha- und Teilhabeleistungen“ und wird darüber hinaus ab 2025 ein zentrales Dokument im Reha- und Teilhabebereich, die überarbeitete GE Reha-Prozess, noch fokussieren und behandeln.

Im Frühjahr 2024 trat die BAR nach erfolgreicher Beendigung des ersten Projekts, Erstellung einer Arbeitshilfe zum Themenkomplex „Datenschutz im trägerübergreifenden Reha-Prozess“ (siehe 48. Tätigkeitsbericht, Kap. 6.4), und des daran anknüpfenden zweiten Projekts, Erstellung einer Arbeitshilfe zum Thema „Datenschutz in der Rehabilitation“ (s. 50. Tätigkeitsbericht, Kap. 13.1), wieder auf die seit 2018 ins Leben gerufene und bestehende multiinstitutionelle Arbeitsgruppe zu.

Neben dem BfDI, dem HBDI und Vertretern der BAR waren und sind Teilnehmer dieser Projektgruppe weiterhin Vertreterinnen und Vertreter u. a. von

– Bundesministerium für Arbeit und Soziales,
– Bundesministerium für Gesundheit,
– Deutsche Rentenversicherung Bund,
– Deutsche Gesetzliche Unfallversicherung (DGUV),
– Bundesagentur für Arbeit,
– GKV-Spitzenverband,
– für die Integrationsämter: Zentrum für Familie und Soziales Bayern.

Für den Sommer 2024 wurde eine Videokonferenz geplant und durchgeführt: Wie nach dem zweiten Projektabschluss im Sommer 2021 vereinbart, wollten die involvierten Institutionen die veröffentlichten beiden Arbeitshilfen

mit Blick auf deren Etablierung in der Praxis mit einigem zeitlichen Abstand nachbetrachten und beurteilen. Darüber hinaus sollten zwei Folgearbeiten der BAR hierzu, einerseits ein „Fact Sheet“, andererseits ein knappes Essay der zweiten Arbeitshilfe in Form eines „FAQ – Datenschutz in der Rehabilitation“, vor deren Veröffentlichung nochmals beleuchtet und abgestimmt werden.

Die Bilanz dieser Videokonferenz war erfreulich: Die Rückmeldungen der Leistungsträger und -erbringer zu den beiden Arbeitshilfen konnten gemäß Rückmeldungen der Institutionen als durchweg positiv und gut konstatiert werden. Und im Rahmen der mittlerweile bewährt guten und konstruktiven Zusammenarbeit konnten auch die beiden von der BAR konzipierten neuen Dokumente zur Veröffentlichung verabschiedet werden (abrufbar auf der Homepage der BAR, https://www.bar-frankfurt.de/fileadmin/dateiliste/_publikationen/reha_grundlagen/pdfs/FactsheetDatenschutzweb.pdf, andererseits unter: https://www.bar-frankfurt.de/themen/reha-prozess/datenschutz/faq-datenschutz-in-der-rehabilitation.html.

Seit Herbst 2024 steht nunmehr bis zum Jahresanfang 2025 die Befassung und datenschutzrechtliche Beurteilung eines von der BAR in einem internen Großprojekt erarbeiteten „Gemeinsamen Grundantrag für Reha- und Teilhabeleistungen“ im Fokus der beiden Aufsichtsbehörden BfDI und HBDI.

Ab Frühjahr / Sommer 2025 wird sich die Arbeitsgruppe dann mit einem der ganz zentralen Dokumente im Reha- und Teilhabebereich befassen und austauschen, der GE Reha-Prozess. Diese wird aktuell überarbeitet und neben fachlichen Erneuerungen und Anpassungen insbesondere auch an die Inhalte der beiden Arbeitshilfen der Arbeitsgruppe angepasst. Es soll hierbei z. B. auch durch passgenaue Querverweise der Praxis die Handhabbarkeit der komplexen Materie weiter erleichtert und die Rechtssicherheit in der Anwendung gestärkt werden.

Ich erlebe die Zusammenarbeit in dieser Projektgruppe weiterhin positiv und bin erneut zuversichtlich, hier wiederholt gute Arbeitsergebnisse von praktischem Nutzen für alle Betroffenen in diesem herausfordernden Arbeitsbereich mitgestalten zu können. Besonders begrüße ich noch immer die Vorgehensweise der BAR, (auch) die Datenschutzaufsichtsbehörden weiterhin direkt „ins Boot zu holen“ und so die datenschutzrechtlichen Aspekte und Implikationen unmittelbar feststellen, erörtern und konsensorientiert lösen zu können. Insofern bin ich auch zuversichtlich, für die Belange des Datenschutzes wie bei den bisherigen Projekten wieder bilanzieren zu können, dass BfDI und HBDI in erfreulichem Sinn mitgestaltend Einfluss nehmen und mithelfen konnten, ein weiteres Ergebnis miterzielt zu haben, das auch die Datenschutzperspektive angemessen und gut berücksichtigt.

6. Schulen und Hochschulen

In Schulen und in schulnahen Gremien werden viele personenbezogene Daten verarbeitet, die viele Datenschutzfragen hervorrufen. In einer Arbeitsgemeinschaft, die sich mit der datenschutzrechtlichen Verantwortlichkeit in dem Verhältnis zwischen Schulen und Schulträgern des Landes Hessen befasste, konnten viele Frage der datenschutzrechtlichen Beziehungen zwischen Schulen und Schulträgern geklärt werden und Mustervorlagen für Vereinbarungen zur gemeinsamen Verantwortung oder Auftragsverarbeitung erstellt werden (Kap. 6.1). Elternbeiräte nutzen zur Kommunikation gern Messenger-Dienste. Elternbeiräte sind gesetzlich vorgesehene Gremien, keine privaten Vereinigungen. Sie müssen daher bei der Auswahl von Messenger-Diensten auf deren Datenschutzkonformität achten und für Mitglieder auch gleichwertige alternative Kommunikationsmöglichkeiten vorsehen (Kap. 6.2).

6.1 Datenschutzrechtliches Verhältnis zwischen Schulen und Schulträgern

Wie schon in meinem Tätigkeitsbericht für das Jahr 2023 berichtet (52. Tätigkeitsbericht Kapitel 6.2), wurde auf meine Initiative hin Mitte des Jahres 2023 eine Arbeitsgruppe (AG) 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 Ministeriums für Kultus, Bildung und Chancen (HMKB), des Landkreis- und Städtetages sowie der Schulträger an. Ziel der Arbeitsgruppe ist es, den Beteiligten Mustervorlagen für Vereinbarungen nach Art. 26 und 28 DS-GVO 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.

Nach einer sehr gut besuchten Auftaktsitzung der AG im Herbst 2023 folgten im Jahr 2024 zwei weitere Sitzungen der AG mit erfreulich hohen Teilnehmerzahlen. Während in der Auftaktsitzung noch diskutiert wurde, wie die datenschutzrechtlichen Verantwortlichkeiten zwischen Schulen und Schulträgern am besten geregelt werden könnten, konnten in einer zweiten Sitzung im April 2024 den Teilnehmerinnen und Teilnehmern seitens des HMKB und mir bereits erste Ergebnisse in Form von Entwürfen von Mustervorlagen für die Regelung der datenschutzrechtlichen Verantwortlichkeiten im Verhältnis zwischen hessischen Schulen und Schulträgern als Diskussionsgrundlage für

weitere Treffen zur Verfügung gestellt werden. Dies war nicht zuletzt deshalb möglich, weil etliche Schulträger sich im Rahmen der ersten Sitzung bereit erklärt hatten, einen Fragenkatalog zu datenschutzrechtlichen Verantwortlichkeiten im Verhältnis zwischen Schulen und Schulträgern auszufüllen. Anhand der Antworten der Schulträger war es möglich, die zu erstellenden Mustervorlagen besser an die Bedürfnisse der Schulen und Schulträger in Hessen anzupassen.

Dies machte es möglich, bereits in einer dritten Sitzung der Arbeitsgruppe im Herbst 2024 Ergebnisse in Form von Mustervorlagen für die Schulen und Schulträger zu präsentieren und einen vorläufigen Abschluss der Tätigkeit der Arbeitsgruppe festzustellen. Mit diesen können nun die datenschutzrechtlichen Beziehungen zwischen Schulen und Schulträgern ausgestaltet und die Verantwortlichkeiten definiert und klargestellt werden, soweit konkrete Anwendungsfälle vor Ort identifiziert werden. So können die genannten Stellen besser ihren Pflichten aus der DS-GVO nachkommen, da beispielsweise geregelt wird, wer für die Einhaltung der Informationspflichten im Sinne der Art. 12 bis 14 DS-GVO gegenüber Schülerinnen und Schülern, Eltern und Lehrkräften verantwortlich ist. Auch die Zuständigkeit hinsichtlich der Erfüllung von Auskunftsanfragen nach Art. 15 DS-GVO wird geregelt.

Abschließend wurde vereinbart, dass die Möglichkeit besteht, dass sich die Arbeitsgruppe Mitte des Jahres 2025 erneut trifft, um Erfahrungen aus der praktischen Umsetzung zu erörtern und zu evaluieren. Aber auch in der Zwischenzeit stehe ich den Schulträgern wie auch den Verbänden bezüglich der datenschutzrechtlichen Verantwortlichkeiten bei Bedarf beratend zur Seite.

6.2
Messenger-Dienste für Elternbeiräte

Messenger-Dienste haben sich in den letzten Jahren zu einem beliebten und alltäglichen Kommunikationsmittel entwickelt. Mir wird daher immer wieder die Frage gestellt, ob diese als einfach und praktisch wahrgenommene Kommunikationsmöglichkeit auch im Rahmen der ehrenamtlichen Tätigkeit als Elternbeirat im schulischen Bereich eingesetzt werden kann.

Klassen- und Schulelternbeiräte sind in §§ 106 ff. HSchG gesetzlich vorgesehene Gremien, die im Schulleben die Interessenvertretung und die Mitwirkungsrechte der Eltern wahrnehmen. Im Rahmen ihrer Tätigkeit verarbeiten sie regelmäßig personenbezogene Daten von Schülerinnen und Schülern, Eltern und Lehrkräften, beispielsweise bei der Einladung zu einem Elternabend oder der Weitergabe von Informationen der Klassenleitung an die

Klassenelternschaft. Hierbei sind die Grundsätze der DS-GVO zu beachten, was auch die Wahl des Kommunikationsmittels einschließt.

Aus diesem Grund habe ich im Berichtszeitraum auf meiner Website einen Beitrag mit dem Titel „Die Nutzung von Messenger-Diensten durch Elternbeiräte“ veröffentlicht (https://datenschutz.hessen.de/datenschutz/hochschulen-schulen-und-archive/die-nutzung-von-messenger-diensten-durch-elternbeiraete). Dieser soll Elternbeiräte bei der Wahl eines geeigneten, datenschutzkonformen Messenger-Dienstes unterstützen und enthält insbesondere eine Aufzählung von wesentlichen Anforderungen, die bei der Auswahl des Dienstanbieters zu überprüfen sind. Der Beitrag weist darauf hin, dass aus einer Nichtnutzung des Messenger-Dienstes durch einzelne Eltern keine Nachteile entstehen dürfen. Vielmehr ist durch den Elternbeirat stets auch ein alternativer Kanal für die Kommunikation zur Verfügung zu stellen. Ferner werden dort technische Eigenschaften und Funktionalitäten dargestellt, die für einen datenschutzkonformen Einsatz zu erwarten sind.

7. Beschäftigungsverhältnisse

Im Bereich des Beschäftigtendatenschutzes erhalten wir viele Beschwerden. Beispiele hierfür betreffen Datenschutzerklärungen von Personalvermittlern (Kap. 7.1), mündliche Datenoffenbarungen (Kap. 7.2), Ermittlungen gegenüber Beschäftigten (Kap. 7.3), Totalüberwachungen der Korrespondenz von Beschäftigten (Kap. 7.4) und Personalausweis- und Führerscheinkontrollen durch Arbeitgeber (Kap. 7.5)

7.1 Transparenzanforderungen an Datenschutzerklärungen von Personalvermittlern

Anlässlich einer Beschwerde habe ich mich mit den Datenschutzerklärungen auf der Website eines Personalvermittlers in Hessen beschäftigt. Hierbei habe ich bezogen auf die Transparenzanforderungen der DS-GVO einige Mängel festgestellt. Der Beitrag beschreibt an Hand konkreter Fallbeispiele die festgestellten Defizite und zeigt auf, wie man es besser machen kann.

Personalvermittler, auch Recruiter oder Headhunter genannt, unterstützen Arbeitgeber bei der Personalsuche und im Bewerbungsverfahren, z. B. durch die Vermittlung passender Kandidatinnen und Kandidaten, der Erstellung von Stellenausschreibungen oder durch Hilfe beim Bewerberauswahlprozess. Zudem bieten sie Bewerberinnen und Bewerbern Hilfestellung bei der Arbeitsplatzsuche. Um die Dienstleistung eines Personalvermittlers in Anspruch zu nehmen, müssen Bewerberinnen und Bewerber sich in der Regel auf der Website des Personalvermittlers registrieren und in einem Bewerberportal ein Bewerberprofil anlegen. In dem Bewerberprofil werden für das Beschäftigungsverhältnis potenziell relevante Daten der Kandidatinnen und Kandidaten gespeichert (z. B. Name, Anschrift, Lebenslauf, Zeugnisse). Der Personalvermittler nutzt sodann die in dem Bewerberportal gespeicherten Daten der Kandidatinnen und Kandidaten, um die Dienstleistung der Personalvermittlung gegenüber Kunden (Arbeitgebern) erbringen zu können.

Auch in dem von mir zu prüfenden Fall musste sich der Beschwerdeführer beim betroffenen Personalvermittlungsunternehmen registrieren. Hierzu wurde dem Beschwerdeführer ein einseitiges Formular zur Unterschrift vorgelegt. Neben der Abfrage personenbezogener Daten (Name, Anschrift, E-Mail-Adresse, Geburtsdatum und Staatsangehörigkeit) erläuterte das Formular einige Datenverarbeitungsverfahren des Personalvermittlers. Für zusätzliche Informationen zum Datenschutz verwies das Formular zudem auf die Datenschutzerklärung auf der Website des Personalvermittlers.

Der Beschwerdeführer legte mir das Formular vor und äußerte datenschutzrechtliche Bedenken bezüglich der hierin beschriebenen Datenverarbeitungen. Ich nahm die Beschwerde des Betroffenen zum Anlass, sowohl das Formular als auch die auf der Website des Personalvermittlers vorhandenen Datenschutzerklärungen auf ihre Übereinstimmung mit den Transparenzanforderungen der DS-GVO, insbesondere Art. 12 Abs. 1 Satz 1, zu überprüfen.

Transparenzanforderungen der DS-GVO

Die DS-GVO enthält zwar keine Definition des Begriffes Transparenz. Art. 12 Abs. 1 Satz 1 DS-GVO konkretisiert aber den in Art. 5 Abs.1 Buchst. b DS-GVO enthaltenen Transparenzgrundsatz. Hiernach trifft der Verantwortliche geeignete Maßnahmen, um der betroffenen Person alle Informationen, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Erwägungsgrund 39 Satz 2 bis 4 der DS-GVO führt hierzu weitergehend aus:

ErwGr. 39 Satz 2 bis 4 der DS-GVO

Für natürliche Personen sollte „Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden.

Neben den Transparenzanforderungen des Art. 12 DS-GVO ergeben sich die inhaltlichen Anforderungen an Datenschutzerklärungen aus den Art. 13 und Art. 14 DS-GVO. Gemäß Art. 13 Abs. 1 und Abs. 2 DS-GVO hat der Verantwortliche die genannten Informationen zur Verfügung zu stellen, wenn er Daten bei der betroffenen Person erhebt. Gemäß Art. 13 Abs. 3 DS-GVO entstehen zudem weitere Informationspflichten, wenn der Verantwortliche die erhobenen Daten zu einem anderen Zweck als dem ursprünglichen Erhebungszweck weiterverarbeiten will. Werden personenbezogene Daten nicht bei der betroffenen Person erhoben, richtet sich die Informationspflicht nach Art. 14 DS-GVO, der partiell andere Informationskategorien vorgibt.

In meiner Prüfung habe ich mich an den Leitlinien des EDSA (WP 260 rev.01) orientiert. Ich habe festgestellt, dass die Datenschutzerklärungen des Personalvermittlers teilweise unspezifisch und insgesamt schwer verständlich waren.

Festgestellte Transparenzdefizite

Die Forderung nach einer **präzisen und transparenten Information und Kommunikation** mit den Betroffenen bedeutet, dass der Verantwortliche die Informationen auf eine einfache Formel gebracht und griffig formuliert zur Verfügung stellen soll (EDSA, WP 260 rev.01, Rn. 8). Ziel ist es, dem Betroffenen die wesentlichen den Datenschutz betreffenden Informationen bereitzustellen.

Beispiel
Im Rahmen meiner Prüfung der Datenschutzerklärung des Personalvermittlers fiel auf, dass zwischen Informationen über den Datenschutz und Informationen, die sich nicht auf den Datenschutz bezogen, nicht differenziert wurde.

Tipp
Um einer Informationsübermüdung des Lesers vorzubeugen, sollten Informationen über den Datenschutz klar von Informationen, die sich nicht auf den Datenschutz beziehen, getrennt werden.

Beispiel
Die untersuchte Datenschutzerklärung enthielt sowohl den Begriff der Verarbeitung als auch einzelne Verarbeitungsformen (z. B. Erhebung, Erfassung, Speicherung und Übermittlung), ohne dass zwischen den Begriffen differenziert wurde. Im Einleitungssatz der Datenschutzerklärung wurde z. B. beschrieben, dass die Datenschutzerklärung im Folgenden die Verwendung, Verarbeitung, Speicherung und Weitergabe personenbezogener Daten thematisiere.

Tipp
„Verarbeitung“ ist ein Oberbegriff und umfasst die in Art. 4 Nr. 2 DS-GVO definierten Verarbeitungsformen. Es sollte daher darauf geachtet werden, dass der Begriff der „Verarbeitung“ gemäß Art. 4 Nr. 2 DS-GVO konsistent gebraucht wird. Nur soweit erforderlich, sollte zwischen den einzelnen Verarbeitungsformen differenziert werden, etwa wenn spezifische Informationen zur konkreten Verarbeitungsform bereitgestellt werden (z. B. zur Speicherdauer oder Übermittlung personenbezogener Daten in Drittstaaten).

Der Begriff der „**Verständlichkeit**“ setzt voraus, dass die Informationen für den Leser nachvollziehbar sein sollen (EDSA, WP 260 rev.01, Rn. 9). Von der Nachvollziehbarkeit ist auszugehen, wenn dem Leser klar vermittelt wird, ob, wie und welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden.

Beispiel
Die Datenschutzerklärungen des Personalvermittlers enthielten Begriffe, die die DS-GVO nicht kennt. Beispielsweise wurde der Begriff der Zustimmung verwendet, obgleich die DS-GVO von einer Einwilligung spricht. Als weiteres Beispiel ist die Verwendung des Begriffs der Weitergabe personenbezogener Daten im o. g. Einleitungssatz der Datenschutzerklärung (siehe vorheriges Beispiel) zu nennen.

Tipp
Um Missverständnisse und fehlerhafte Interpretationen des Betroffenen zu vermeiden, sind die Terminologien der DS-GVO zu verwenden. Statt des Begriffs der Zustimmung ist deshalb der Begriff der Einwilligung und statt des Begriffs der Weitergabe der Begriff der Übermittlung zu verwenden.

Beispiel
In der untersuchten Datenschutzerklärung des Personalvermittlers wurde zunächst über die Quellen für die Sammlung personenbezogener Daten sowie die Kategorien der personenbezogenen Daten des Betroffenen informiert. Daraufhin folgte ein Hinweis zu Stellenangebotsbenachrichtigungen von Personalberatern und eine Beschreibung zur Abbestellung dieser Benachrichtigungen.

Tipp
Die Informationen über den Datenschutz sind thematisch (etwa durch Bildung von Überschriften) voneinander zu trennen. So kann die betroffene Person die für sie interessanten Informationen heraussuchen, ohne ausführliche Texte lesen zu müssen. Im Hinblick auf die Gesamtstruktur der Datenschutzerklärung empfiehlt es sich, eine Mehrebenen-Datenschutzerklärung zu verwenden.

Beispiel
Die untersuchte Datenschutzerklärung enthielt vereinzelt englische Fachbegriffe („Business Solutions“, „Retargeting Cookies“ oder „Double-Opt-In-Verfahren“), ohne dass die Begriffe erklärt wurden.

Tipp
Fremdsprachige Begriffe und unbekannte Verfahren sollten dem Leser übersetzt und erklärt werden. Denn der Verantwortliche kann nicht voraussetzen, dass der Leser über ausreichende Sprach- oder Fachkenntnisse verfügt. Mit der Übersetzung und Erklärung von unbekannten Begriffen wird das Verständnis über die Datenverarbeitung und damit die Transparenz gefördert. Es empfiehlt sich, die Sprache grundsätzlich an den Empfängerhorizont des Lesers anzupassen. „So kann ein Verantwortlicher, der personenbezogene Daten von Fachkräften erhebt, von einem breiteren Verständnishorizont bei seinem Zielpublikum ausgehen als ein Verantwortlicher, der die personenbezogenen Daten von Kindern erhebt“, EDSA, WP 260 rev.01, Rn. 9.

Der Begriff der „**leichten Zugänglichkeit**“ setzt voraus, dass der Betroffene die Informationen über die Datenverarbeitung nicht selbst ausfindig machen muss (EDSA, WP 260 rev.01, Rn. 11). Stattdessen soll für ihn direkt ersichtlich sein, wo und wie er eine Information abrufen kann.

Beispiel
Die Datenschutzerklärungen des Personalvermittlers verwiesen auf ergänzende Datenschutzinformationen, die weder verlinkt noch so eindeutig beschrieben waren, dass für die betroffene Person erkennbar war, welche ergänzenden Datenschutzbestimmungen für ihren Sachverhalt zur Anwendung gelangten. Um ein klares Bild der Verarbeitung ihrer Daten zu erhalten, musste die betroffene Person insoweit erhebliche, unzumutbare Aufwände betreiben.

Tipp
Um der betroffenen Person die Informationen leicht zugänglich zu machen, empfiehlt es sich, eine direkte Verlinkung (Hyperlink) bereitzustellen oder auf die genaue Stelle in der Datenschutzerklärung zu verweisen. Verantwortliche sollten zudem einen Prozess etablieren der sicherstellt, dass regelmäßig überprüft wird, dass etwaige Verlinkungen funktionstüchtig sind und die Datenschutzerklärung dauerhaft abrufbar ist.

Die Forderung nach einer **klaren und einfachen Sprache** bedeutet, dass Datenschutzerklärungen konkrete und belastbare Aussagen enthalten sollen (EDSA, WP 260 rev.01, Rn. 12). Im Besonderen sind die Zwecke und Rechtsgrundlagen der Verarbeitungen nach Art. 5 Abs. 1 Buchst. a und b DS-GVO eindeutig darzulegen. Auch sind die Informationen in einer einfachen Art und

Weise zur Verfügung zu stellen. Auf komplexe Satzstrukturen sollte daher weitestgehend verzichtet werden.

Beispiel
Die untersuchte Datenschutzerklärung des Personalvermittlers enthielt Modalwörter wie „möglicherweise“ und „in der Regel“. Die häufige Verwendung von Modalverben und -wörtern verringern die Belastbarkeit der enthaltenen Aussagen und sind dazu geeignet, den Betroffenen mit Blick auf die Verarbeitung seiner personenbezogenen Daten im Unklaren zu lassen.

Tipp
Modalverben und -wörter sollten vermieden und möglichst belastbare Aussagen getroffen werden (s. EDSA, WP 260 rev.01, Rn. 12 f.).

Beispiel
In der untersuchten Datenschutzerklärung war für Betroffene nicht erkennbar, welche Verarbeitungssituation welchem Zweck dient und welche Rechtsgrundlage einschlägig ist.

Tipp
Es sollte klar strukturiert und in einfachen Worten herausgearbeitet werden, welche Verarbeitungssituation welchem Zweck dient und welche Rechtsgrundlage hierfür zur Anwendung gelangt. Nur auf diese Weise kann die betroffene Person feststellen, ob die Verarbeitung seiner personenbezogenen Daten rechtmäßig ist.

Beispiel
Die untersuchte Datenschutzerklärung des Personalvermittlers enthielt Überschriften, die eine unterschiedliche Interpretation der hierunter beschriebenen Verarbeitungssituation zuließ. Unter der Überschrift „Besucher“ konnte zum Beispiel eine Datenverarbeitung durch den Besuch der Website des Personalvermittlers als auch der Vor-Ort-Besuch in dessen Büroräumlichkeiten verstanden werden.

Tipp
Um Irritationen des Lesers vorzubeugen, sollten Überschriften möglichst „sprechend“ sein, d. h. die unter dem Oberbegriff beschriebene Datenverarbeitung eindeutig und präzise beschreiben.

Meiner Prüfung lag zwar die Datenschutzerklärung eines Personalvermittlers zugrunde. Die zuvor genannten Beispiele und Tipps lassen sich aber auch auf andere Datenschutzerklärungen übertragen.

Neben diesen konkreten Fallbeispielen empfiehlt es sich, einen Prozess zu etablieren, bei dem die Datenschutzerklärung vor der Veröffentlichung oder sonstigen Verwendung von fachfremden Personen gesichtet und auf ihre Verständlichkeit hin überprüft wird. Zudem sollte die Datenschutzerklärung regelmäßig auf etwaig notwendig gewordene Änderungen und auf technische Erreichbarkeit (z. B Erreichbarkeit von Verlinkungen, Abrufbarkeit der Datenschutzerklärung) geprüft werden.

Mit Blick auf die geprüften Datenschutzhinweise des Personalvermittlers habe ich aufgrund der beschriebenen Defizite Verstöße gegen Art. 5 Abs. 1 Buchst. a i. V. m. Art. 12 Abs. 1 Satz 1 DS-GVO festgestellt. Das Personalvermittlungsunternehmen war bezüglich der von mir geäußerten Mängel von Beginn an einsichtig und kooperativ. Zwischenzeitlich wurde die Datenschutzerklärung vollständig und zu meiner Zufriedenheit überarbeitet. Obgleich das betroffene Unternehmen von Beginn an daran mitwirkte, DS-GVO-konforme Zustände herzustellen, habe ich aufgrund der Schwere des Verstoßes das Verfahren zur Prüfung der Einleitung eines Bußgeldverfahrens an das Justiziariat meiner Behörde abgegeben. Dieses Verfahren dauert derzeit noch an.

Aufgrund der Bedeutsamkeit des Transparenzgrundsatzes werde ich mich auch in Zukunft mit der Ausgestaltung von Datenschutzerklärungen beschäftigen und auf eine DS-GVO-konforme Ausgestaltung hinwirken.

7.2
Mündliche Datenverarbeitungen im Beschäftigungsverhältnis

Die Regelung des § 26 Abs. 7 BDSG, die mündliche Datenverarbeitungen im Beschäftigungsverhältnis wie etwa Befragungen von Beschäftigten oder Spindkontrollen erfasst, ist auch nach der Grundsatzentscheidung des EuGH (Urteil vom 30. März 2023, C-34/21) zu dem mit § 26 BDSG weitgehend inhaltsgleichen § 23 HDSIG weiterhin anwendbar.

Ein Beschäftigter, demgegenüber eine Verdachtskündigung ausgesprochen worden war, bat mich im Rahmen einer Beschwerde um eine datenschutzrechtliche Prüfung und Bewertung des folgenden Sachverhalts: Im Zusammenhang mit der Verdachtskündigung war ein Kollege von ihm durch die Geschäftsführung des Arbeitgebers befragt worden. Im Verlauf der Befragung waren Details zum vermeintlichen Fehlverhalten des Beschwerdeführers offengelegt worden. Hierzu hat der Befragte ein Gedächtnisprotokoll der

mündlichen Befragung gefertigt, das durch den Beschwerdeführer in das Beschwerdeverfahren eingebracht wurde. Es enthält Ausführungen darüber, dass die Geschäftsführung den Befragten über eine Abmahnung des Beschwerdeführers wegen Mobbings informierte. Ferner sei Gegenstand der Unterredung die Initiative des Beschwerdeführers zur Gründung eines Betriebsrats gewesen. Diese habe nach Einschätzung der Geschäftsführung lediglich dazu gedient, einen besonderen Kündigungsschutz in Anspruch nehmen zu können.

Aufgrund der Beschwerde habe ich den Arbeitgeber angehört. Hierbei habe ich erklärt, dass ich die Bedenken des Beschwerdeführers an der Rechtmäßigkeit der Befragung teile und insbesondere keine Rechtsgrundlage für die mündliche Verarbeitung der Daten des Beschwerdeführers erkennen kann.

Der Arbeitgeber verneinte einen Datenschutzverstoß. Er führte aus, dass mündliche Datenverarbeitungen grundsätzlich vom Anwendungsbereich der DS-GVO nicht erfasst seien und § 26 Abs. 7 BDSG auch nicht zur Erweiterung des Anwendungsbereiches der DS-GVO herangezogen werden könne. § 26 Abs. 7 BDSG erfülle nicht die vom EuGH aufgestellten Anforderungen an die Öffnungsklausel des Art. 88 DS-GVO (EuGH, Urteil vom 30. März 2023, C-34/21), nach denen nationale Vorschriften auf den Schutz der Rechte und Freiheiten der Beschäftigten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten im Beschäftigungskontext abzielen und geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person umfassen müssten.

§ 26 BDSG

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

(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Art. 88 DS-GVO

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

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

Diese Auffassung ist jedoch nicht zutreffend. Die Regelung des § 26 Abs. 7 BDSG beruht nicht auf der Öffnungsklausel des Art. 88 DS-GVO. Vielmehr ist die DS-GVO bei Verarbeitung personenbezogener Daten, ohne dass die Daten in einem Dateisystem gespeichert sind oder gespeichert werden sollen, gar nicht einschlägig. Daher kann der nationale Gesetzgeber eine derartige mündliche Datenverarbeitung im Beschäftigungsverhältnis selbst regeln.

Die DS-GVO gilt gemäß Art. 2 Abs. 1 für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Das deutsche Beschäftigtendatenschutzrecht geht mit der Regelung des § 26 Abs. 7 BDSG darüber hinaus. Danach sind die Absätze 1 bis 6 auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen (etwa bei Befragungen von Beschäftigten oder Bewerbern sowie Spindkontrollen). Mit dem den Anwendungsbereich der DS-GVO überschießenden Bereich wird § 26 Abs. 7 BDSG als nationale Sondervorschrift nicht von der DS-GVO verdrängt und hat daher auch nach der Grundsatzentscheidung des EuGH Bestand (s. Simitis/Hornung/Spiecker/Seifert, Datenschutzrecht DS-GVO/BDSG, 2. Aufl. 2025, § 26 BDSG Rn. 28; Kühling/Buchner/Maschmann, DS-GVO BDSG, 4. Aufl. 2024, § 26 BDSG Rn. 4; s. zu den Auswirkungen des EuGH-Urteils Roßnagel/Wetzstein/Horlbeck, DuD 2023, 429 ff.; s. auch BAG, Urteil vom 20. Juni 2013 – 2 AZR 546/12, zur Spindkontrolle; sowie BT-Drs. 18/11325, 99).

Durch die Befragung des Kollegen wurde rechtswidrig in das Persönlichkeitsrecht des Beschwerdeführers eingegriffen. Mangels entsprechender Rechtsgrundlage habe ich einen Verstoß gegen Art. 5 Abs. 1 Buchst. a, Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO in Verbindung mit § 26 Abs. 1 Satz 1 und Abs. 7 BDSG festgestellt.

7.3
Keine Ermittlungen ins Blaue hinein

Zwar haben betroffene Personen grundsätzlich das Recht auf Beschwerde bei der zuständigen Aufsichtsbehörde nach Art. 77 Abs. 1 DS-GVO, wenn sie der Ansicht sind, in ihren Datenschutzrechten verletzt worden zu sein. Allerdings müssen Beschwerden einen gewissen Aussagegehalt haben. Weitere Sachverhaltsermittlungen führe ich nur durch, wenn zumindest Tatsachen vorgetragen werden, die einen Datenschutzverstoß nahelegen.

Im Berichtszeitraum gingen bei meiner Behörde verschiedene Beschwerden zum Beschäftigtendatenschutz ein, bei denen der Sachvortrag keinen beweisbaren Datenschutzverstoß erkennen ließ. So machte ein Bürger geltend, er würde im Homeoffice durch seinen Arbeitgeber überwacht. Als Indiz für die Überwachung führte er an, vor seinem Wohnhaus würden verschiedene Lieferwagen parken; auf dem Feldweg hinter dem Haus hingegen habe er Hundespaziergänger gesehen, die ihm unbekannt seien. Vom Feldweg aus könne man sehen, ob er am heimischen Arbeitsplatz arbeite oder anderen Tätigkeiten im Haus nachgehe. Ein anderer Beschwerdeführer gab an, von seiner Vorgesetzten beim Telefonieren abgehört worden zu sein. Er habe aber keine Beweise dafür, sondern lediglich eine Ahnung, dass es so gewesen sei. Auf meine Nachfragen konnten die Beschwerdeführer keine stichhaltigen Anhaltspunkte für die gerügten Datenschutzverstöße liefern.

Grundsätzlich ist eine Leistungskontrolle von Beschäftigten durch Erscheinen an ihrer Privatwohnung als Datenverarbeitung im Beschäftigungskontext anzusehen und kann daher von meiner Behörde auf ihre Rechtmäßigkeit hin überprüft werden. Dies ergibt sich aus § 26 Abs. 7 BDSG.

§ 26 Abs. 7 BDSG

(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Das Abhören von Telefongesprächen stellt hingegen einen Straftatbestand dar, nämlich die Verletzung der Vertraulichkeit des Wortes nach § 201 Abs. 2 Nr. 1 StGB.

§ 201 Abs. 2 Nr. 1 StGB

(2) Ebenso wird bestraft, wer unbefugt

1. *das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört (…).*

Für einen Sachverhalt, der eine Strafbarkeit des Verantwortlichen begründen könnte, wäre die Beschwerde von meiner Behörde an die Staatsanwaltschaft abzugeben.

Betroffene Personen haben nach Art. 77 Abs. 1 DS-GVO das Recht auf Beschwerde bei einer Aufsichtsbehörde, wenn sie der Meinung sind, dass die Verarbeitung ihrer personenbezogenen Daten gegen die Bestimmungen der DS-GVO verstößt.

Art. 77 Abs. 1 DS-GVO

(1) Jede betroffene Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen Rechtsbehelfs das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

Es sind dabei nur geringe Anforderungen an die Darlegung des vermeintlichen Rechtsverstoßes zu stellen (Bergt, in: Kühling/Buchner, 4. Aufl. 2024, DS-GVO Art. 77 Rn. 10). Eine Beschwerde muss aber zumindest alle Informationen enthalten, die erforderlich sind, damit die Aufsichtsbehörde den Sachverhalt erfassen und gegebenenfalls weiter aufklären und etwaige Datenschutzverstöße prüfen kann. Beschwerdeführer können von mir keine Ermittlungen ins Blaue hinein verlangen. Dabei kann zwar von der betroffenen Person keine rechtliche Analyse erwartet werden; allerdings muss die Behauptung eines Rechtsverstoßes substantiiert durch Tatsachen belegt werden (zum Vorstehenden VG Mainz, Urteil vom 22. Juli 2020, Az. 1 K 473/19.MZ, R. 26). Dies war vorliegend nicht der Fall, da es nicht möglich ist, aufgrund der Sichtung von Hundespaziergängern hinter dem Haus oder einer Ahnung der betroffenen Person weitere Ermittlungen zu möglichen Datenschutzverstößen anzustellen. In beiden Fällen habe ich mich daher dazu entschlossen,

nicht weiter zu ermitteln. Zwar habe ich den Untersuchungsgrundsatz nach § 24 HVwVfG einzuhalten; jedoch machten die Beschwerdeführer in den erwähnten Fällen keine Angaben, die eine weitere Sachverhaltsermittlung möglich gemacht hätten.

§ 24 HVwVfG

(1) Die Behörde ermittelt den Sachverhalt von Amts wegen. Sie bestimmt Art und Umfang der Ermittlungen; an das Vorbringen und an die Beweisanträge der Beteiligten ist sie nicht gebunden. Setzt die Behörde automatische Einrichtungen zum Erlass von Verwaltungsakten ein, muss sie für den Einzelfall bedeutsame tatsächliche Angaben des Beteiligten berücksichtigen, die im automatischen Verfahren nicht ermittelt würden.

(2) Die Behörde hat alle für den Einzelfall bedeutsamen, auch die für die Beteiligten günstigen Umstände zu berücksichtigen.

(3) Die Behörde darf die Entgegennahme von Erklärungen oder Anträgen, die in ihren Zuständigkeitsbereich fallen, nicht deshalb verweigern, weil sie die Erklärung oder den Antrag in der Sache für unzulässig oder unbegründet hält.

Im Interesse der Funktionsfähigkeit meiner Behörde und unter Berücksichtigung des Grundsatzes des § 10 HVwVfG, wonach das Verwaltungsverfahren einfach, zweckmäßig und zügig durchzuführen ist, habe ich daher darauf verzichtet, die zuvor dargestellten Beschwerden weiter zu verfolgen.

§ 10 HVwVfG-

Das Verwaltungsverfahren ist an bestimmte Formen nicht gebunden, soweit keine besonderen Rechtsvorschriften für die Form des Verfahrens bestehen. Es ist einfach, zweckmäßig und zügig durchzuführen.

Selbst wenn Datenschutzverstöße festgestellt werden sollten, besteht im Übrigen für Beschwerdeführer kein Anspruch auf Ergreifen einer bestimmten aufsichtsbehördlichen Maßnahme (EuGH, Urteil vom 11. April 2024, Rs. 786/21). Zu diesem Urteil siehe näher Kap. 1.3.

7.4
Keine anlass- und lückenlose Totalüberwachung der Korrespondenz von Beschäftigten

Auch bei nicht gestatteter Privatnutzung von E-Mail-Diensten am Arbeitsplatz darf die Korrespondenz von Beschäftigten nicht lückenlos überwacht werden. Eine solche Maßnahme verstößt gegen den Grundsatz der Rechtmäßigkeit der Datenverarbeitung aus Art. 5 Abs. 1 Buchst. a DS-GVO.

Die Beschäftigte einer Behörde, die Aufgaben im sozialen Bereich wahrnimmt, wandte sich mit einer Beschwerde über eine Dienstanweisung, zum Vorlegen sämtlichen Schriftverkehrs gegenüber ihrem Vorgesetzten, an mich. Zuvor habe sie versucht, in Gesprächen auf fehlende Strukturen und mangelnde Unterstützung bei nicht zu bewältigender Arbeitslast innerhalb der Behörde hinzuweisen. Die Gespräche seien jedoch erfolglos geblieben, weshalb sie zwei Überlastungsanzeigen gestellt habe. In einem Gespräch mit ihrem Vorgesetzten seien ihr sodann Vorwürfe gemacht worden, z. B. dass ihre Akten viel zu dick seien. Außerdem sei die Behörde von dritter Stelle darauf hingewiesen worden, dass die Beschwerdeführerin E-Mails verschicken würde, die nicht im Sinne der Behörde seien. Die Beschwerdeführerin sei dann schriftlich angewiesen worden, dass zukünftig sämtlicher Schriftverkehr ihrem Vorgesetzten vor dem Postausgang vorzulegen wäre. Hiervon sei der E-Mail-Verkehr ausgenommen, an dem der Vorgesetzte stets unter cc zu beteiligen sei. Auf meine Rückfrage erklärte die Beschwerdeführerin, dass die Privatnutzung von E-Mail- und anderen Internet-Programmen nicht erlaubt sei.

Ich habe daraufhin die öffentliche Stelle zum Sachverhalt angehört. Diese trug vor, die Amtsleitung habe bezüglich dieser Dienstanweisung von ihrem Direktionsrecht nach § 106 Gewerbeordnung (GewO) Gebrauch gemacht. Im Vorfeld habe es interne und externe Hinweise gegeben, die diese engere Führung notwendig gemacht hätten. Es habe Anlass zur Sorge gegeben, dass die Außendarstellung der Behörde und der Beschwerdeführerin durch ihre Schreiben und E-Mails beschädigt würde. Auch seien die Schreiben der Beschwerdeführerin, die der Amtsleitung bzw. Abteilungsleitung vorgelegt wurden, in Rechtschreibung und Grammatik fehlerhaft gewesen. Man habe bei der Beschwerdeführerin eine negative Stimmung erahnen können, sie sei nicht in den Austausch mit ihren Vorgesetzten gegangen und nicht reflektiert mit der Außenwirkung ihrer Arbeitsweise umgegangen. Die Maßnahme habe daher als eine vorübergehende Hilfestellung dienen sollen. Es habe keine inhaltliche oder fachliche Prüfung des Schriftverkehrs gegeben. Es handele sich keinesfalls um eine lückenlose Überwachung der Beschwerdeführerin. Vielmehr habe der Schutzgedanke im Vordergrund gestanden.

Die Behörde führte außerdem aus, dass die Datenverarbeitung ihrer Ansicht nach gem. Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DS-GVO gerechtfertigt sei, da es sich nicht um eine Datenverarbeitung zur Durchführung des Beschäftigungsverhältnisses handele. Grammatik und Rechtschreibung seien zulässige Qualitätskriterien, da nach § 19 Abs. 1 Satz 1 SGB X Deutsch als Amtssprache zu verwenden ist. Die Maßnahme sei nach Einarbeitung einer neuen Sachgebietsleiterin als Vorgesetzte der Beschwerdeführerin beendet worden.

Nach eingehender Prüfung der Sach- und Rechtslage habe ich festgestellt, dass die Datenverarbeitung ohne Rechtsgrundlage erfolgte und damit nicht datenschutzkonform war.

Bei der Einsichtnahme in sämtliche Korrespondenz der Beschwerdeführerin in dem angegebenen Zeitraum handelte es sich um eine Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DS-GVO, für die keine Erlaubnistatbestände ersichtlich sind. Dabei stellt auch eine Einsichtnahme in briefliche Korrespondenz im Beschäftigungsverhältnis gemäß § 23 Abs. 7 Satz 1 HDSIG eine Datenverarbeitung dar, selbst wenn diese nicht in einem Dateisystem gespeichert werden sollte.

§ 23 Abs. 7 Satz 1 HDSIG

(7) Die Absätze 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. (…)

Die Behörde konnte sich nicht auf das Weisungs- und Direktionsrecht des Arbeitgebers bzw. Dienstherrn nach § 106 Gewerbeordnung (GewO) berufen.

§ 106 GewO

Der Arbeitgeber kann Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrages oder gesetzliche Vorschriften festgelegt sind. Dies gilt auch hinsichtlich der Ordnung und des Verhaltens der Arbeitnehmer im Betrieb. Bei der Ausübung des Ermessens hat der Arbeitgeber auch auf Behinderungen des Arbeitnehmers Rücksicht zu nehmen.

Zwar ist zutreffend, dass Arbeitgeber gegenüber ihren Beschäftigten ein Weisungsrecht i. S. d. § 106 GewO haben. Für die Rechtmäßigkeit einer auf diesem Weisungsrecht beruhenden Datenverarbeitung hätte diese dennoch erforderlich i. S. d. Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO sein müssen.

Art. 6 DSGVO

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

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

Für die Erforderlichkeit der Datenverarbeitung im Beschäftigungsverhältnis ist zu beachten: Der Arbeitgeber darf mit der Datenverarbeitung jeden Zweck verfolgen, der von der Rechtsordnung gebilligt ist. Die Datenverarbeitung muss jedoch das mildeste Mittel zur Erreichung des verfolgten Zwecks darstellen. Dies ist der Fall, wenn die Abwägung ergibt, dass der Eingriff in das Persönlichkeitsrecht des Beschäftigten und sein Recht auf informationelle Selbstbestimmung nicht außer Verhältnis zu den Interessen des Arbeitgebers steht, die mit der Datenverarbeitung verfolgt werden (s. z. B. Schantz in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 2. Auflage 2025, Rn. 34).

Eine Abwägung der widerstreitenden Interessen von Arbeitgeber und Beschäftigter durch die Behörde hat nicht stattgefunden. Eine Erforderlichkeit der Überwachung sämtlicher Korrespondenz der Beschwerdeführerin zur Wahrung der positiven Außendarstellung der Behörde nach Überlastungsanzeigen von Beschäftigten ist nicht erforderlich. Zwar kann es zu den Interessen eines Arbeitgebers gehören, Qualitätskontrollen der Arbeit durchzuführen. Jedoch können diese nicht dazu führen, dass sämtlicher ausgehender Schriftverkehr der Beschäftigten inhaltskontrolliert und überwacht wird. Dies stellt einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Zudem ist zweifelhaft, ob eine solche Überwachungsmaßnahme überhaupt geeignet ist, die Fehlerquote zu senken, da alleine durch die Vorlage der Schreiben bzw. das In-cc-Setzen des Vorgesetzten bei E-Mails keine Verbesserung eintreten wird.

Die Tatsache, dass die Beschwerdeführerin zwei Überlastungsanzeigen gestellt hatte, rechtfertigt keine lückenlose Totalüberwachung sämtlicher Korrespondenz der Beschwerdeführerin. Eine solche ist datenschutzrechtlich in der Regel unzulässig. Ist die Privatnutzung der E-Mail-Systeme untersagt, darf der Arbeitgeber zwar überprüfen, ob die Nutzung tatsächlich zu dienstlichen Zwecken erfolgt. Es sind dann aber allenfalls Stichproben denkbar, jedoch keine Vollkontrolle des Schriftverkehrs.

Eine systematische, lückenlose Kontrolle ist aber auch bei untersagter Privatnutzung allenfalls bei konkretem, schwerwiegendem Missbrauchsverdacht zulässig (Stück, Arbeitnehmer können E-Mails der Arbeitnehmer bei Verbot der Privatnutzung überwachen, CCZ 2016, 285, 286; Anmerkung zu; EGMR, Urteil vom 12. Januar2016, 61496/08, *Barbulescu/Rumänien*). Ein solcher schwerwiegender Missbrauchsverdacht war aber in diesem Fall nicht ersichtlich.

Ein Rechtfertigungstatbestand für die Datenverarbeitung ergibt sich auch nicht aus Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DS-GVO. Die rechtliche Verpflichtung zur Datenverarbeitung nach Art. 6 Abs. 1 UAbs. 1 Buchst. c

DS-GVO muss sich gemäß Art. 6 Abs. 2 und Abs. 3 DS-GVO aus dem Unionsrecht oder dem Recht eines Mitgliedsstaats ergeben, vgl. Keinesfalls kann der Verantwortliche über diese Pflicht bestimmen (Roßnagel in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Auflage 2025, Art. 6 Abs. 1 Rn. 51). Unionsrechtliche oder mitgliedsstaatliche Regelungen zur Datenverarbeitung sind hier nicht erkennbar. Die Verpflichtung aus § 19 Abs. 1 Satz 1 SGB X, Deutsch als Amtssprache zu verwenden, auf die die verantwortliche Stelle sich berief, kann jedenfalls keine Überwachungsmaßnahmen von Beschäftigten, die in der Vergangenheit Rechtschreib- und Flüchtigkeitsfehler gemacht hatten, begründen.

In der Regel ist auch Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO als Rechtsgrundlage für eine solche Datenverarbeitung denkbar. Dann wäre eine Abwägung zwischen den berechtigten Interessen des Verantwortlichen und den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Person durchzuführen. Der Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO ist jedoch nach Art. 6 Abs. 1 UAbs. 2 DS-GVO nicht anwendbar, wenn Behörden in Erfüllung ihrer Aufgaben handeln.

Art. 6 Abs. 1 DS-GVO

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

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

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

Da keine Rechtsgrundlage für die Datenverarbeitung erkennbar war und diese nicht erforderlich und verhältnismäßig war, habe ich einen Verstoß gegen den Grundsatz der Rechtmäßigkeit der Datenverarbeitung gemäß Art. 5 Abs. 1 Buchst. a DS-GVO festgestellt und die Behörde gemäß Art. 58 Abs. 2 Buchst. b DS-GVO und § 14 Abs. 1 Satz 1 HDSIG verwarnt.

7.5
Personalausweis und Führerscheinkontrollen durch Arbeitgeber

Arbeitgeber dürfen die personenbezogenen Daten ihrer Beschäftigten aus Personalausweisen und Fahrerlaubnispapieren nur in engen Grenzen verarbeiten. Das Anfertigen von Kopien oder Scans sowie deren Speicherung sind grundsätzlich unzulässig.

Immer wieder erreichen mich Beschwerden von Beschäftigten, deren Arbeitgeber ihre personenbezogenen Daten verarbeiten, indem sie Personalausweise und Führerscheine kontrollieren und Kopien davon anfertigen. Auch im Berichtszeitraum gingen einige Beschwerden dazu bei meiner Behörde ein. Im Folgenden werde ich kurz darstellen, unter welchen Voraussetzungen solche Verarbeitungsvorgänge zulässig sind.

Personalausweiskontrollen zum Zweck der Identifizierung der Beschäftigten – besonders bei Begründung des Beschäftigungsverhältnisses – durch Arbeitgeber sind erlaubt. Außerdem können Arbeitgeber berechtigt und in Einzelfällen sogar verpflichtet sein, die Fahrerlaubnis ihrer Beschäftigten zu kontrollieren. Anders verhält es sich hingegen mit dem Anfertigen von Kopien von Ausweis- und Fahrerlaubnispapieren.

Personalausweiskontrollen

Die Vorschriften des Personalausweisgesetzes (PAuswG) sind bereichsspezifische Datenschutzvorschriften, die denen des BDSG vorgehen (VG Hannover, Urteil vom 28.11.2013, Az. 10 A 5342/11). Nach § 14 PAuswG ist die Erhebung und Verwendung von Daten aus dem Personalausweis nur unter engen Voraussetzungen zulässig.

§ 14 PAuswG-

Die Erhebung und Verwendung personenbezogener Daten aus dem Ausweis oder mithilfe des Ausweises darf ausschließlich erfolgen durch

1. *zur Identitätsfeststellung berechtigte Behörden nach Maßgabe der §§ 15 bis 17,*
2. *öffentliche Stellen und nichtöffentliche Stellen nach Maßgabe der §§ 18 bis 20.*

Die Vorlage von Personalausweisen zur Identitätsfeststellung richtet sich dabei nach § 20 Abs. 1 PAuswG.

§ 20 Abs. 1 PAuswG

(1) Der Inhaber kann den Ausweis bei öffentlichen und nichtöffentlichen Stellen als Identitätsnachweis und Legitimationspapier verwenden.

Der Zweck der Verarbeitung liegt nur in der Identitätsfeststellung durch den Arbeitgeber. Wenn diese Identitätsfeststellung durch Kontrolle des Ausweises in Anwesenheit der beschäftigten Person erfolgt ist, ist eine weitere Verarbeitung durch das Anfertigen und Speichern von Ablichtungen nicht mehr notwendig.

Personalausweiskopien

Unter Ablichtungen versteht man das Fotografieren, Kopieren oder Einscannen von Personalausweisen (Begründung des Gesetzes zur Förderung des elektronischen Identitätsnachweises vom 22. Februar 20217, BT-Drucks. 18/11279, S. 27, https://dserver.bundestag.de/btd/18/112/1811279.pdf). Ablichtungen von Personalausweisen sind nach § 20 Abs. 2 PAuswG nur mit Zustimmung der Ausweisinhaberin bzw. des Ausweisinhabers möglich.

§ 20 Abs. 2 PAuswG

(2) Der Ausweis darf nur vom Ausweisinhaber oder von anderen Personen mit Zustimmung des Ausweisinhabers in der Weise abgelichtet werden, dass die Ablichtung eindeutig und dauerhaft als Kopie erkennbar ist. Andere Personen als der Ausweisinhaber dürfen die Kopie nicht an Dritte weitergeben. Werden durch Ablichtung personenbezogene Daten aus dem Personalausweis erhoben oder verarbeitet, so darf die datenerhebende oder -verarbeitende Stelle dies nur mit Einwilligung des Ausweisinhabers tun. Die Vorschriften des allgemeinen Datenschutzrechts über die Erhebung und Verwendung personenbezogener Daten bleiben unberührt.

Das Tatbestandsmerkmal der Zustimmung ist nicht notwendigerweise gleichzusetzen mit dem der Einwilligung, sondern ist ein Oberbegriff. Bei der Einwilligung im Sinne der DS-GVO handelt es sich um eine vorherige Zustimmung. Zu beachten ist, dass das Ablichten von Personalausweisen durch Arbeitgeber auch an den datenschutzrechtlichen Bestimmungen der DS-GVO zu messen ist, da die DS-GVO als unmittelbar geltende EU-Verordnung, die dem nationalen Recht vorgeht, auf Personalausweise anwendbar ist. Danach sind Ablichtungen von Personalausweisen durch Arbeitgeber nicht oder nur mit Einwilligung der Ausweisinhaberinnen und Ausweisinhaber erlaubt. Solche Ablichtungen und deren weitere Verarbeitung ohne Einwilligung verstoßen gegen den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchst. c

DS-GVO sowie gegen den Grundsatz der Speicherbegrenzung aus Art. 5 Abs. 1 Buchst. e DS-GVO.

Art. 5 Abs. 1 DS-GVO

(1) Personenbezogene Daten müssen

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“); (…)

Für die Beurteilung der Frage, ob eine wirksame Einwilligung vorliegt, sind die Voraussetzungen des Art. 7 Abs. 3 und Abs. 4 DS-GVO zu berücksichtigen.

Art. 7 DS-GVO

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

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

Da Einwilligungen jederzeit mit Wirkung für die Zukunft widerrufen werden können (Art. 7 Abs. 3 Satz 1 DS-GVO) und an wirksame Einwilligungen im Beschäftigungsverhältnis wegen des Über- und Unterordnungsverhältnisses hohe Anforderungen zu stellen sind, rate ich von der Anfertigung von Personalausweiskopien, auch mit Einwilligung der Personalausweisinhaberin oder des Personalausweisinhabers, ab.

Führerscheinkontrollen

Die Kontrolle einer Fahrerlaubnis durch Arbeitgeber ist nicht nur zulässig, sondern im Einzelfall sogar verpflichtend. Dies ist z. B. dann der Fall, wenn Beschäftigte auf ein Dienstfahrzeug oder einen Firmenwagen zugreifen dürfen. Lässt die Halterin oder der Halter eines Kraftfahrzeugs zu, dass eine Person ohne gültige Fahrerlaubnis ihr bzw. sein Fahrzeug führt, macht sie bzw. er sich selbst wegen des Fahrens ohne Fahrerlaubnis nach § 21 Abs. 1 Nr. 2 des Straßenverkehrsgesetzes (StVG) strafbar.

§ 21 Abs. 1 StVG

(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer

1. *ein Kraftfahrzeug führt, obwohl er die dazu erforderliche Fahrerlaubnis nicht hat oder ihm das Führen des Fahrzeugs nach § 44 des Strafgesetzbuchs oder nach § 25 dieses Gesetzes verboten ist, oder*
2. *als Halter eines Kraftfahrzeugs anordnet oder zulässt, dass jemand das Fahrzeug führt, der die dazu erforderliche Fahrerlaubnis nicht hat oder dem das Führen des Fahrzeugs nach § 44 des Strafgesetzbuchs oder nach § 25 dieses Gesetzes verboten ist.*

Die Führerscheinkontrolle ist nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO rechtmäßig, da sie zur Erfüllung einer rechtlichen Verpflichtung erfolgt, der der Verantwortliche unterliegt. Da es vorkommen kann, dass gegenüber Beschäftigten ein Fahrverbot verhängt und die Fahrerlaubnis eingezogen wird, empfiehlt es sich für Arbeitgeber, in regelmäßigen Abständen die Fahrerlaubnis ihrer Beschäftigten zu kontrollieren. Hierbei hat sich eine halbjährliche Kontrolle als praktikabel erwiesen.

Art. 6 DS-GVO

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

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

Die Verarbeitung von personenbezogenen Daten aus der Fahrerlaubnis ist nach Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO zulässig, wenn das Führen des Fahrzeugs zur arbeitsvertraglich geschuldeten Tätigkeit oder generell zur Durchführung des Beschäftigungsverhältnisses gehört.

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, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; (…)

Führerscheinkopien

Nicht zulässig ist hingegen das Anfertigen von Führerscheinkopien durch den Arbeitgeber. Dies ergibt sich aus den Grundsätzen der Datenminimierung und der Speicherbegrenzung gemäß Art. 5 Abs. 1 Buchst. c und e DS-GVO (siehe oben). Der Arbeitgeber sollte allerdings bei der halbjährlichen Führerscheinkontrolle diejenigen personenbezogenen Daten der oder des Beschäftigten protokollieren, die zur Erfüllung des Nachweises der Fahrerlaubniskontrolle notwendig sind. Dies sind der vollständige Name, die Führerscheinklasse, das Ausstellungsdatum des Führerscheins und eine Bestätigung der Kontrolle durch die betroffenen Personen. Eine darüber hinausgehende Verarbeitung personenbezogener Daten durch den Arbeitgeber ist nicht zur Erfüllung der Verpflichtung aus § 21 Abs. 1 Nr. 2 StVG notwendig und damit nicht datenschutzkonform. Die Kopie der Fahrerlaubnispapiere wäre allenfalls auf Grundlage einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO zulässig. Da an eine Einwilligung im Beschäftigungsverhältnis, wie bereits dargestellt, hohe Anforderungen gestellt sind, halte ich eine einwilligungsbasierte Anfertigung einer Fotokopie für nicht empfehlenswert.

Elektronisches Fuhrparkmanagement

Inzwischen greifen immer mehr Arbeitgeber auf ein elektronisches Fuhrparkmanagement zurück, durch das auch die Fahrerlaubniskontrolle automatisiert durchgeführt wird. Arbeitgeber als Verantwortliche haben hierbei die datenschutzrechtlichen Anforderungen zu beachten, insbesondere den Grundsatz der Integrität und Vertraulichkeit aus Art. 5 Abs. 1 Buchst. f DS-GVO.

Art. 5 Abs. 1 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“); (…)

Hier sind besonders Art. 25 DS-GVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen) und Art. 32 DS-GVO (Sicherheit der Verarbeitung) vom Arbeitgeber zu berücksichtigen. Bedient er sich eines Auftragsverarbeiters, ist auch Art. 28 DS-GVO einschlägig.

Arbeitgeber sind also dazu berechtigt und teilweise auch verpflichtet, die Personalausweise und Fahrerlaubnispapiere ihrer Beschäftigten zu kontrollieren. Dabei haben sie aber die geltenden datenschutzrechtlichen Bestimmungen zu beachten. Diese erlauben das Anfertigen von Kopien und das Speichern der Papiere nicht oder nur mit Einwilligung der Beschäftigten. Von einer Einwilligungslösung rate ich wegen der hohen Anforderungen an eine wirksame Einwilligung im Beschäftigungsverhältnis ab.

8. Internet und Medien

Bezogen auf das Internet ist die wichtigste Entwicklung der letzten Jahre die Verbreitung cloud-gestützter Systeme Künstlicher Intelligenz. Diese verursacht durch völlig neue Verarbeitungsweisen personenbezogener Daten vielfältige neue Datenschutzprobleme, weil weder die DSGVO noch das BDSG oder das HDSIG diese neuen Verarbeitungsformen berücksichtigen konnten. Daher müssen angesichts der schnellen und revolutionären Entwicklung „alte" Regelungen auf neue Sachverhalte angewendet werden, für die sie nicht unmittelbar passen (Kap. 8.1). Eine im Verhältnis dazu vergleichsweise konventionelle Frage ist die, ob und wann Einwilligungen der richtige Erlaubnistatbestand für Datenverarbeitungen im Internet darstellen. Dies ist viel seltener als gemeinhin gedacht der Fall (Kap. 8.2). Oft erreichen mich Beschwerden gegen die Datenverarbeitung zur Erhebung des Rundfunkbeitrags, die allerdings unbegründet sind (Kap. 8.3).

8.1 Datenschutz und KI – Aktuelle Entwicklungen

In den letzten Jahren hat das Thema Künstliche Intelligenz (KI) in allen Bereichen der Datenverarbeitung enorm an Bedeutung gewonnen. Mit der zunehmenden Einführung und Nutzung von KI-Anwendungen in unterschiedlichsten Lebensbereichen und zu verschiedensten Zwecken stellen sich auch immer mehr grundlegende datenschutzrechtliche Fragen. Zusammen mit den deutschen und europäischen Datenschutzaufsichtsbehörden befasse ich mich mit deren Beantwortung. Zu Fragen des Datenschutzes bei Systemen Künstlicher Intelligenz s. auch Kap. 2 (Beschluss des EDSA zu LLM) und Kap. 5.1 (Datenschutz und Künstliche Intelligenz in der Verwaltung).

Große Sprachmodelle als Herausforderungen des Datenschutzes

KI-Anwendungen sind inzwischen im digitalen Mainstream und im Alltag vieler Menschen angekommen. Seitdem vor allem auf Large Language Models (LLM) basierende Chatbots wie z. B. ChatGPT oder Gemini große Popularität und Verbreitung gefunden haben, stellen sich aus datenschutzrechtlicher Sicht eine Vielzahl von Fragen, wie mit dieser Technologie im Einzelfall umzugehen ist und welche Auswirkungen das Training und die Nutzung von KI auf das Persönlichkeitsrecht hat und zukünftig noch haben wird.

Ich beschäftige mich daher auf verschiedenen Ebenen ausführlich mit dem Thema Künstliche Intelligenz. So erreichen mich Anfragen zum Einsatz von KI, mit denen Verantwortliche Rat bei der Frage suchen, ob bestimmte KI-Anwendungen überhaupt bzw. für den jeweils vorgesehenen Zweck ein-

gesetzt werden dürfen. Daneben gibt es umfangreiche Abstimmungen über grundlegende Fragen der Datenverarbeitung mittels KI. Diese geschehen sowohl mit den deutschen Aufsichtsbehörden, im Rahmen der Konferenz der DSK und ihrer Untergliederungen als auch mit den anderen europäischen Aufsichtsbehörden im Rahmen des EDSA. Ziel dabei ist, dass die datenschutzrechtliche Bewertung von KI-Anwendungen deutschland- und europaweit einheitlich erfolgt und die Anwender und betroffenen Personen Klarheit und Rechtssicherheit im Umgang mit diesen zumindest in der Massenanwendung noch recht neuen Technologien erhalten. Siehe zum Verfahren nach Art. 64 Abs. 2 DS-GVO, das die irische Aufsichtsbehörde zu vier Fragen hinsichtlich der datenschutzrechtlichen Bewertung von LLM angestrengt hat und zu dessen Abschluss der EDSA am 17. Dezember 2024 eine Stellungnahme abgegeben hat, Kap. 2.

In der Praxis zeigt sich dabei, dass die Anwendung des Datenschutzrechts auf moderne KI-Anwendungen keineswegs trivial ist. Beim Erlass des geltenden Datenschutzrechts hatten die europäischen und deutschen Gesetzgeber die „klassische“ Datenverarbeitung vor Augen. In dieser werden Daten in klar geordneten Systemen eindeutig und physisch nachvollziehbar gespeichert, zugeordnet, verändert und gelöscht. All dies ist bei KI-Anwendungen hingegen nicht in der bisherigen Form gegeben.

Künstliche Intelligenz kann in sehr vielen verschiedenen Varianten auftreten, mit denen in ganz unterschiedlicher Weise zu unterschiedlichsten Zwecken Daten verarbeitet werden können. Der Fokus meiner Betrachtungen im Berichtszeitraum lag vor allem auf generativen Large Language Models (LLM), die schriftliche und zunehmend auch mündliche Anfragen verarbeiten und umfassende schriftliche und mündliche Antworten ausgeben können. Gerade textbasierte KI-Anwendungen, die ein Training mittels riesiger Mengen an Texten und Informationen voraussetzen, bergen besondere Risiken im Zusammenhang mit der Verarbeitung von personenbezogenen Daten. Hierbei dürfte es nahezu unmöglich sein, ein LLM zu trainieren, ohne dass in den Trainingsdatensätzen vielfältige Informationen zu einer großen Anzahl natürlicher Personen enthalten sind.

Im Kontext „Großer Sprachmodelle“ standen daher wie auch im vergangenen Berichtszeitraum Datenschutzgrundsätze wie Zweckbindung und Datenminimierung im Zentrum der Aufmerksamkeit und wurden in der DSK eingehend und teilweise öffentlich diskutiert. Die Frage, ob personenbezogene Daten in LLM gespeichert sind, wenn diese in Trainingsdaten enthalten waren, war eine der wesentlichen Fragen, in deren Diskussion ich mich maßgeblich eingebracht habe. Die unter meinem DSK-Vorsitz vorgenommene rechtliche und technische Erörterung des Trainings von generativen

KI-Modellen (LLM) ergab, dass in den allermeisten Fällen eine Verarbeitung personenbezogener Daten nicht auszuschließen ist (DSK, Strategieklausur der Datenschutzkonferenz in Speyer: Nutzung von KI zentrales Thema, 2. September 2024, https://datenschutzkonferenz-online.de/media/pm/2024-09-02_Klausurtagung_KI.pdf).

Entwicklungen an der Schnittstelle KI und Datenschutz

Innerhalb der Datenschutzkonferenz wurden Fragestellungen zum Thema Künstliche Intelligenz zunächst von der Task Force KI begleitet, die vor einigen Jahren gegründet wurde, um in Einzelfällen Themen aus dem Bereich KI zu bearbeiten. Da die Nutzung Künstlicher Intelligenz mittlerweile aber eine zentrale Herausforderung für die Datenschutzpraxis darstellt, hat die Datenschutzkonferenz unter meinem Vorsitz den „Arbeitskreis Künstliche Intelligenz“ gegründet. Dadurch soll eine dauerhafte und regelmäßige Befassung mit dem Thema gewährleistet werden. Der Arbeitskreis KI ist interdisziplinär mit Fachleuten aus allen deutschen Datenschutzaufsichtsbehörden besetzt. Durch diese Bündelung von juristischem und technischem Fachwissen ist dieser in der Lage, die Datenschutzkonferenz dabei zu unterstützen, Entwicklungen im Bereich Künstlicher Intelligenz zu begleiten und einen wertvollen Beitrag zur öffentlichen Diskussion zu leisten. Er hat daher im Wesentlichen die Aufgaben, innerhalb der Datenschutzkonferenz sowie mit Blick auf die Gremien der europäischen Datenschutzaufsichtsbehörden eine Schnittstelle zu bilden, an der sämtliche Informationen zum Thema KI zusammengetragen werden. Zum anderen wird der Arbeitskreis aktuelle Fragestellungen für die Datenschutzkonferenz aufbereiten und gegebenenfalls Orientierungshilfen für die Verantwortlichen in Deutschland erarbeiten.

Wichtig für den Datenschutz ist die klare Definition dessen, was unter KI zu verstehen ist (s. zur Definition von KI Kap. 5.1). Aufgrund der jahrzehntelangen Entwicklung von KI lässt sich nur schwer eine allgemeingültige Definition finden, die für die Bewältigung konkreter datenschutzrechtlicher Probleme geeignet ist.

Am 1. August 2024 ist die europäische Verordnung über Künstliche Intelligenz in Kraft getreten. Diese Verordnung ist weltweit eine der ersten umfassenden Regelungen im Bereich der Künstlichen Intelligenz. Ihr Ziel ist es sicherzustellen, dass in der Europäischen Union entwickelte und eingesetzte Künstliche Intelligenz vertrauenswürdig ist und die Grundrechte der Menschen schützt. Die Verordnung schafft einen harmonisierten Binnenmarkt für KI, der Innovationen und Investitionen verantwortungsvoll fördert. Die Verordnung definiert verschiedene Risikostufen für Systeme Künstlicher Intelligenz, die verschiedenen gestuften Pflichten unterliegen. KI-Systeme

wie Empfehlungssysteme und Spamfilter unterliegen keinen besonderen Verpflichtungen, da sie ein geringes Risiko darstellen. Unternehmen können jedoch freiwillig Verhaltenskodizes implementieren. Systeme wie Chatbots müssen Nutzer darüber informieren, dass sie mit einer Maschine interagieren. So müssen zum Beispiel Deepfakes und biometrische Erkennungssysteme gekennzeichnet werden und synthetische Inhalte müssen maschinenlesbar als künstlich erzeugt erkennbar sein. Strenge Anforderungen gelten für hochriskante KI-Systeme, wie solche zur Personalauswahl oder zur Kreditwürdigkeitsbewertung. Diese Systeme müssen robust, genau und sicher sein und umfangreiche Dokumentations- und Überwachungsanforderungen erfüllen. Abschließend aufgelistete Systeme, die eine klare Bedrohung für Grundrechte darstellen, sind verboten. Dazu gehören beispielsweise Systeme, die das Verhalten manipulieren oder eine soziale Bewertung ermöglichen, und bestimmte Anwendungen der polizeilichen Überwachung.

Unternehmen können bei Verstößen mit hohen Geldstrafen belegt werden. Diese Strafen können bis zu 7% des weltweiten Jahresumsatzes für Verstöße im Zusammenhang mit verbotenen KI-Anwendungen betragen, bis zu 3 % für Verstöße gegen andere Verpflichtungen und bis zu 1,5 % für die Übermittlung falscher Informationen.

Die meisten Vorschriften der neuen KI-Verordnung gelten ab dem 2. August 2026. Die Mitgliedstaaten müssen bis zum 2. August 2025 ihre nationalen Behörden benennen, welche die Einhaltung der Vorschriften für KI-Systeme überwachen und die Marktaufsicht übernehmen. Die Bundesregierung beabsichtigt, diese Aufsicht allein der Bundesnetzagentur zu übertragen. Da die KI-Verordnung in Art. 77 KI-VO für den Grundrechtsschutz ohnehin die Datenschutzbehörden vorgesehen hat und diesen außerdem in Art. 74 Abs. 8 KI-VO in vier von acht Risikobereichen die Marktaufsicht überträgt, ist es jedoch sinnvoll, die Marktüberwachung in den anderen Risikobereichen auch den unabhängigen und sachkundigen Datenschutzbehörden anzuvertrauen.

Es wird künftig eine der Aufgaben der Datenschutzaufsichtsbehörden sein, die Entwicklungen an der Schnittstelle zwischen DS-GVO und KI-Verordnung zu beobachten und zu begleiten.

Herausforderungen und Antworten

Von den vielen datenschutzrechtlichen Fragen, die sich im Zusammenhang mit KI derzeit stellen, ist die Frage nach dem Personenbezug von Daten innerhalb von KI-Systemen für die Anwendbarkeit des Datenschutzrechts von wesentlicher Bedeutung. Aus diesem Grund stand sie auch zum Berichtszeitpunkt im Mittelpunkt der Betrachtungen.

Datenschutzrechtliche Vorgaben gelten nach Art. 2 Abs. 1 DS-GVO nur, soweit Informationen verarbeitet werden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DS-GVO). Ausgehend von der Frage, ob LLM, die mit personenbezogenen Daten trainiert wurden, auch personenbezogene Daten enthalten, ergaben sich deshalb im Berichtszeitraum eine Reihe von zum Teil noch in Klärung befindlichen datenschutzrechtlichen Herausforderungen.

Davon ausgehend, dass unter den Milliarden notwendiger Trainingsdaten auch personenbezogene Daten sind, enthalten auch LLM personenbezogene Daten. Das Ungewöhnliche an der Speicherung personenbezogener Daten in LLM ist, stark vereinfacht gesagt, dass die Speicherung nicht nur auf die einzelnen Parameter verteilt erfolgt. Sie geschieht im Rahmen eines iterativen Optimierungsansatzes auch zeitlich hintereinander, so dass die Werte der einzelnen Parameter durch die Daten des jeweils nächsten Schritts erneut verändert werden. Parameter in LLM definieren die Transformation der Eingabedaten in die Ausgabe des KI-Modells. Diese Parameter, etwa Gewichtungen zwischen den neuronalen Knoten oder Korrekturen, steuern die Auswirkungen bestimmter Eingabemerkmale auf die resultierende Ausgabe. Die Komplexität und Richtigkeit der Antworten eines LLM steigt mit der Anzahl der Parameter, die bei großen LLM in dreistelliger Milliardenhöhe liegen.

Da bei diesem Verfahren zum Beispiel die sinnhafte Nähe und die Position aller in den Trainingsdaten enthaltenen Inhalte im Bezug zueinander verarbeitet und in die sogenannten Parameter eingebracht werden, bleibt bei personenbezogenen Daten auch der Personenbezug erhalten. So können gegebenenfalls sogar aus nicht personenbezogenen Eingaben während der Nutzung personenbezogene Daten hergestellt werden. Dazu kommt, dass LLM sich neben herkömmlichen IT-Komponenten auch aus unterschiedlichen KI-Modellen zusammensetzen. Einige dieser KI-Modelle sind für die Vor- und Nachverarbeitung von Daten verantwortlich. Deshalb muss bei der datenschutzrechtlichen Bewertung von LLM nicht nur das Herzstück des KI-Systems analysiert werden, sondern auch die KI-Systeme und -Modelle, die zum Beispiel für die Vor- und Nachverarbeitung eingesetzt werden.

Irritierend wirkte zu Beginn der geführten Diskussion, dass die Daten im Vergleich zur klassischen Datenspeicherung nicht linear einsehbar oder auslesbar sind. Die primäre Aufgabe von LLM, die zum Beispiel als Chat-Bots eingesetzt werden, ist nicht die Speicherung von Daten, sondern die Generierung von Ausgaben, die menschliche Kommunikation imitieren. Hierzu sollen sie möglichst kohärent erscheinen und ihre Ausgaben der menschlichen Sprache möglichst ähnlich sein. Deshalb können die in den

Parametern gespeicherten personenbezogenen Daten nicht mit einer Datenbanksprache, wie zum Beispiel SQL, abgefragt werden. Die Ausgabe erlernter personenbezogener Daten erfolgt unmittelbar durch die Verwendung des KI-Modells. Die Stärke von LLM liegt in der guten Korrelationsfähigkeit, das heißt in der Fähigkeit, Ähnlichkeiten und Muster zu erkennen. Das Schließen kausaler Zusammenhänge gehört jedoch nicht zu ihren Stärken. Daher gibt es qualitative Probleme bei dem Versuch, so menschlich wie möglich aussehende Ergebnisse zu erhalten. Zum Beispiel kann es systembedingt dazu kommen, dass Antworten, die auch personenbezogene Daten enthalten können, sachlich und ethisch falsch sind. Die Tatsache steht aber nicht im Widerspruch zu der Aussage, dass personenbezogene Daten in den LLM gespeichert sind. Die genannten Defizite sind ein Hinweis auf qualitative Mängel bei der Speicherung und der Ausgabe. Diese Erkenntnisse führen zu einer Reihe von Herausforderungen für den Datenschutz, wie etwa bei der Umsetzung der Betroffenenrechte.

Angesichts der oben skizzierten außergewöhnlichen Art und Weise, in der personenbezogene Daten in LLM gespeichert werden, haben sich im Berichtszeitraum wichtige und zum Teil noch offene Fragen zu den Rechten der betroffenen Personen ergeben. Die DS-GVO gibt Betroffenen eine Reihe von Rechten an die Hand, die diese in die Lage versetzen sollen, auf unterschiedliche Weise Informationen über die genaue Verarbeitung ihrer Daten zu erhalten und zum Beispiel gespeicherte Daten gegebenenfalls zu berichtigen oder zu löschen. Im Berichtszeitraum haben sich aus der Diskussion um die Frage, ob personenbezogene Daten in LLM enthalten sind, neue zusätzliche Fragestellungen ergeben, z. B. mit Blick auf die Betroffenenrechte aus Art. 15 ff. DS-GVO. Der Verantwortliche kann personenbezogene Daten in KI-Systemen nicht in der gleichen Weise, wie dies vom bisherigen Datenschutzrecht vorausgesetzt und in herkömmlichen Datenbanken möglich ist, beauskunften oder löschen. Daher müssen aus Sicht des Datenschutzes technologisch bedingt andere angemessene und wirksame Ansätze gefunden werden, um eine datenschutzkonforme Verarbeitung personenbezogener Daten in LLM zu ermöglichen.

So können beispielsweise mit dem Recht auf Auskunft nach Art. 15 DS-GVO betroffene Personen von dem für die Datenverarbeitung in einem LLM Verantwortlichen Auskunft darüber verlangen, welche Daten über sie im LLM gespeichert sind bzw. im Rahmen des Trainings verarbeitet wurden. LLM haben jedoch in der Regel die Eigenschaft, dass die Trainingsdaten nach Abschluss des Trainings für den weiteren Betrieb des KI-Systems nicht mehr benötigt werden. Ohne die Trainingsdaten kann nach derzeitigem Kenntnisstand in der Regel keine verlässliche und vollständige Auskunft darüber erteilt werden, ob und welche Daten konkret als Trainingsdaten verarbeitet wurden und in

dem LLM enthalten sind. Hier müssen zukünftig Lösungsansätze gefunden werden, die im Einklang mit der DS-GVO stehen.

Außerdem gewährt die DS-GVO allen Betroffenen, deren personenbezogene Daten im Rahmen des Trainings verarbeitet werden, nach Art. 16 DS-GVO das Recht auf Berichtigung. Nach Art. 17 DS-GVO haben darüber hinaus Betroffene das Recht auf Löschung ihrer personenbezogenen Daten. Wie bereits erwähnt, weisen LLM zum Teil qualitative Defizite auf, die im Betrieb zur Ausgabe falscher personenbezogener Daten führen. Eine gezielte Korrektur oder Löschung von einzelnen personenbezogenen Daten aus trainierten Parametern von LLM ist nach heutigem Stand mit vertretbarem Aufwand nicht vollumfänglich und zuverlässig möglich. Deshalb muss die weitere Entwicklung vorhandener Ansätze beobachtet und zum Beispiel über andere kompensierende Maßnahmen nachgedacht werden.

Ausblick

Obwohl viele Menschen in ihrem privaten oder beruflichen Alltag bereits mit KI-Anwendungen in Kontakt gekommen sind, steht deren Einsatz in Unternehmen, Behörden sowie auch im privaten Umfeld sicherlich noch am Anfang. Ebenso sind auch die vielfältigen, damit im Zusammenhang stehenden datenschutzrechtlichen Probleme und Aufgaben noch nicht vollständig gelöst. Auch über die bisher bekannten Anwendungen hinaus werden in Zukunft viele weitere KI-Anwendungen und neue Technologien entwickelt werden und in einigen Bereichen zweifellos umfassende Änderungen mit sich bringen.

Es ist Aufgabe der Datenschutzbehörden, diese Entwicklungen zu beobachten, kritisch, aber auch konstruktiv zu begleiten und sowohl den Anwendern als auch insbesondere den betroffenen Personen solcher Datenverarbeitungen mit Rat und Tat zur Seite zu stehen. Dabei kommt den gesetzlich in Art. 5 DS-GVO festgeschriebenen Grundsätzen des Datenschutzrechts besondere Bedeutung zu. Auch wenn der im Rahmen von KI erforderliche Umgang mit riesigen Datenmengen auf den ersten Blick im Widerspruch zu Grundsätzen wie Datenminimierung, Zweckbindung oder Speicherbegrenzung stehen mag, können deren Hersteller und Anwender dennoch an verschiedenen Stellen wirksame Maßnahmen ergreifen, um diese Grundsätze hinreichend zu beachten. KI-Anwendungen, die diesen Grundsätzen genügen und in transparenter, nachvollziehbarer, integrer und vor allem rechtmäßiger Weise Daten verarbeiten, können eine enorme technische Bereicherung sein, ohne dabei Persönlichkeitsrechte zu gefährden oder gar zu verletzen.

8.2
Nicht überall nur Einwilligungen!

Viele Verantwortliche für Online-Angebote holen für die dortigen Verarbeitungen personenbezogener Daten Einwilligungen der Nutzer ein, ohne dass dies erforderlich ist. Checkboxen zur Erteilung einer Einwilligung unter Anfrage-, Kontakt- und Bestellformularen im WWW sind oftmals unnötig, wenn nicht gar falsch und können zudem rechtliche Probleme nach sich ziehen. Solche Checkboxen und Einwilligungstexte sind auch bei Datenschutzhinweisen fehl am Platz, denn in einseitige Unterrichtungen durch Verantwortliche, die ausschließlich der Transparenz dienen sollen, können Nutzer grundsätzlich nicht einwilligen.

Grundlegendes Missverständnis

Bei der Einführung der DS-GVO im Jahr 2018 war in vielen populären Medien immer wieder fälschlicherweise die Rede davon, dass nun für alle Verarbeitungen personenbezogener Daten stets eine Einwilligung der betroffenen Personen rechtlich erforderlich sei. Die Folge war eine wahre Einwilligungsflut, der die Bevölkerung in so gut wie jeder alltäglichen Datenerhebungssituation ausgesetzt war. Es entstand ein Mythos von der Einwilligung als „Königin der Rechtsgrundlagen“, der sich leider bis heute gehalten hat, was ich auch im Rahmen meiner Aufsichtstätigkeit bei digitalen Diensten immer wieder feststellen muss.

Für die Verarbeitung personenbezogener Daten kommen aber nach Art. 6 Abs. 1 UAbs. 1 DS-GVO neben der Einwilligung noch weitere und durchaus geeignetere, praktikablere und einfachere Rechtsgrundlagen als die Einwilligung in Frage:

Art. 6 Abs. 1 UAbs. 1 DS-GVO

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

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

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

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

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

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

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

Einwilligungen bei Kontakt- und Anfrage-Formularen im WWW

Viele WWW-Anbieter erheben personenbezogene Daten ihrer Nutzenden zu unterschiedlichsten Zwecken über Online-Formulare, um die Daten dann zu dem jeweiligen Zweck weiterzuverwenden. Dabei holen die für die Online-Angebote Verantwortlichen oftmals Einwilligungen für die Verarbeitung der Daten ihrer Nutzenden ein, ohne dass dies rechtlich wirklich notwendig wäre. So befinden sich bei vielen Kontakt- und Anfrageformularen, über die sich Dienste-Nutzende mit ihren Anliegen an die Anbieter wenden können, unter den Datenerhebungsmasken neben einem Link zum Datenschutzhinweis unvorbelegte Optionsfelder oder Checkboxen mit Texten wie „*Ich stimme der Verarbeitung meiner Daten zu*“ oder „*Ich willige in die Verarbeitung meiner Daten ein*“, die vor dem Absenden des Formulars zu bestätigen sind.

Wenn Nutzende digitaler Dienste dem Anbieter eine Frage über ein Online-Formular stellen, sei es – je nach Angebot – zu seinen angebotenen Informationen, seinem Forum, seiner Plattform, seiner Community oder seinen Dienstleitungen oder Produkten, haben sie selbstverständlich immer ein großes Interesse an einer Antwort. Sie erwarten dann, dass der Anbieter ihre angegebenen Kontaktdaten zügig dazu verwendet, um je nach Angebot, Frage und Erhebungssituation auf ihre Fragen per Telefon, Post oder E-Mail zu reagieren. Und der Anbieter eines solchen digitalen Dienstes ist i. d. R. bestrebt, den Kontakt zu seinen Interessenten herzustellen und bei diesen so gut wie möglich das Interesse an seinem Online-Angebot zu wecken oder aufrechtzuerhalten. Der Anbieter hat also ein berechtigtes Interesse an der Verarbeitung der von den Nutzenden in einem Anfrage- oder Kontaktformular angegebenen Daten und die Nutzenden haben selbst ein großes Interesse an der Verarbeitung seiner Daten zum Erhalt einer Antwort. Und die Verarbeitung der erhobenen Kontaktdaten ist zur Beantwortung der gestellten Frage auch erforderlich. Hier ist ganz deutlich Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO die passende und richtige Rechtsgrundlage für die Datenverarbeitung, da berechtigte Interessen des Verantwortlichen bestehen, die Erforderlichkeit der Datenverarbeitung außer Frage steht und die in der Vorschrift geforderte Interessenabwägung klar zugunsten des Verantwort-

lichen und seiner Datenverarbeitung ausgeht. Eine zusätzliche Einwilligung der Dienstenutzenden in die Verarbeitung ihrer Daten ist in solchen Fällen offensichtlich nicht notwendig, sie ist überflüssig.

Eine zusätzliche Einwilligung wäre nur dann notwendig, wenn die erhobenen Daten auch noch für andere Zwecke verwendet werden sollten als zur Beantwortung der gestellten Anfrage. Dann aber müsste diese Einwilligung transparent, hinreichend bestimmt, also informiert und auch wahlfrei sein. Das bedeutet, sie müsste konkret, deutlich und verständlich über diese weiteren Zwecke informieren und als freiwillige Einwilligung ausgestaltet sein. Ein Anfrageformular muss sich also stets auch ohne Erteilung einer Zusatz-Einwilligung für die Datenverarbeitung zu anderen Zwecken absenden lassen:

Art. 4 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

11. „Einwilligung" der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist; (…)

Einwilligungen bei Registrierungs- und Bestellformularen

Ähnliche Fehler fallen mir auch regelmäßig bei Registrierungs-, Anmelde- und Bestellformularen gewerblicher Anbieter auf, die über ihre Online-Dienste kostenpflichtig ihre Dienstleistungen und Produkte anbieten und über ihre Websites entsprechende Verträge mit ihren Kunden abschließen. Auch dort findet sich oftmals ein zu bestätigender Einwilligungstext unter den jeweiligen Datenerhebungsformularen. Dabei lässt sich das Formular in manchen Fällen nicht absenden, also die Registrierung als Kunde nicht vornehmen oder die Bestellung nicht aufgeben, wenn die Checkbox vor dem Einwilligungstext nicht angehakt wurde. Abgesehen davon, dass eine solche „Einwilligung" schon aufgrund mangelnder Freiwilligkeit nicht wirksam ist, ist das Einholen einer Einwilligung auch hier gar nicht erforderlich, da schon der Vertrag oder das vertragsähnliche Verhältnis zwischen Anbieter und Nutzenden nach Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO als Rechtsgrundlage hinreichend belastbar ist.

Eine Einwilligung ist also auch in solchen vertraglichen, vorvertraglichen oder vertragsähnlichen Verarbeitungskontexten nicht notwendig und überflüssig. Und sie wäre bei genauerer Betrachtung sogar schädlich, denn Einwilligungen

müssen stets auch widerrufen werden können. Über das Widerrufsrecht ist zu informieren:

Art. 7 Abs. 3 Satz 1 – 3 DS-GVO

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

Sollten also Nutzende oder Kunden ihre Einwilligung – aus welchem Grund auch immer – später widerrufen, würde dem verantwortlichen Anbieter plötzlich die ursprüngliche Rechtsgrundlage für die Verarbeitung der Daten seiner Nutzenden oder Kunden fehlen. Die weitere Verarbeitung der Bestandskundendaten nach Rücknahme der Einwilligung könnte dann möglicherweise rechtswidrig sein. Um solche juristisch komplexen Fragen erst gar nicht aufkommen zu lassen, sollten Einwilligungslösungen in vertraglichen, vorvertraglichen und vertragsähnlichen Datenerhebungssituationen unterlassen werden.

Einwilligungen bei Online-Datenschutzhinweisen

Ein weiterer Fehler, den das eingangs erwähnte vermeintliche „Einwilligungs-Dogma“ der DS-GVO hervorgerufen hat und auf den ich auch heute immer noch bei Online-Angeboten treffe, ist das Einholen einer Einwilligung in die Datenschutzhinweise, also in die Unterrichtungen über die Verarbeitung personenbezogener Daten, die Anbieter nach Art. 13 DS-GVO für ihre Nutzer bei der Erhebung personenbezogener Daten bereithalten müssen. Hierfür finden sich unter Datenerhebungsformularen unvorbelegte Checkboxen mit Texten wie „Ich bin mit den Datenschutzhinweisen einverstanden“ oder „Die Datenschutzhinweise habe ich zur Kenntnis genommen und stimme ihnen zu“. Die Checkboxen müssen oftmals zwingend angekreuzt werden, bevor das Online-Formular abgesandt werden kann.

Bei Datenschutzhinweisen handelt es sich aber lediglich um einseitige datenschutzrechtliche Unterrichtungen, die der Transparenz dienen sollen. Die dortigen Informationen sollen den Nutzenden die Möglichkeit geben, dort nachzulesen, welche Daten zu welchen Zwecken auf welcher Rechtsgrundlage verarbeitet werden, an welche Empfänger die Daten weitergegeben werden, wie lange die Speicherung voraussichtlich erfolgt, etc. Es handelt sich also um Informationen, zu deren Bereitstellung die Verantwortlichen gesetzlich verpflichtet sind. Nutzende digitaler Dienste sind allerdings nicht rechtlich

verpflichtet, diese Informationen auch zur Kenntnis zu nehmen oder zu lesen. Sie müssen lediglich die Möglichkeit dazu haben. Ob ein Websitebesucher oder Dienste-Nutzer etwas bestätigt, akzeptiert, zur Kenntnis nimmt oder nicht, spielt einerseits keine Rolle für die Erfüllung der Informationspflicht durch den Anbieter nach Art. 13 DS-GVO und wirkt sich andererseits nicht auf die Rechtmäßigkeit der Datenverarbeitungen aus, über die informiert wird.

Wenn Nutzende sich an Informationen über die beabsichtigten Verarbeitungen ihrer personenbezogenen Daten stören, die sie in Datenschutzhinweisen lesen, können sie die Entscheidung darüber treffen, ihre Daten dort eventuell gar nicht anzugeben und den Dienst nicht zu nutzen. Nutzende können den Datenschutzhinweisen aber nicht widersprechen und sie können grundsätzlich auch nicht in diese Pflichtinformationen einwilligen. Daher sind solche Einwilligungslösungen mit Bezug auf Datenschutzhinweise stets falsch und i. d. R. nur ein Anzeichen rechtlicher Unsicherheit des Verantwortlichen.

Einwilligungen innerhalb von Online-Datenschutzhinweisen

Etwas seltener, aber immer wieder fallen mir Online-Datenschutzhinweise auf, in denen nicht nur die Pflichtinformationen nach Art. 13 DS-GVO enthalten sind, zu deren Bereitstellung Verantwortliche verpflichtet sind, sondern die zusätzlich auch Textelemente enthalten, die als Einwilligungen formuliert sind. Datenschutzhinweise nach Art. 13 DS-GVO dienen, wie bereits dargestellt, jedoch nur der Unterrichtung, also der Information der Seitennutzenden. Websiteanbieter und Verantwortliche erfüllen so ihre einseitige Informationspflicht bei der Online-Datenerhebung.

Auf keinen Fall sollten datenschutzrechtliche Unterrichtungen für Betroffene mit Willenserklärungen von Betroffenen, an die auch noch besondere rechtliche Wirksamkeitsanforderungen (transparent, bestimmt, informiert, freiwillig, widerrufbar) zu stellen sind, vermischt werden. Und wenn dann wirklich als Rechtsgrundlage über Art. 6 Abs. 1 UAbs. 1 Buchst. b oder f DS-GVO hinaus noch eine gesonderte Einwilligungserklärung erforderlich wäre, z. B. bei zusätzlichen Verwendungszwecken, muss die dafür erforderliche Einwilligung zwingend an einer anderen Stelle außerhalb des Datenschutzhinweises eingeholt werden. Denn ein Ersuchen um eine Einwilligung muss nach Art. 7 Abs. 2 Satz 1 DS-GVO immer in einer Form so erfolgen, dass es von anderen Sachverhalten klar zu unterscheiden ist. Eine Einwilligung mitten in einem Datenschutzhinweistext unterzubringen, wie es ab und zu geschieht, und damit eher unauffällig, ja schon fast „versteckt“ zu positionieren, entspricht diesen Anforderungen nicht. Daher sind solche Einwilligungen auch nicht wirksam und können eine darauf gestützte Datenverarbeitung nicht rechtfertigen.

Zusammenfassend bleibt festzuhalten, dass Verantwortliche immer darauf achten sollten, dass Einwilligungen oftmals gar nicht erforderlich sind, da Art. 6 Abs. 1 DS-GVO den Anbietern durchaus noch weitere belastbare und auch praktikablere Rechtsgrundlagen zur Verfügung stellt als die Einwilligung der betroffenen Person.

8.3
Die Beitreibung des Rundfunkbeitrags

Immer wieder richten sich Beschwerden gegen die Datenverarbeitung der öffentlich-rechtlichen Rundfunkanstalten, die zum Zweck erfolgt, den Rundfunkbeitrag einzuziehen. Diese ist jedoch nicht zu beanstanden. Der Rundfunkbeitrag stellt die wesentliche Finanzierungsquelle der Rundfunkanstalten dar, denn er versetzt sie in die Lage, ihren verfassungsrechtlichen Auftrag umzusetzen.

Im Berichtszeitraum erreichten mich vielfach Eingaben, die Datenverarbeitungen im Rahmen der Beitreibung fälliger Rundfunkbeiträge zum Gegenstand hatten. So wurden die Übermittlungen personenbezogener Daten der Rundfunkbeitragsschuldner an Vollstreckungsbeamte der Landkreise oder Gemeinden oder an Inkassounternehmen gerügt.

Zur Gewährleistung der Rundfunkfreiheit gehört auch die Sicherung der Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks unter Einschluss seiner bedarfsgerechten Finanzierung. Dementsprechend steht den öffentlich-rechtlichen Rundfunkanstalten, wie etwa dem Hessischen Rundfunk, ein grundrechtlicher Finanzierungsanspruch zu. Daher finanziert sich der öffentlich-rechtliche Rundfunk neben Einnahmen aus Rundfunkwerbung und sonstigen Einnahmen entsprechend § 35 Satz 1 MStV vorrangig aus dem Rundfunkbeitrag. Ihm kommt im Rahmen der dualen Rundfunkordnung eine besondere Bedeutung zu. Er soll unabhängig von Einschaltquoten und Werbeaufträgen ein Programm anbieten, das den verfassungsrechtlichen Anforderungen gegenständlicher und meinungsmäßiger Vielfalt entspricht. Gemäß seinem Auftrag – festgehalten in § 26 Abs. 1 Satz 1 MStV – hat er durch die Herstellung und Verbreitung seiner Angebote als Medium und Faktor des Prozesses freier, individueller und öffentlicher Meinungsbildung zu wirken und dadurch die demokratischen, sozialen und kulturellen Bedürfnisse der Gesellschaft zu erfüllen. Daher ist er im Wesentlichen öffentlich finanziert und nicht, wie die privaten Programmanbieter, von Werbeaufträgen oder Einschaltquoten abhängig (s. zu alledem BVerfGE 119, 181, 214 m. w. N.; BVerfGE 158, 389, Rn. 79).

Die Regelungen über die Entstehung, Erhebung und Vollstreckung der Rundfunkbeitragsschuld finden sich im Rundfunkbeitragsstaatsvertrag. Dieser stellt einen Staatsvertrag zwischen allen Bundesländern dar. Da Rundfunk Ländersache ist, regelt er die Erhebung von Rundfunkbeiträgen durch die öffentlich-rechtlichen Rundfunkanstalten. Durch die Zustimmungsgesetze der Landesparlamente wird der Staatsvertrag in den Rang eines Landesgesetzes erhoben.

Die Landesrundfunkanstalten verarbeiten zum Zwecke des Beitragseinzugs Daten der Beitragsschuldner. Die Datenverarbeitung zum Zwecke des Beitragseinzugs stellt ein wichtiges Ziel des allgemeinen öffentlichen Interesses dar, denn sie dient dazu, die verfassungsrechtlich garantierte, funktionsgerechte Finanzausstattung des öffentlich-rechtlichen Rundfunks sicherzustellen (Hessischer Landtag, Drucksache 19/6048, S. 17f.). Damit besteht für diese Datenverarbeitung eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO i. V. m. § 1 RBStV, § 26 Abs. 1 MStV. Sie ist daher zulässig.

Rückständige Rundfunkbeiträge werden gemäß § 10 Abs. 5 RBStV durch Verwaltungsakt der zuständigen Rundfunkanstalt festgesetzt. Die Vollstreckung des Bescheides erfolgt gemäß § 10 Abs. 6 RBStV im Verwaltungsvollstreckungsverfahren entsprechend § 17 Abs. 1 HessVwVG. Allerdings entsteht die Beitragspflicht nicht erst durch den Erlass des Verwaltungsaktes, sondern nach § 7 RBStV kraft Gesetzes durch die Verwirklichung des beitragspflichtigen Tatbestandes. Daher muss die Rundfunkanstalt keinen zusätzlichen, der Festsetzung vorausgehenden Bescheid erlassen, um Vollstreckungsmaßnahmen einzuleiten. Die Gemeinden bzw. die Landkreise für Gemeinden ohne eigene Vollziehungsbeamte oder Vollstreckungsstellen sind auf Ersuchen des Hessischen Rundfunks verpflichtet, rückständige Rundfunkgebühren beizutreiben (Art. 4 § 1 Abs. 1 des Gesetzes zu dem Staatsvertrag über den Rundfunk im vereinten Deutschland in der Fassung des Gesetzes zu dem Neunzehnten Rundfunkänderungsstaatsvertrag und zur Änderung des Gesetzes zu dem Staatsvertrag über den Rundfunk im vereinten Deutschland vom 27. Juni 2016). Der Hessische Rundfunk ist damit berechtigt, die personenbezogenen Daten der säumigen Rundfunkbeitragsschuldner an die Vollstreckungsstellen zu übermitteln.

Nach § 10 Abs. 7 Satz 2, § 9 Abs. 2 Satz 1 RBStV i. V. m. § 16 Abs. 1, 2 der Satzung des Hessischen Rundfunks über das Verfahren zur Leistung der Rundfunkbeiträge kann der Hessische Rundfunk auch Dritte wie Inkassounternehmen mit Inkassomaßnahmen beauftragen. Es ist vertraglich und technisch-organisatorisch sicherzustellen, dass diese Stellen die Daten der Beitragsschuldner nur für Zwecke des Rundfunkbeitragseinzugs speichern,

verarbeiten und nutzen (§ 16 Abs. 3 S. 2 der Satzung des Hessischen Rundfunks über das Verfahren zur Leistung der Rundfunkbeiträge).

Insofern ist die ist die Datenverarbeitung der öffentlich-rechtlichen Rundfunkanstalten, die zum Zwecke des Einzuges des Rundfunkbeitrages erforderlich ist, zulässig und zur Gewährleistung ihrer verfassungsrechtlichen Finanzierungsgarantie auch notwendig. Die an meine Dienststelle diesbezüglich adressierten Beschwerden waren daher unbegründet.

9. Werbung und Adresshandel

Aufgrund des Wertes qualifizierter Adress- oder Profildaten kommt es immer wieder vor, dass Mitarbeiter, die das Unternehmen verlassen, solche wertvollen Daten mitnehmen und im Rahmen des neuen Arbeitsverhältnisses für Werbezwecke verwenden (Kap. 9.1). Vielfach brechen beim Online-Einkauf Interessenten, die bereits Waren in den Warenkorb gelegt haben, den Einkaufsvorgang ab. Diese mit Follow-Up-E-Mails doch noch zum Kauf der Waren zu verleiten, ist datenschutzrechtlich fragwürdig (Kap. 9.2). Das Recht zur Beschwerde nach Art. 77 DS-GVO dient dem individuellen Schutz der betroffenen Person, darf aber nicht zur Verfolgung sachfremder Ziele eingesetzt werden (s. Kap. 1.3 und Kap. 3.1). Vielfach wird es jedoch genutzt, um anderweitige Ziele ohne persönlichkeitsrechtlichen Bezug zu verfolgen oder sogar um die Aufsichtsbehörde davon abzuhalten, berechtigten Beschwerden nachzugehen (Kap. 9.3).

9.1
Keine Mitnahme von Kontaktdaten bei Wechsel des Arbeitgebers

Wenn Mitarbeiter eines Unternehmens den Arbeitsplatz wechseln und das Unternehmen verlassen, besteht immer auch das Risiko, dass wertvolle Daten aus dem Unternehmen mitgenommen werden. Die wechselnden Arbeitnehmer bleiben häufig in der gleichen Branche und finden ihren neuen Arbeitsplatz bei Mitbewerbern. Nicht alle Beschäftigten nehmen lediglich ihr erarbeitetes Knowhow und ihre Topfpflanzen mit, manche greifen leider auch auf Kundenkontakte des bisherigen Arbeitgebers zurück, lockt doch die Möglichkeit, unmittelbare Erfolge und lukrative Ergebnisse beim neuen Arbeitgeber zu erzielen, indem die mitgenommenen Kontaktdaten für die werbliche Kontaktaufnahme genutzt werden. Doch dürfen solche im letzten Arbeitsverhältnis entwendeten elektronischen Kontaktdaten zu werblichen Zwecken auch im Rahmen des neuen Arbeitsverhältnisses verarbeitet werden?

Innerhalb des Berichtszeitraums erreichten meine Behörde mehrere gleichlautende Beschwerden unterschiedlicher Betroffener bezüglich erhaltener Werbe-E-Mails. Diese wurden durch einen Mitarbeiter versandt, den die Betroffenen aus Kontakten mit einem Unternehmen aus der gleichen Branche in Rheinland-Pfalz kannten. Er warb nunmehr allerdings für einen den Betroffenen gänzlich unbekannten Anbieter.

Die Zulässigkeit von Werbe-E-Mails und der damit einhergehenden Verarbeitung von personenbezogenen Daten wird im Wesentlichen bestimmt

durch die Datenschutzgrundverordnung (DS-GVO) und das Gesetz gegen den unlauteren Wettbewerb (UWG).

Der Versand von Werbe-E-Mails ist unter datenschutzrechtlichen Aspekten zulässig, wenn der Betroffene hierzu eine ausdrückliche, informierte und freiwillige Einwilligung nach Art. 6 Abs. 1 UAbs. 1 Buchst. a und Art. 7 DS-GVO erteilt hat. 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 (bei Werbung insbesondere mit dem Wettbewerbsrecht). 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 Rechtsgrundlage für E-Mail-Werbung in Anspruch nehmen, da ein wirtschaftliches Interesse an ungesetzlicher Werbung nie als berechtigtes Interesse anerkannt werden kann.

In allen im Berichtszeitraum eingegangenen Beschwerden war kein vorheriges Bestandskundenverhältnis mit dem neuen Arbeitgeber des Versenders der Werbemails gegeben.

Eine freiwillige und informierte Einwilligung in die Verarbeitung der personenbezogenen Daten der Betroffen zu werblichen Zwecken liegt zwar vor, allerdings lediglich gegenüber dem ehemaligen Arbeitgeber. Eine Einwilligung wurde hier von den Betroffenen gegenüber einem spezifischen Unternehmen einer Wirtschaftsbranche und damit einem bestimmten datenschutzrechtlich Verantwortlichen erteilt. Es handelt sich nicht um eine Generalvollmacht an jedwedes Unternehmen der gleichen Branche.

Erwägungsgrund 32 der DS-GVO führt hierzu detailliert aus:

ErwGr. 32 DS-GVO

Die Einwilligung sollte durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist, etwa in Form einer schriftlichen Erklärung, die auch elektronisch erfolgen kann, oder einer mündlichen Erklärung.

Das verantwortliche Unternehmen mit Sitz in Hessen musste eingestehen, dass eine Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden kann. Da auch keine Einwilligung durch die Betroffenen nach Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO vorlag, löschte der Verantwortliche unmittelbar alle vom früheren Arbeitgeber des Mitarbeiters stammenden Daten. Darüber hinaus wurden unterschiedliche technische und organisatorische Maßnahmen getroffen, um sicherzustellen, dass ein solcher Datenschutzverstoß zukünftig ausgeschlossen werden kann. Vor allen Dingen veranlasste der Verantwortliche weitreichende datenschutzrechtliche Sensibilisierungs- und Schulungsmaßnahmen für die Belegschaft. Auf Grund der festgestellten begangenen Datenschutzverstöße wird die Einleitung eines Bußgeldverfahrens geprüft.

Festzuhalten ist, dass die Mitnahme von Daten, seien es Kunden- oder sonstige geschäftliche Daten, vom ehemaligen Arbeitgeber zum neuen Arbeitgeber nicht erlaubt ist. Hierbei ist es völlig gleichgültig, um welche Art von Daten es sich handelt und ob diese elektronisch oder in Papierform vorgelegen haben. Entscheidend ist lediglich, dass es sich um Daten handelt, die nur der alte Arbeitgeber verarbeiten darf und auf welche ein Beschäftigter selbst keinen Anspruch hat, außer für den Zweck der Durchführung seiner Arbeitstätigkeit für diesen bestimmten Arbeitgeber.

Allgemein muss gerade in Hinsicht auf Unternehmen festgehalten werden, dass das primäre Ziel eines Unternehmens sein muss, dass aus dem Verlust eines Mitarbeiters nicht noch ein Datenverlust wird und dass aus dem bisherigen Angestellten nicht plötzlich ein potenzielles Unternehmensrisiko wird.

Um eine ungewollte Datenmitnahme zu verhindern, ist eine bewusste Auseinandersetzung mit diesem Risiko im Unternehmen zwingend notwendig. Hierfür ist eine enge Zusammenarbeit zwischen dem Datenschutzbeauftragten und der IT-Abteilung zur Entwicklung geeigneter technischer und organisatorischer Maßnahmen sinnvoll. Diese technischen und organisatorischen Maßnahmen müssen sodann sicherstellen, dass Mitarbeiterinnen und Mitarbeiter, die das Unternehmen verlassen, keine Zugriffsberechtigungen und Rollen behalten, die es ihnen ermöglichen könnten, weiterhin auf Daten des Unternehmens zuzugreifen. Auch regelmäßige, präventive und vor allen Dingen verpflichtende Mitarbeiterschulungen können derartige Datenschutzverletzungen eindämmen.

Weiterhin ist es für Unternehmen ratsam, Vertraulichkeitsvereinbarungen mit ihren Mitarbeitenden zu treffen. In schriftlichen Verpflichtungserklärungen werden die Pflichten wie die Unterlassung unbefugter Nutzung, Bekanntgabe oder Verbreitung von Daten festgehalten. Diese Pflichten gelten zeitlich unbegrenzt, somit auch über das jeweilige Arbeitsverhältnis hinaus.

9.2
Werbe-E-Mails nach Abbruch von Warenkorbbestellungen

Niemand ist so wankelmütig wie ein Online-Käufer im WWW. Studien belegen, dass die Abbruchquote bei Onlinekäufen je nach Sparte zwischen 65 % bis knapp über 80 % liegt. Denn mit nur einem weiteren Klick werden dem potenziellen Online-Käufer unzählige weitere Angebote und Rabatte zur Auswahl gestellt. Selbstverständlich ist es für den betroffenen Online-Händler frustrierend, wenn potenzielle Kunden ihren Einkauf nur wenige Schritte vorm Check-Out abbrechen. Doch ist eine ausgeweitete E-Mail-Marketing-Strategie in Form von E-Mails an Warenkorbabbrecher (sogenannten Follow-Up-E-Mails) die ideale Lösung und ist es überhaupt datenschutzrechtlich konform?

Innerhalb des Berichtszeitraums erreichten mich mehrere Beschwerden gleichlautender Art, die unterschiedliche Webshops betroffen haben. Übereinstimmend berichteten die betroffenen Personen, dass sie sich innerhalb eines Webshops eine oder mehrere Waren ausgesucht, den Bestellvorgang gestartet und im Verlauf des Prozesses die Bestellung abgebrochen und den Webshop ohne den Abschluss eines Kaufvertrages wieder verlassen hatten. Nur wenige Stunden später erhielten alle Betroffenen eine E-Mail des jeweiligen verantwortlichen Shop-Betreibers mit einer Erinnerung zum nicht abgeschlossenen Kauf.

In allen im Berichtszeitraum eingegangenen Beschwerden war kein vorheriges Bestandskundenverhältnis gegeben und keiner der Betroffenen hatte dem jeweiligen Verantwortlichen eine freiwillige, ausdrückliche und informierte Einwilligung zur Verarbeitung der personenbezogenen Daten zu werblichen Zwecken nach Art. 6 Abs. 1 UAbs. 1 Buchst. a i. V. m. Art. 7 Abs.1 DS-GVO erteilt.

Die Besonderheit in diesen Fällen liegt darin, dass die Kunden zwar im Rahmen des begonnenen Bestellvorgangs ihre E-Mail-Adresse angegeben haben, es jedoch mangels Abschlusses des Vorgangs nicht zum tatsächlichen Kauf gekommen ist. Von daher sind alle weiteren Aktivitäten des verantwortlichen Shop-Betreibers nicht auf einen Kaufvertrag beziehbar.

Die versandte elektronische Erinnerung stellt somit Werbung dar und ist in der Regel nur mit einer ausdrücklichen Einwilligung im Sinne von Art. 6 Abs. 1 UAbs.1 Buchst. a DS-GVO i. V. m § 7 UWG zulässig.

Eine solche ausdrückliche, informierte und freiwillige Einwilligung kann allerdings durch betroffene Personen nicht erteilt worden sein, wenn ihre personenbezogenen Daten aus einer abgebrochenen Onlinebestellung abgeschöpft und im Anschluss zu werblichen Zwecken verarbeitet werden.

Datenschutzrechtlich muss die Einwilligungserklärung für die betroffene Person eindeutig als solche identifiziert werden können. Schon aus der Formulierung muss hervorgehen, dass die Person mit der Zustimmung in die Datenerhebung und -verarbeitung einwilligt. Für eine betroffene Person ist nicht absehbar, dass die alleinige Eingabe ihrer E-Mail-Adresse im Rahmen eines Online-Bestellvorgangs eine Einwilligung in die zukünftige Verarbeitung ihrer personenbezogenen Daten zu werblichen Zwecken darstellt.

Lediglich unter ganz strengen Voraussetzungen entsprechend des Ausnahmetatbestands des § 7 Abs. 3 UWG (Bestandskundenverhältnis) könnte eine solche Follow-Up-Werbe-E-Mail ohne vorherige explizit erteilte Einwilligung als zulässig erachtet werden.

Die Follow-Up-E-Mail stellt nur dann keine unzumutbare Belästigung dar, wenn die werbliche E-Mail an einen eingeloggten Kunden übermittelt wird, der zuvor bereits eine Registrierung im Shop abgeschlossen und eine Bestellung getätigt hat.

Auch in diesem Fall gibt es aber noch weitere Voraussetzungen dafür, dass der Kunde ohne ausdrückliche Einwilligung nach einem Warenkorbabbruch kontaktiert werden darf. Dazu zählen die folgenden:

– Die E-Mail-Adresse des Kunden darf für Direktwerbung nur für eigene ähnliche Waren oder Dienstleistungen genutzt werden.
– Der Kunde darf der Direktwerbung per E-Mail nicht ausdrücklich widersprochen haben.
– In der Warenkorbabbrecher-Mail muss auf die Möglichkeit zum Widerspruch gegen die Werbung hingewiesen werden. Im Idealfall sollte dazu direkt eine Möglichkeit zur Ausübung des Widerspruchsrechts bestehen. Das heißt, der Kunde sollte der Verwendung seiner E-Mail-Adresse per Klick auf einen Link in der Mail jederzeit widersprechen können.

In den von mir überprüften Fällen begründeten die Verantwortlichen die Rechtmäßigkeit ihrer Follow-Up-E-Mails in unterschiedlicher Weise, zum Beispiel:

– Follow-Up-E-Mails seien keine Werbung im eigentlichen Sinne.
– Ein Vertragsverhältnis sei bereits durch das Ausfüllen der Formularfelder angebahnt worden und somit läge ein Bestandskundenverhältnis bereits vor.

Die Argumentation, dass es sich bei der Follow-Up-E-Mail nicht um Werbung im eigentlichen Sinne handele, ist rechtlich nicht tragbar. Was unter den Begriff „Werbung“ fällt, wird von den Gerichten im Zusammenhang mit Direktmarketingmaßnahmen sehr weit verstanden. Werbung ist entsprechend Art. 2 Buchst. a EU-Richtlinie 2006/114/EG jede direkte oder indirekte Maß-

nahme, die der Förderung des Absatzes bzw. der Imagepflege des eigenen oder eines fremden Unternehmens dient.

Follow-Up-E-Mails verfolgen den eindeutigen Zweck der Umsatzsteigerung durch eine anschließende Beeinflussung des ausgewerteten Warenkorbs und sind demzufolge Werbung.

Auch die Behauptung, dass es sich hierbei um vorvertragliche Maßnahmen handele und sich die Verarbeitung der personenbezogenen Daten auf Art 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO stütze, ist rechtlich nicht haltbar. Nach Abbruch des Bestellvorgangs kann eine werbliche E-Mail vor dem Hintergrund des Schutzcharakters aus dem Wettbewerbsrecht grundsätzlich nicht mehr auf die Rechtsgrundlage der Durchführung vorvertraglicher Maßnahmen gestützt werden.

In allen im Berichtszeitraum aufgetretenen Fällen erfolgte eine Verwarnung nach Art. 58 Abs. 2 Buchst. b DS-GVO. Weitere Maßnahmen mussten nicht ergriffen werden, da die Verantwortlichen bereits im Rahmen des Verwaltungsverfahrens proaktiv alle personenbezogenen Daten, die durch Warenkorbabbrüche erhoben wurden, gelöscht hatten. Ebenfalls haben sie technische und organisatorische Maßnahmen getroffen, damit systemseitig sichergestellt ist, dass keine Verarbeitung zu werblichen Zwecken mehr erfolgen kann, ohne dass eine Einwilligung der betroffenen Person im System hinterlegt ist.

9.3
Die Beschwerde bei der Aufsichtsbehörde – ein Recht für betroffene Personen

Das im Datenschutzrecht fest verankerte Recht, sich bei der Aufsichtsbehörde über einen mutmaßlichen Datenschutzverstoß zu beschweren, dient vor allem dem individuellen Schutz der betroffenen Person. Auf das Beschwerderecht berufen kann sich daher nur, wer von einem möglichen Verstoß selbst betroffen ist. Nicht selten fehlt es bei Beschwerden aber an der Betroffenheit, teilweise wird das Beschwerderecht sogar mutwillig ausgenutzt, um anderweitige Ziele ohne persönlichkeitsrechtlichen Bezug zu verfolgen. Das Beschwerderecht dient aber nicht zur Verfolgung sachfremder Ziele (s. hierzu auch Kap. 1.3 und Kap. 3.1).

Mir wurden vom europäischen, vom Bundes- und Landesgesetzgeber in Art. 57 DS-GVO, § 40 Abs. 1, 6 BDSG und § 13 HDSIG sowie in diversen Spezialgesetzen (z. B. § 46 HPMG) eine Vielzahl von Aufgaben zugewiesen, um die Einhaltung des Datenschutzrechts zu überwachen und sicherzustel-

len. Diejenige Aufgabe, die im behördlichen Alltag zeitlich und personell den größten Umfang einnimmt, ist die Bearbeitung von Beschwerden.

Das Recht auf Beschwerde ist fest im deutschen Datenschutzrecht verankert und bildet einen Grundpfeiler der Tätigkeit der Datenschutzbehörden. In der DS-GVO wurde es noch verbindlicher als zuvor ausgestaltet und die Position der Beschwerdeführerinnen und Beschwerdeführer gestärkt. Seither sind mit einer Beschwerde verschiedene Rechte der Beschwerdeführenden und konkrete Pflichten der Aufsichtsbehörde verbunden.

Mir gehen jeden Monat mehrere Hundert schriftliche Beschwerden zu allen erdenklichen Lebenssachverhalten und Konstellationen zu, mit denen die Beschwerdeführenden mutmaßliche Datenschutzverstöße monieren. Meine Aufgabe nach Art. 57 Abs. 1 Buchst. f DS-GVO und § 13 Abs. 2 Nr. 6 HDSIG ist es, mich mit diesen Beschwerden zu befassen, den Gegenstand der Beschwerden in angemessenem Umfang zu untersuchen und die Beschwerdeführenden innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten. Den Beschwerdeführenden steht nach Art. 77 ff. DS-GVO u. a. das Recht zu, über den Stand und das Ergebnis der Beschwerde unterrichtet zu werden sowie gegen meine Entscheidung einen wirksamen gerichtlichen Rechtsbehelf einzulegen.

Neben der Beschwerde besteht auch die Möglichkeit, eine Aufsichtsbehörde informell zu kontaktieren und z. B. einen Hinweis auf einen möglichen Datenschutzverstoß zu geben. Ein solcher kann im Gegensatz zur Beschwerde auch anonym erfolgen (z. B. bei Whistleblowing oder bei einer persönlichen Verbindung zwischen Beteiligten) oder auch wenn der Hinweisgeber nicht selbst von der möglicherweise unzulässigen Datenverarbeitung betroffen ist. Ob und wie intensiv die Aufsichtsbehörde einem Hinweis oder einer Prüfungsanregung nachgeht, liegt in ihrem Ermessen und hängt vor allem von der Schwere des möglichen Verstoßes sowie dessen möglichen Auswirkungen ab. Somit können Hinweise faktisch die gleichen Folgen wie Beschwerden haben und zu ähnlichen Maßnahmen führen. Anders als Beschwerden lösen sie jedoch nicht die oben genannten Rechte der Beschwerdeführenden und Pflichten der Aufsichtsbehörde aus. Beispielsweise hat ein Hinweisgeber kein verbindliches Recht darauf, über den Verlauf und den Ausgang eines Verfahrens informiert zu werden, das die Aufsichtsbehörde aufgrund seiner Anregung eingeleitet hat.

Einzige Voraussetzung einer Beschwerde und damit zugleich Abgrenzungskriterium zu einem informellen Hinweis ist, dass der Beschwerdeführer oder die Beschwerdeführerin selbst von der in Frage stehenden Datenverarbeitung betroffen ist. Oftmals wird dies in Beschwerden ausdrücklich beschrieben oder geht aus dem geschilderten Sachverhalt eindeutig hervor. Wird in einer

Eingabe jedoch keine eigene Betroffenheit geltend gemacht und enthält sie auch keine nachvollziehbaren Hinweise auf eine eigene Betroffenheit des Absenders, handelt es sich nicht um eine Beschwerde. Dies gilt auch dann, wenn eine Eingabe anonym oder sogar unter bewusster Täuschung über die Identität des Absenders erfolgt. Entsprechende Eingaben werden als Hinweise behandelt.

In der Praxis ist die Beschwerde ein wichtiges Instrument, das nicht nur dem Schutz der betroffenen Personen dient, sondern mir auch ermöglicht, meine Aufgaben in einem thematisch möglichst breiten Spektrum in ganz Hessen wahrzunehmen. Meiner Behörde obliegt die Aufsicht über mehrere Hundert staatliche Stellen sowie über mehrere Zehntausend Unternehmen, Vereine, Verbände und andere Verantwortliche in Hessen. Präventives Vorgehen und umfassende Prüfungen können daher immer nur einen Teil der Verantwortlichen erreichen und sind nicht flächendeckend zu bewerkstelligen. Durch Beschwerden werde ich jedoch tagtäglich über kleinere und größere Verstöße gegen das Datenschutzrecht informiert und kann so Maßnahmen ergreifen, um diese zu untersuchen, deren Folgen abzumildern und zukünftige Verstöße zu verhindern. So werden regelmäßig auch systematische Missstände aufgedeckt, beseitigt und somit Verbesserungen beim Datenschutz erzielt.

Kehrseite des zum Schutz der Betroffenen großzügig ausgestalteten Beschwerderechts ist allerdings, dass bei mir auch viele „Beschwerden“ eingehen, deren Inhalt am Kern des Beschwerderechts oder sogar des Datenschutzrechts an sich vorbeigeht. Häufig sind dabei folgende Konstellationen:

1. Immer wieder gibt es „Beschwerden“, die keinerlei Bezug zum Datenschutzrecht aufweisen oder zumindest keine Hinweise auf einen datenschutzrechtlichen Verstoß enthalten. Vermutlich vor allem aus Unwissenheit über die Inhalte und die Ziele des Datenschutzrechts schreiben mich Menschen mit Anliegen an, die nicht datenschutzrechtlicher Natur sind. Teilweise bestehen auch Missverständnisse über die Reichweite des Datenschutzrechts oder die Befugnisse einer Aufsichtsbehörde. Solche Beschwerden sind offensichtlich unbegründet.
2. Häufig sind zudem Beschwerden, die zwar oberflächlich einen Bezug zum Datenschutzrecht aufweisen, hinter denen eigentlich aber erkennbar andere Ziele und Motive stehen. Oft ist dabei schon anhand der geschilderten Hintergründe oder der persönlichen oder rechtlichen Verhältnisse zwischen Beschwerdeführenden und Verantwortlichen erkennbar, dass nicht eine mögliche Beeinträchtigung des Persönlichkeitsrechts im Vordergrund steht. Stattdessen ist zumeist das Ziel, unliebsame Geschäftspartner, Wettbewerber, Nachbarn, Ex-Partner oder sonstige „Gegner“ zu schikanieren. Das weitreichende Beschwerderecht wird dabei ausgenutzt,

um die Aufsichtsbehörde zu instrumentalisieren, wegen zum Teil banaler Verfehlungen gegen diese Verantwortlichen vorzugehen. Teilweise stehen hinter solchen Beschwerden auch finanzielle (z. B. Forderung von Schadensersatz, Vorbereitung eines Rechtsstreits) oder politische Motive (z. B. Reichsbürgertum, fehlende Akzeptanz des öffentlich-rechtlichen Rundfunks (s. Kap. 8.3)).

Solches Vorgehen wird dadurch begünstigt, dass nahezu alle geschäftlichen Vorgänge mit der Verarbeitung von personenbezogenen Daten verbunden sind und das Datenschutzrecht somit bei sehr vielen alltäglichen Lebenssachverhalten eine Rolle spielt. Zudem ist z. B. auf Websites öffentlich und ohne nennenswerten Aufwand einsehbar, ob deren Betreiber Anforderungen z. B. an Datenschutzhinweise oder Cookie-Banner korrekt erfüllen oder nicht. Auch weil die Beschwerde bei der Aufsichtsbehörde im Gegensatz zur Einschaltung eines Rechtsanwalts oder einer Klage kein Kostenrisiko mit sich bringt, wird das Instrument gerne genutzt, um bei bereits bestehendem Streit einen „Nebenkriegsschauplatz" zu eröffnen.

3. Gelegentlich bedienen sich auch selbsternannte Datenschutzaktivisten der Beschwerde, um ihre vermeintlich hehren Ziele zu erreichen. So reichen einzelne Personen oder Personengruppen gezielt Beschwerden zu Themen ein, die sie selbst als besonders bedeutend wahrnehmen, mit dem Ziel, die Aufsichtsbehörde dazu zu bewegen, sich des jeweiligen Themas anzunehmen. Dazu werden teilweise bewusst mutmaßliche Verstöße provoziert und sogar Beschwerden unter verschiedenen Pseudonymen eingereicht, um die Aufsichtsbehörde über die Identität des Beschwerdeführers zu täuschen und so dem Vorwurf exzessiver Beschwerdetätigkeit zu entgehen. Trotz der aus Sicht dieser Beschwerdeführenden vermeintlich gut gemeinten und dem Datenschutz nützenden Motive binden solche Beschwerden personelle Kräfte in meiner Dienststelle, um subjektiv als wichtig empfundene Angelegenheiten zu bearbeiten, zu Lasten der Möglichkeit, objektiv sinnvolle und sachgerechte Schwerpunkte bei der Aufsichtstätigkeit setzen zu können.
4. Nicht zuletzt beruht ein gewisser Anteil des Beschwerdeaufkommens leider auch auf krankhaftem Querulantentum. So stehen einige wenige Personen hinter einer Vielzahl von Beschwerden, die oft unterschiedliche Lebensbereiche betreffen, als verbindendes Element aber lediglich die Beschwerde selbst und das Anstoßen immer neuer Streitigkeiten erkennen lassen. Neben den Verantwortlichen und meiner Behörde werden oftmals auch Gerichte oder der Petitionsausschuss des Landtages befasst, auf unliebsame Entscheidungen wird nicht selten mit aufwendigen, aber letztlich erfolglosen Dienst- und/oder Fachaufsichtsbeschwerden reagiert.

Die Bearbeitung von Beschwerden und Hinweisen aus diesen Fallgruppen bindet nicht unwesentliche zeitliche und personelle Ressourcen meiner Behörde. Dadurch wird es mir und meinen Mitarbeitern erschwert, der Aufsichtstätigkeit effizient und passgenau nachzugehen sowie die vielfältigen wesentlichen Aufgaben jenseits der Bearbeitung von Beschwerden zu erfüllen.

Allerdings haben die Aufsichtsbehörden bei der Untersuchung des Gegenstands von Beschwerden sowie bei der Entscheidung, welche Maßnahmen zur Beseitigung oder Ahndung von Verstößen zu treffen sind, Ermessensspielräume. Unter Abwägung aller Umstände des Einzelfalls ist eine angemessene behördliche Entscheidung zu treffen, die die Einhaltung des Datenschutzes sicherstellt und allen Beteiligten gegenüber verhältnismäßig ist. Im Rahmen des Ermessens ist auch der Hintergrund einer Beschwerde zu berücksichtigen und kann sich somit auf deren Bearbeitung auswirken. Bei Beschwerden, die erkennbar nicht dem Schutz der betroffenen Person oder der Beseitigung eines wesentlichen datenschutzrechtlichen Missstandes dienen, wäre es unverhältnismäßig, großen Ermittlungsaufwand zu betreiben oder weitreichende Maßnahmen zu ergreifen.

Damit Aufsichtsbehörden nicht durch exzessive oder missbräuchliche Beschwerdetätigkeit an der Erfüllung ihrer Aufgaben gehindert werden, wurde in Art. 57 Abs. 4 DS-GVO und für den HBDI in § 13 Abs. 10 HDSIG bestimmt, dass sie bei offensichtlich unbegründeten oder exzessiven Anfragen eine Missbrauchsgebühr erheben oder sich weigern können, im Einzelfall tätig zu werden. Diese Regelung kann beispielsweise relevant werden bei querulatorisch veranlagten Beschwerdeführern, bei vorsätzlicher Täuschung der Aufsichtsbehörde oder wenn das Beschwerderecht anderweitig mutwillig missbraucht wird, um mich für sachfremde Zwecke zu instrumentalisieren. Leider ist es gelegentlich nötig, als ultima ratio auch von dieser Möglichkeit Gebrauch zu machen.

Nur wenn eine Aufsichtsbehörde ihren gesetzlichen Aufgaben effizient nachgehen kann, kann sie die Einhaltung des Datenschutzrechts sicherstellen und Betroffene und Verantwortliche ausreichend unterstützen. Dabei gilt es, so weit wie möglich nach objektivem Maßstab die Rechte und Interessen aller Betroffenen zu wahren und nicht lediglich die teilweise überhöhten und unsachgemäßen Individualinteressen einzelner Beschwerdeführer.

10. Videoüberwachung

Viele Beschwerden betreffen die Videoüberwachung durch nicht öffentliche Stellen. Wegen der steigenden Komplexität der Videoüberwachungssysteme erfordern die aufsichtsbehördlichen Prüfverfahren oft eine – auch unangekündigte – Vor-Ort-Prüfung (Kap. 10.2). Zunehmend wird Videoüberwachung zur Kontrolle von Parkräumen durch private Unternehmen eingesetzt. Hiergegen erreichen mich viele Beschwerden. Diese haben teilweise Erfolg (Kap. 10.1).

10.1 Digitale Parkraumüberwachung

Ein häufiger Gegenstand an mich gerichteter Beschwerden ist die Überwachung von Parkräumen durch private Unternehmen. Bürgerinnen und Bürger fürchten, hierdurch signifikanten Eingriffen in ihre Persönlichkeitsrechte ausgesetzt zu sein, etwa einer langfristigen Speicherung von sie betreffenden Aufnahmen, oder weil sie – vielleicht sogar durch eine Künstliche Intelligenz – mit unberechtigten Zahlungsaufforderungen konfrontiert werden könnten. Mit einem bestimmten Parkraumüberwachungsunternehmen habe ich mich im Berichtszeitraum intensiv auseinandergesetzt.

Parkraumüberwachung durch private Unternehmen

Bei mir sind in den letzten Jahren vermehrt Beschwerden und Eingaben über verschiedene Parkraumüberwachungsunternehmen eingegangen. Diese betrafen u. a. die Zulässigkeit der Abfrage von Halterdaten beim Kraftfahrtbundesamt oder die allgemeine datenschutzrechtliche Bewertung dieser Systeme.

Dies ist dem Umstand geschuldet, dass immer mehr Besitzer von Stellplätzen private Parkraumüberwachungsunternehmen mit der Kontrolle der ordnungsgemäßen Nutzung ihrer Parkplätze beauftragen. Bei den von den privaten Parkraumüberwachungsunternehmen versandten Zahlungsaufforderungen handelt es sich nicht, wie vielfach angenommen, um Bußgelder, sondern um Vertragsstrafen. Bußgelder für „Falschparker“ werden ausschließlich von Behörden (z. B. den örtlichen Ordnungsämtern) verhängt, während die in den Beschwerden angesprochenen Zahlungsaufforderungen ausschließlich von privaten Unternehmen versandt werden.

Mit dem Abstellen des Fahrzeugs geht der Fahrzeugführer einen Vertrag ein, mit dem er die Allgemeinen Geschäfts- und Nutzungsbedingungen akzeptiert. Soweit diese auf Hinweisschildern auf dem Parkplatz ausreichend deutlich bekannt gegeben werden, werden sie Inhalt eines Parkraumnutzungsver-

trags, wenn das Auto auf dem Parkplatz stehen bleibt. Diese regeln auch die Zahlung von Vertragsstrafen bei entsprechender Missachtung.

Für den Eigentümer des Parkraums oder das von ihm beauftragte Unternehmen besteht die Möglichkeit, die KFZ-Halterdaten über die Zulassungsbehörden oder das Kraftfahrtbundesamt zu ermitteln. Gemäß § 31 StVG sind die Zulassungsbehörden als zuständige Registerbehörden verpflichtet, das örtliche Fahrzeugregister zu führen, und das Kraftfahrtbundesamt, das Zentrale Fahrzeugregister zu betreuen. Die Fahrzeugregister verfolgen nach § 32 StVG den Zweck, die im öffentlichen Straßenverkehr zugelassenen Fahrzeuge und deren Halter zu erfassen und diese Daten für verkehrsbezogene Angelegenheiten zur Verfügung zu stellen.

Gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO i. V. m. § 39 Abs. 1 StVG haben die Zulassungsbehörde oder das Kraftfahrtbundesamt demjenigen eine einfache Registerauskunft zu übermitteln, der unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Dabei reicht es aus, wenn der Rechtsanspruch auf Auskunft durch den Interessenten plausibel dargelegt wird (s. BT-Drs. 10/5343 vom 17. April 1986, S. 74). Sofern die Voraussetzungen des § 39 Abs. 1 StVG erfüllt sind, erhält der Anfragende von den Behörden eine einfache Registerauskunft über den Halter des benannten Fahrzeugs und somit auch dessen Kontaktdaten.

Parkraumüberwachung mittels Videoüberwachung

Vielfach wird zur Parkraumüberwachung Videoüberwachungstechnik eingesetzt. Eine technische Einrichtung bewertet die aufgezeichneten Parkvorgänge danach, ob diese vertragsgemäß oder vertragswidrig sind. In der Regel sind solche Parkvorgänge vertragsgemäß, die der Nutzung eines Angebots des Parkplatzbesitzers (z. B. dem Einkaufen in einem Geschäft) dienen. Mit einer Vertragsstrafe belegt werden sollen hingegen solche Parkvorgänge, die fremden Zwecken dienen, wie z. B. einem Spaziergang in der Umgebung oder der Nutzung eines Angebots eines Konkurrenten in anderer räumlicher Lage.

Daher müssen solche technischen Systeme zumindest in der Lage sein zu erkennen, ob sich eine Person von einem parkenden Fahrzeug zu dem Angebot des Parkplatzbesitzers bewegt. Zur Durchsetzung der Vertragsstrafe oder zur Ermittlung des Fahrzeughalters muss auch das Ablesen des Kennzeichens des Fahrzeugs möglich sein. Auch solche Schritte stellen bereits

Verarbeitungen personenbezogener Daten dar, die gemäß den Grundsätzen der DS-GVO auszugestalten sind.

Besonders im Fokus der zahlreichen Beschwerden stand das System eines Unternehmens, das sich von anderen durch die hohe Komplexität der Verarbeitungsvorgänge unterschied. Bei der umfangreichen Aufklärung der Sach- und Rechtslage kam es jedoch aus verschiedenen Gründen immer wieder zu Verzögerungen durch das Unternehmen und damit zu einem gesteigerten Ermittlungsaufwand. Da das Unternehmen nach mehreren Versuchen die Funktionsweise des Systems nicht nachvollziehbar erklärt hatte, habe ich dem Verantwortlichen meine Absicht mitgeteilt, seine Datenverarbeitung wegen Verstoßes gegen die Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) zu untersagen, und ihn dazu gemäß § 28 HVwVfG förmlich angehört.

Erst daraufhin hat der Verantwortliche die aktuelle Funktionsweise des Systems umfassend dargelegt. Diese entsprach nicht mehr der Funktionsweise, die uns durch die Beschwerden geschildert worden waren. Bei der folgenden umfassenden Prüfung stand die Frage im Vordergrund, in welchem Umfang welche Kategorien personenbezogener Daten bei der Parkraumüberwachung verarbeitet werden und wie technisch sichergestellt ist, dass die Datenschutzgrundsätze aus Art. 5 Abs. 1 DS-GVO dabei wirksam umgesetzt sind.

Nach eingehender Prüfung der von dem Unternehmen übermittelten Informationen zur aktuellen Ausgestaltung des Parkraumüberwachungssystems bin ich zu dem Schluss gekommen, dass dieses uns nun beschriebene System eine ausreichend wirksame Umsetzung der Datenschutzgrundsätze gewährleistet. Hierfür waren u. a. folgende Aspekte ausschlaggebend:

– Das System basiert auf der Erkennung beliebiger Personen, die geeignet sind, um die Kriterien zur Kategorisierung eines Parkvorgangs zu erfüllen. Dies können grundsätzlich alle Passagiere des Fahrzeugs sein, das System kann diese Personen nicht voneinander unterscheiden.
– Eine automatisierte Entscheidungsfindung im Sinne des Art. 22 DS-GVO findet nicht statt. Es erfolgt in jedem Fall eine menschliche Überprüfung von Parkvorgängen vor der Festsetzung einer Vertragsstrafe.
– Die Auswahl von Videosequenzen zur Bewertung von Parkvorgängen findet derart statt, dass insbesondere die Grundsätze der Datenminimierung und der Speicherbegrenzung gewährleistet sind. Eine dauerhafte Speicherung von Videomaterial erfolgt nicht.
– Durch die wirksame Markierung öffentlicher Flächen und das Weichzeichnen von nicht relevanten Objekten ist hinreichend sichergestellt, dass nicht-beteiligte Personen von der Verarbeitung ihrer personenbezogenen Daten nicht betroffen sind.

Durch die durchgehende Kommunikation und die erteilten Hinweise zur Rechtsauffassung im Prüfungsverfahren konnte ich erreichen, dass der Verantwortliche die Funktionsweise des Systems nachhaltig verändert und nunmehr prüfbar dargelegt hat. Auch sind etwaige datenschutzrechtliche Mängel beseitigt worden. Im Ergebnis konnte ich letztlich von einer Untersagung absehen. Aufgrund der mangelhaften Zusammenarbeit des Unternehmens mit meiner Behörde, die nicht durchgehend den Anforderungen des Art. 31 DS-GVO entsprochen und somit zu einer aufwändigen und längerdauernden Bearbeitung dieses Vorgangs beigetragen hat, habe ich jedoch ein Ordnungswidrigkeitenverfahren eingeleitet.

10.2
Videoüberwachung durch nicht öffentliche Stellen – Notwendigkeit von Vor-Ort-Prüfungen

Mich erreichen täglich Beschwerden zu vermeintlichen datenschutzrechtlichen Verstößen aufgrund des Einsatzes von Videoüberwachung durch nicht öffentliche Stellen. Diese erfordern ein aufsichtsbehördliches Prüfverfahren (s. zuletzt 52. Tätigkeitsbericht, Kap. 10; 51. Tätigkeitsbericht, Kap. 13; 50. Tätigkeitsbericht, Kap. 13), bei denen wegen der zunehmenden Komplexität der Videoüberwachung oftmals eine (ggf. unangekündigte) Vor-Ort-Prüfung durchzuführen ist. Beispiele aus den Berichtszeitraum betreffen zwei Prüfverfahren (bzgl. einer Arztpraxis sowie einer Bar).

Rechtlicher Hintergrund der Vor-Ort-Prüfung

Die DS-GVO räumt mir in Art. 58 DS-GVO umfangreiche Befugnisse ein. Für die Vor-Ort-Überprüfung einer Videoüberwachung sind vor allem folgende Untersuchungs- und Abhilfebefugnisse relevant:

Nach Art. 58 Abs. 1 Buchst. e DS-GVO kann ich vom Verantwortlichen Zugang zu allen personenbezogenen Daten und Informationen verlangen, die zur Durchführung des Prüfverfahrens notwendig sind. Für die Vor-Ort-Prüfung essenziell ist zudem Art. 58 Abs. 1 Buchst. f DS-GVO. Hiernach kann ich Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräten des Verantwortlichen verlangen. Auch nach § 40 Abs. 5 BDSG bin ich befugt, zur Erfüllung meiner Aufgaben Grundstücke und Geschäftsräume des Verantwortlichen zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten.

Sofern ich aufgrund meiner Untersuchung Verstöße feststelle, habe ich nach Art. 58 Abs. 2 Buchst. b DS-GVO die Befugnis, den Verantwortlichen zu verwarnen. Nach Art. 58 Abs. 2 Buchst. d DS-GVO kann ich den Verant-

wortlichen anweisen, die Videoüberwachung gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen. Gemäß Art. 58 Abs. 2 Buchst. f DS-GVO kann ich auch eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, verhängen. Sofern eine von mir nach Art. 58 Abs. 2 DS-GVO verhängte Maßnahme vom Verantwortlichen nicht oder nicht hinreichend erfüllt wird, kann ich diese im Wege der Zwangsvollstreckung durchsetzen. Möglich ist dann auch die Festsetzung eines Zwangsgeldes nach § 76 HessVwVG, das bis zu 50.000 Euro betragen kann.

Zusätzlich oder anstelle der genannten Maßnahmen kann ich gemäß Art. 58 Abs. 2 Buchst. i in Verbindung mit Art. 83 eine Geldbuße verhängen. Diese kann bis zu 20.000.000 Euro oder im Fall eines Unternehmens von bis zu vier Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs betragen, je nachdem, welcher der Beträge höher ist.

Art. 58 DS-GVO

(1) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse, die es ihr gestatten,

e) von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten,

f) gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Räumlichkeiten, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

(2) Jede Aufsichtsbehörde verfügt über sämtliche folgenden Abhilfebefugnisse, die es ihr gestatten,

b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen diese Verordnung verstoßen hat,

d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit dieser Verordnung zu bringen,

f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen,

i) eine Geldbuße gemäß Artikel 83 zu verhängen, zusätzlich zu oder anstelle von in diesem Absatz genannten Maßnahmen, je nach den Umständen des Einzelfalls, (…)

§ 40 BDSG

(5) Die von einer Aufsichtsbehörde mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen sind befugt, zur Erfüllung ihrer Aufgaben Grundstücke und Geschäftsräume der Stelle zu betreten und Zugang zu allen Datenverarbeitungsanlagen und -geräten zu erhalten. Die Stelle ist insoweit zur Duldung verpflichtet.

§ 76 HessVwVG

(1) Wird die Verpflichtung zu einer Handlung, die ein anderer als der Pflichtige nicht vornehmen kann (unvertretbare Handlung), oder zu einer Duldung oder Unterlassung nicht oder nicht vollständig erfüllt, so kann die Vollstreckungsbehörde den Pflichtigen zu der geforderten Handlung, Duldung oder Unterlassung durch Festsetzung eines Zwangsgeldes anhalten. Auch zu einer vertretbaren Handlung kann der Pflichtige durch Festsetzung eines Zwangsgeldes angehalten werden.

(2) Das Zwangsgeld beträgt mindestens 10 und höchstens 50.000 Euro.

Die Entscheidung über die Auswahl und Inanspruchnahme der Untersuchungs- und Abhilfebefugnisse liegt grundsätzlich in meinem Ermessen. Sie wird insbesondere von der Erfüllung der Mitwirkungspflicht der verantwortlichen Stelle gemäß Art. 31 DS-GVO sowie der Gesamtbeurteilung des Sachverhaltes aufgrund der vorliegenden Anhaltspunkte abhängig gemacht. Dies soll die folgende Berichterstattung verdeutlichen

Art. 31 DS-GVO

Der Verantwortliche und der Auftragsverarbeiter und gegebenenfalls deren Vertreter arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

Nicht mit der DS-GVO im Einklang stehende Videoüberwachung in einer Arztpraxis

Im Rahmen einer Beschwerde wurde der Vorwurf einer versteckten Kamera in der Wanduhr am Empfang einer Arztpraxis durch eine zwischenzeitlich ausgeschiedene Beschäftigte geäußert. Der Sachverhaltsdarstellung war zu entnehmen, dass es sich um eine Kamera mit Bild- und Tonaufzeichnungsmöglichkeit handelte, die in der Ziffer 10 der Uhr versteckt war und den Bereich des Empfangstresens der Arztpraxis aufzeichnete. Die Aufzeichnungen sollten auf eine in der Wanduhr befindlichen SD-Karte übertragen werden.

Die Gesamtbeurteilung des Sachverhaltes erforderte ein umgehendes Handeln. Neben datenschutzrechtlichen Verstößen bestand mit Blick auf die Tonaufzeichnungen die Gefahr der Verwirklichung von Straftatbeständen, insbesondere eine Verletzung der Vertraulichkeit des Wortes nach § 201 StGB. Die Beschwerdeführerin erstattete daher neben der Beschwerde bei meiner Behörde zugleich auch eine Strafanzeige bei dem örtlich zuständigen Polizeipräsidium.

§ 201 StGB

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. *das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder*
2. *eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.*

(2) Ebenso wird bestraft, wer unbefugt

1. *das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder*
2. *das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.*

Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

(3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter die Vertraulichkeit des Wortes verletzt (Absätze 1 und 2).

(4) Der Versuch ist strafbar.

(5) Die Tonträger und Abhörgeräte, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

Die Vor-Ort-Überprüfung wurde bereits am darauffolgenden Tag aufgrund des dringenden Verdachtes einer unzulässigen Videoüberwachung nach Rücksprache mit dem zuständigen polizeilichen Fachkommissariat durch zwei Beschäftigte meiner Behörde unangekündigt vollzogen.

Vor Ort konnte der Beschwerdegegner als Verantwortlicher der installierten Videoüberwachung angetroffen werden. Er war einsichtig und kooperativ. Den Einsatz der Wanduhr als Überwachungsapparat sowie die Aufzeichnungsfunktion bestätigte er. Die Wanduhr mit Ton- und Videoüberwachungsfunktionen war zum Zeitpunkt der Vor-Ort-Prüfung vom Verantwortlichen bereits entfernt worden. Eine Inaugenscheinnahme war somit nicht möglich. Zum Vorwurf der unzulässigen Videoüberwachung gab er an, dass er die Wanduhr angebracht habe, weil es Unklarheiten über die Rückgabe von Schlüsseln mit einer ausgeschiedenen Beschäftigten gegeben habe. Diese sei unter anderem noch im Besitz eines Kassenschlüssels gewesen. Die Kasse habe sich im Empfangsbereich befunden und sei daher für die ausgeschiedene Mitarbeiterin zugänglich gewesen. Der Beschwerdegegner befürchtete, dass sich seine ehemalige Beschäftigte gegebenenfalls Zutritt zur Praxis und zur Kasse verschaffen könnte. Er wollte die Wanduhr mit Ton- und Videoüberwachungsfunktion daher vorrangig zum Zwecke einer etwaig erforderlichen Beweissicherung nutzen.

Die Befürchtung trat nicht ein und die ausgeschiedene Beschäftigte händigte dem Beschwerdegegner im Einvernehmen die Schlüssel zeitnah aus. Weiterhin gab der Beschwerdegegner an, dass das Abhängen der Wanduhr seither vergessen worden sei. Erst aufgrund des Vorfalls mit der Beschwerdeführerin sei die mit der Kamera ausgestattete Wanduhr wieder in Erinnerung geraten. Aufgrund der Hinweise der Beschwerdeführerin tauschte der Beschwerdegegner die bisherige Wanduhr zeitnah gegen eine übliche Wanduhr aus.

Vor Ort konnten die vorhandene Aufzeichnung sowie die gefertigte Tonaufzeichnung gesichtet werden. Hierbei handelte es sich um eine Videosequenz von wenigen Minuten. Der Beschwerdegegner gab hierzu an, dass die Bild- und Tonaufzeichnung – vermutlich aufgrund eines Bedienfehlers – insgesamt nur für wenige Minuten nach Inbetriebnahme erfolgt sei.

Zusammengefasst konnte festgestellt werden, dass die Wanduhr als mögliches Überwachungsinstrument etwa ein halbes Jahr installiert war und eine Überwachung und Speicherung von Bild- und Tonaufzeichnungen des Empfangs der Praxis durch den Verantwortlichen zumindest kurzfristig erfolgte und zeitweise beabsichtigt war. Die damaligen Beschäftigten wurden über den Einsatz der Wanduhr informiert. Dies wurde mir durch eine schriftliche Erklärung der Beschäftigten im Nachgang bestätigt. Die Beschwerdeführerin war eine neue Beschäftigte der Praxis. Sie wurde über die Wanduhr als mögliches Überwachungsgerät nicht informiert. Auch erfolgte keine Beschilderung zu dem Einsatz einer Videoüberwachung, so dass die Video- und Tonüberwachung auch für Patientinnen und Patienten nicht erkennbar war. Die Videoüberwachung erfolgte somit nicht nur ohne erkennbare Rechtsgrundlage, sondern auch unter Verstoß gegen die Informationspflichten nach den Vorgaben der Art. 12 bis 14 DS-GVO.

Im weiteren Verlauf der Vor-Ort-Prüfung wurde dem Beschwerdegegner eine ergänzende schriftliche Anhörung ausgehändigt. Dieser war ein Fragebogen zur Videoüberwachung beigefügt. Zudem wurde der Beschwerdegegner auf die mögliche Verwirklichung des Straftatbestandes der Verletzung der Vertraulichkeit des Wortes hingewiesen. Mein Tätigwerden wurde aufgrund der parallelen Strafanzeige durch die anschließende Dokumentation vorerst beendet.

Schließlich erfolgte in Zusammenarbeit mit der Polizei die Übersendung der gefertigten Akte mitsamt der vorliegenden Strafanzeige zuständigkeitshalber an die Staatsanwaltschaft zur Entscheidung über das weitere Verfahren. Dieses Vorgehen wird durch § 21 Abs. 1 OWiG begründet.

§ 21 OWiG

(1) Ist eine Handlung gleichzeitig Straftat und Ordnungswidrigkeit, so wird nur das Strafgesetz angewendet. Auf die in dem anderen Gesetz angedrohten Nebenfolgen kann erkannt werden.

(2) Im Falle des Absatzes 1 kann die Handlung jedoch als Ordnungswidrigkeit geahndet werden, wenn eine Strafe nicht verhängt wird.

Demnach ist bei Handlungen, die gleichzeitig eine Straftat und Ordnungswidrigkeit sind, zunächst das Strafgesetz anzuwenden und von den Strafermittlungsbehörden zu verfolgen. Im vorliegenden Fall stand eine Straftat im Raum, weshalb hier die Tätigkeit der Staatsanwaltschaft vorgeht. Wenn eine Strafe nicht verhängt wird, kann die Handlung jedoch gemäß § 21 Abs. 2 OWiG als Ordnungswidrigkeit geahndet werden, was meine weitere Zuständigkeit begründen kann.

Vor-Ort-Überprüfung in einer Bar – Ausbleibende Mitwirkung

Im Rahmen einer weiteren Beschwerde wurde mir mitgeteilt, dass in einer Bar in einer großen hessischen Stadt eine Videoüberwachung mit diversen Kameras innerhalb der Bar und im Aufenthaltsraum der Beschäftigten betrieben würde. Im Rahmen der Anhörung des Beschwerdegegners bestätigte sich der geäußerte Verdacht. Zudem stellte ich fest, dass die Speicherdauer zu lange erfolgte und keine ausreichende Hinweisbeschilderung vorhanden war.

Aufgrund des nach der Anhörung feststehenden Sachverhaltes erließ ich – hier zunächst ohne Vor-Ort-Prüfung – eine Maßnahme nach Art. 58 Abs. 2 Buchst. d DS-GVO, um die Videoüberwachung hinsichtlich der Speicherdauer und der Hinweisbeschilderung in Einklang mit der DS-GVO zu bringen. Der Beschwerdegegner reagierte mehrfach nicht, weshalb nach mehrfacher Androhung schließlich die angedrohten Zwangsgelder gemäß § 76 HessVwVG verhängt wurden.

Infolge der völlig fehlenden Reaktionen des Beschwerdegegners hinsichtlich der vollstreckten Maßnahmen führte ich sodann eine unangekündigte Vor-Ort-Prüfung unter polizeilicher Begleitung durch. Hierbei äußerte der Beschwerdegegner, dass ihm die zu erfüllenden Maßnahmen trotz mehrfacher erfolgreicher Zustellung an die private Postanschrift nicht bekannt seien. Es fand eine Inaugenscheinnahme der festinstallierten Kameras statt. Die Verstöße in Form der Nichteinhaltung der zulässigen Speicherdauer sowie der hinreichenden Beschilderung bestanden fort. Dem Beschwerdegegner wurde der Bescheid mit dem Inhalt, die Videoüberwachung bis zur nachweislichen Maßnahmenumsetzung auszuschalten, persönlich ausgehändigt. Das Zwangsvollstreckungsverfahren ist derzeit noch nicht abgeschlossen.

Fazit & Empfehlung

Die beiden dargestellten Prüfverfahren verdeutlichen die möglichen Folgen einer fehlenden oder falschen Anwendung der Rechtsgrundlagen der Videoüberwachung. Sie zeigen zugleich die Notwendigkeit meiner Befugnisse, insbesondere auch derjenigen zur (ggf. unangekündigten) Vor-Ort-Prüfung, bei der Videoüberwachung. Um unangenehme Situationen wie die aus der Praxis beschriebenen Vorfälle zu vermeiden, empfiehlt es sich, vorab umfassend über die datenschutzrechtlichen Anforderungen der Videoüberwachung zu informieren. Die DSK hat hierzu eine ausführliche Orientierungshilfe bereitgestellt, die die Anforderungen an eine datenschutzkonforme Videoüberwachung durch nicht öffentliche Stellen darlegt: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf. Weiterhin hat der EDSA Leitlinien zum datenschutzkonformen Einsatz von Videoüberwachung beschlossen und veröffentlicht: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_de.pdf.

11. Wirtschaft

Im Bereich der Wirtschaft war im Berichtszeitraum für mich die deutschlandweit geltende datenschutzrechtliche Genehmigung der neuen Verhaltensregeln für die Prüf- und Speicherfristen von rechtmäßig gespeicherten personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien von besonderer Bedeutung (Kap. 11.1). Wichtig ist auch, dass die datenschutzrechtliche Rolle von Inkassounternehmen geklärt werden konnte. In aller Regel ist davon auszugehen, dass sie Verantwortliche im Sinne des Art. 4 Nr. 7. DS-GVO und nur im Ausnahmefall Auftragsverarbeiter sind (Kap. 11.2). Interessante Beschwerdeverfahren haben zur Klärung geführt, ob die Deutsche Bahn für Sparpreistickets Daten erheben darf, die für die Nutzung der Bahn als Mittel der Mobilität nicht erforderlich sind (Kap. 11.3), wann eine Trennungs- und Scheidungsfolgenvereinbarung für die Bonitätsprüfung durch ein Kreditinstitut geschwärzt werden müssen (Kap. 11.4) und wann in Hotels Ausweiskopien angefertigt werden dürfen (Kap. 11.5).

11.1
Neue Verhaltensregeln für Auskunfteien

Die ersten Monate des Berichtsjahres waren geprägt durch die Verhandlungen mit dem Verband „Die Wirtschaftsauskunfteien" über dessen neue Verhaltensregeln. Mit diesen sollten neue Regelungen für spezifische Datenverarbeitungen durch seine Verbandsmitglieder geschaffen werden. Diese Verhaltensregeln konnte ich am 24. Mai 2024 gemäß Art. 40 Abs. 5 DS-GVO genehmigen. Sie entsprechen nun besser den Vorgaben der DS-GVO (s. hierzu auch Kap. 1.6).

Der Verband „Die Wirtschaftsauskunfteien" musste seine bisherigen Verhaltensregeln vom 25. Mai 2018 nach sechs Jahren überarbeiten, weil ich sie als zuständige Aufsichtsbehörde am 23. Oktober 2023 beanstandet hatte. Die Überarbeitung fand in mehreren Runden statt, weil über die immer weiter fortgeschrittenen Entwürfe verhandelt werden musste, ob sie die Bedingungen für eine datenschutzrechtliche Genehmigung erfüllten. An den Verhandlungen von Januar bis Mai 2024 nahmen neben mir auch die Aufsichtsbehörden aus Baden-Württemberg, Bayern und Nordrhein-Westfalen teil.

Gemäß Erwägungsgrund 99 DS-GVO wurden im Rahmen einer Verbändeanhörung der Bundesverband Deutscher Inkasso-Unternehmen (BDIU), der Bundesverband E-Commerce und Versandhandel Deutschland e. V. (bevh), der Verband „Die Deutsche Kreditwirtschaft" (DK), die Verbraucherzentrale Bundesverband (vzbv), die Bundesarbeitsgemeinschaft Schuldnerberatung

e. V. (BAG-SB) sowie die Deutsche Industrie- und Handelskammer (DIHK) gebeten, zu dem Entwurf der Verhaltensregeln Stellung zu nehmen. Lediglich die DIHK hat keine Stellungnahme abgegeben. Während die BAG-SB sowie der vzbv Änderungsvorschläge übermittelt haben, äußerten sich die übrigen Stellungnahmen der Verbände dem Entwurf der Verhaltensregeln gegenüber im Wesentlichen befürwortend.

Vor seiner Genehmigung informierte ich auch die DSK über das erzielte Ergebnis. Deren Mitglieder, die den nichtöffentlichen Bereich beaufsichtigen, stimmten am 14. Mai 2024 meiner Absicht, die Verhaltensregeln zu genehmigen, einstimmig zu.

Die neuen Verhaltensregeln betreffen nur die Prüf- und Speicherfristen von rechtmäßig gespeicherten personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien. Sie ersetzen nicht die Regelungen der DS-GVO, sondern konkretisieren die aus ihnen abzuleitenden speziellen Anforderungen an die Auskunfteien für den Teilbereich der Prüf- und Speicherfristen von personenbezogenen Daten. Sie präzisieren insbesondere die abstrakten Vorgaben des Art. 5 Abs. 1 Buchst. e DS-GVO und erfüllen die Verpflichtung des jeweiligen Verantwortlichen, gemäß Erwägungsgrund 39 DS-GVO entsprechende Fristen festzulegen. Sie stellen sicher, dass rechtmäßig gespeicherte personenbezogene Daten nicht länger als nötig gespeichert werden, indem sie branchenweit einheitliche und auf bestimmte Verarbeitungsvorgänge und Datenkategorien bezogene Speicher- und Prüffristen bestimmen. Diese Fristen sind für die Kreditwürdigkeitsprüfung erforderlich und entsprechen in ihrer Verkürzung, in der Beschränkung hinsichtlich der erfassten Daten und hinsichtlich der begrenzten Zwecke gegenüber den bisherigen Verhaltensregeln einer vertretbaren Abwägung der sich widersprechenden Interessen.

Im Vergleich mit den alten Verhaltensregeln führen die neuen zu vielen Verbesserungen für den Datenschutz. Sie enthalten keine Speicherregelungen mehr zu den von der DSK kritisierten Positivdaten und zu Kontomissbrauchsdaten (s. DSK, Beschluss vom 22. September 2022 „Verarbeitung von Positivdaten von Privatpersonen aus Verträgen über Mobilfunkdienste und Dauerhandelskonten durch Auskunfteien“, https://www.datenschutzkonferenz-online.de/media/dskb/20210929_top_07_beschluss_positivdaten.pdf). Sie schränken die Speicherung von Vertragsdaten auf Vertragsverhältnisse nach dem Kreditwesengesetz ein – z. B. auf Informationen über störungsfreie Verträge zu Girokonten und Kreditkarten. Die Verhaltensregeln präzisieren die geregelten Speicherungen durch Definitionen in einem Glossar und durch die Bezugnahme auf Rechtsvorschriften. Dadurch konkretisieren sie die Zweckbestimmung und Zweckbindung der Speicherungen. So werden z. B. Anschriftendaten und Geldwäschedaten nicht für das Kredit-Scoring

gespeichert. Sie präzisieren die Speicherfristen hinsichtlich Beginn und Ende und legen für Anschriftendaten ein Fristenende fest. Schließlich verkürzen sie die Fristen für nachträglich beglichene Forderungen für alle Insolvenzdaten sowie für Daten über die Restschuldbefreiung und über die ihr zugrundeliegenden Forderungen.

Die Verhaltensregeln enthalten keine Regelungen zu der Frage, ob die Speicherung bestimmter Daten berechtigt ist. Auch lassen sie sowohl die Rechte betroffener Personen als auch die Befugnisse der Aufsichtsbehörden unberührt. Für diese Themen gilt die DS-GVO unmittelbar.

Die Genehmigung der Verhaltensregeln ordnete an, dass zwei Verpflichtungen der Auskunfteien erst ab dem 1. Oktober 2024 und eine Verpflichtung ab dem 1. Januar 2025 galten. Diese drei neuen Verpflichtungen schränken die Speicher- und Prüffristen, die Zwecke der Datenspeicherung sowie ihren Anwendungs- oder Gegenstandsbereich ein. Um sie umzusetzen, mussten die Auskunfteien umfangreiche technisch-organisatorische Anpassungen vornehmen, die entsprechende Zeit in Anspruch nahmen. Um für diesen Zeitraum eine Rechtsunsicherheit zu vermeiden, galten die einschlägigen Regelungen der bisherigen Verhaltensregeln bis zum jeweiligen Geltungsbeginn der neuen Regelungen fort.

Mit der Umsetzung dieser Verpflichtungen konnte für die betroffenen Personen spürbare Erleichterungen erzielt werden. Bei der Schufa Holding AG wurden zum 1. Januar 2025 für ca. 120.000 der Auskunftei übermittelte, aber kurz darauf ausgeglichene Forderungen die Speicherfristen verkürzt. Eine Speicherung dieser Forderungen erfolgt dann nur noch für 18 Monate statt wie bisher für 36 Monate. Etwa 56.000 derartige Forderungen wurden zudem direkt gelöscht, da sie bereits mindestens 18 Monate bei der Schufa Holding AG gespeichert waren.

11.2
Inkassounternehmen: Auftragsverarbeiter oder Verantwortliche?

Die Qualifizierung eines Inkassounternehmens als eigener Verantwortlicher (Art. 4 Nr. 7 DS-GVO) oder als Auftragsverarbeiter (Art. 4 Nr. 8 DS-GVO) ist gesetzlich nicht geregelt. Der Abschluss eines Auftragsverarbeitungsvertrages im Sinne des Art. 28 DS-GVO ist vielmehr eine Frage des Einzelfalles. Maßgebend ist eine Untersuchung des konkreten Vertragsverhältnisses. Je enger der vorgegebene Rahmen des Forderungsmanagements ist, desto eher wäre eine Auftragsverarbeitung anzunehmen. In aller Regel ist zunächst jedoch davon auszugehen, dass es sich bei einem Inkassounternehmen um einen eigenen Verantwortlichen im Sinne des Art. 4 Nr. 7. DS-GVO handelt.

Beschwerdeverfahren

In dem zu beurteilenden Fall hatte ein Inkassounternehmen zu einer betroffenen Person Forderungsdaten an die SCHUFA Holding AG (folgend: SCHUFA) übermittelt. Hiergegen richtete sich die bei mir eingereichte Beschwerde der betroffenen Person. Sie begehrte von mir, gegenüber der SCHUFA eine Löschung der Forderungsdaten aus dem dort zu ihrer Person geführten Datensatz anzuordnen. Diese Forderung lehnte ich ab. Gegen den entsprechenden Bescheid klagte die betroffene Person vor dem Verwaltungsgericht Wiesbaden (VG Wiesbaden).

Gerichtsverfahren

Das VG Wiesbaden, 6. Kammer, gab der Klage statt, hob meinen ablehnenden Bescheid auf und verpflichtete mich mit Urteil vom 27. September 2021, 6 K 549/21.WI, die SCHUFA zu verpflichten, die streitgegenständlichen Forderungsdaten zu löschen.

Im Rahmen der Prüfung, ob das Inkassounternehmens (Beigeladene zu 2.) die Forderungsdaten an die SCHUFA (Beigeladene zu 1.) übermitteln durfte, stufte das VG Wiesbaden das übermittelnde Inkassounternehmen dem Grunde nach als Auftragsverarbeiter ein und formulierte

> „(…) bereits erhebliche Zweifel daran, dass Rechtsdienstleister im Rahmen von Inkassodienstleistungen Einmeldungen an die Beigeladene zu 1. ohne gesonderte Beauftragung durch ihren Auftraggeber vornehmen dürfen. (…) Dass eine Beauftragung der Beigeladenen zu 2. über die reine Rechtsdienstleistung hinaus erfolgt ist, wurde nicht kundgetan. (…)“

Dieses Urteil des VG Wiesbaden erlangte keine Rechtskraft. Vielmehr wurde es im Berufungserfahren vom 10. Senat des Hessischen Verwaltungsgerichtshofs (Hess. VGH) mit Beschluss vom 29. September 2022, 10 A 2358/21.Z, für unwirksam erklärt. Dieser Beschluss wurde jedoch nicht veröffentlicht.

Das VG Wiesbaden hatte sein Urteil noch vor Ablauf der Rechtsmittelfrist veröffentlicht (bspw. bei openJur 2021, 44721). Dies hatte zur Folge, dass sich Beschwerdeführende und ihre Rechtsvertretungen in Beschwerdeverfahren und in einem weiteren Gerichtsverfahren auf dieses veröffentlichte Urteil beriefen. Der genannte Beschluss des Hess. VGH war der Öffentlichkeit mangels Veröffentlichung bislang unbekannt.

Anlässlich einer weiteren Klage befasste sich das VG Wiesbaden – unter anderer Besetzung der 6. Kammer – daher erneut mit der Frage, ob es sich bei einem Inkassounternehmen um einen Auftragsverarbeiter oder einen eigenen Verantwortlichen handelt.

Zu dieser Frage führte das VG Wiesbaden mit bislang ebenfalls unveröffentlichtem Beschluss vom 18. März 2024, 6 K 1425/22.WI, nunmehr wie folgt aus:

„(…) In jedem Falle beruht die Auffassung des Klägers auf einer von Literatur und Rechtsprechung eher abgelehnten Auffassung zum Status von Inkassounternehmen im Wirtschaftsleben.

Überwiegend wird die Auffassung vertreten, dass Inkassounternehmen eigene Verantwortliche seien, da sie regelmäßig die Zwecke und Mittel der Datenverarbeitung weitgehend selbst bestimmen und nur ausnahmsweise, beispielsweise bei der teilweisen weisungsgebundenen Übertragung des Forderungsmanagements, auch Auftragsverarbeitungen i. S. d. Art. 28 DSGVO denkbar seien (Eßer in Eßer/Kramer/von Lewinski (Hrsg.), DSGVO/BDSG Nebengesetze, Kommentar, 8. Auflage 2024, Art. 4 Rn. 83). Gegen eine Einordnung der Auftragsverarbeitung spricht jedoch, dass oftmals auch diese Konstellationen des Inkassos durch eine weitgehend selbstständige Aufgabenwahrnehmung des Inkassounternehmens geprägt sind, die deren Einordnung als Verantwortliche nahelegen (Buchner/Petri in Kühling/Buchner, DS-GVO BDSG, Kommentar, 4. Auflage 2024, Art. 6 DS-GVO Rn. 51a).

Aus der sog. teilweisen weisungsabhängigen „Einziehungsermächtigung“, bei der der Auftraggeber rechtlicher Eigentümer der Forderung bleibt, folgt keine andere Bewertung. Wie der Beklagte zu Recht ausführt, unterscheidet das Rechtsdienstleistungsgesetz (RDG) nicht zwischen der Einziehung fremder oder zum Zwecke der Einziehung auf fremde Rechnung abgetretener Forderungen (§ 2 Abs. 2 RDG). Die rechtliche Inhaberschaft einer Forderung bleibt auf die Zulässigkeit der Rechtsdienstleistung ohne Einfluss, wie auch die Ausführung der Inkassotätigkeit vom Status der Forderung nicht abhängt.

Gegen eine Einordnung als Auftragsverarbeiter sprechen der nur graduelle Unterschied zu Rechtsanwälten im erforderlichen Know-how und Professionalisierungsgrad, die häufig völlige Freiheit bei der Wahl der Mittel zur Umsetzung, die sehr weitgehende Freiheit bei der Bestimmung des Zwecks bzw. die erheblichen Eigeninteressen an dieser Dienstleistung, die ebenfalls eine Einordnung als Verantwortlichen nahelegen (Hartung in Kühling/Buchner, DS-GVO BDSG, Kommentar, 4. Auflage 2024, Art. 28 DSGVO Rn. 50 a).

Bei externem Inkassomanagement steht der Einordnung einer Auftragsverarbeitung regelmäßig entgegen, dass eine vollständige Bestimmung über die Mittel der Verarbeitung durch die Verantwortlichen nicht mehr gewährleistet sein dürfte (Ingolf in Sydow/Marsch, DS-GVO BDSG Handkommentar, 3. Auflage 2022, Art. 28 DSGVO Rn. 22).

Nach Auffassung des VG Mainz scheidet eine Auftragsverarbeitung bei der Übermittlung von Daten im Rahmen einer Forderungsabtretung eines Tierarztes an ein Inkassobüro mangels Weisungsgebundenheit aus, weil die Abtretung auf einer freien Entscheidung des Zessionars beruht und der Zedent keinen Einfluss auf die nach seinem Vorstellungsbild gewünschte mit der Abtretung einhergehende datenschutzrechtliche Veränderung hat (VG Mainz, Urteil vom 20.02.2020, 1 K 467/19.MZ, juris, Rn. 22 ff.).

Auch wenn die Unabhängigkeit des Inkassodienstleisters nicht gesetzlich verpflichtend vorgegeben wird und somit nicht bereits deswegen die Zwecke der Verarbeitung in die Sphäre des Inkassounternehmens verlagert werden, bestimmt das

> Inkassounternehmen doch faktisch die Zwecke und Mittel der Datenverarbeitung derart autonom, dass es datenschutzrechtlich als der für die Datenverarbeitung personenbezogener Daten Verantwortliche erscheint. In aller Regel ist daher auch das Inkassounternehmen im Mandatsverhältnis für die Verarbeitung personenbezogener Daten Verantwortlicher und nicht Auftragsverarbeiter (Ziegenhorn/Fokken, Rechtsdienstleister: Verantwortliche oder Auftragsverarbeiter? in ZD 2019, 194 [199]).
>
> Soweit sich aus dem Urteil der Kammer – in anderer Besetzung – vom 27.09.2021 – 6 K 549/21.WI, juris, etwas anderes ergibt, wird daran nicht festgehalten. Das Urteil ist zudem nicht rechtskräftig geworden. (…)“

Im Ergebnis teilt die 6. Kammer des VG Wiesbaden nunmehr auch die bislang von mir vertretene Auffassung, dass es sich bei einem Inkassounternehmen in aller Regel um einen eigenen Verantwortlichen im Sinne des Art. 4 Nr. 7. DS-GVO handelt.

Die DSK äußerte sich im Rahmen des Kurzpapiers Nr. 13 (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf) diesbezüglich wie folgt:

> „(…) Keine Auftragsverarbeitung, sondern die Inanspruchnahme fremder Fachleistungen bei einem eigenständig Verantwortlichen, für die bei der Verarbeitung (einschließlich Übermittlung) personenbezogener Daten eine Rechtsgrundlage gemäß Art. 6 DS-GVO gegeben sein muss, sind beispielsweise in der Regel die Einbeziehung eines·(…) Inkassobüros mit Forderungsübertragung. (…)“

11.3
Prüfung digitaler Zugangshürden

Das spezifische Thema für das Jahr meines Vorsitzes in der DSK (s. Kap. 1.1) hatte als praktisches Vollzugsproblem mehrere Beschwerden gegen die Deutsche Bahn. Die Beschwerden konnten am Ende durch das kooperative Verhalten der Deutschen Bahn beseitigt werden.

Mehrere Beschwerden beklagten, dass Sparpreistickets für die Deutsche Bahn nur noch als digitale Tickets erworben werden können. Um diese zu übertragen, verlangte die Deutsche Bahn die Angabe eines E-Mail-Kontos oder die Nummer eines Smartphones. Wer keinen Internetanschluss oder kein E-Mail-Konto oder kein Smartphone hatte, konnte kein Sparpreisticket erwerben und war darauf angewiesen, Normaltickets zu einem erheblich höheren Preis zu erwerben, wenn er mit der Deutschen Bahn fahren wollte.

Dies ist nur ein Beispiel für die zunehmende Tendenz, Leistungen, die weiterhin erbracht werden wie bisher, von einer digitalen Anmeldung, Terminvereinbarung, Buchung oder Bezahlung oder einem digitalen Antrag oder Ticket abhängig zu machen. Unternehmen und Behörden erlangen dadurch personenbezogene Daten, die sie bisher nicht hatten, und können diese fürviele weitere Zwecke nutzen. Der damit verbundene Eingriff in Grundrechte auf Datenschutz und informationelle Selbstbestimmung wird in vielen Fallgruppen noch dadurch intensiviert, dass Dritte, auch in unsicheren Drittstaaten, für die Betroffenen teilweise nicht erkennbar in die Datenverarbeitung einbezogen und ihnen Daten preisgegeben werden (s. zum Folgenden ausführlich Roßnagel, Kein Zwang zur Preisgabe personenbezogener Daten, Zeitschrift für Datenschutz (ZD) 2025, Heft 4, 184ff.).

Diese Bedingung wird zum Zwang, wenn jemand vor die Alternative gestellt wird, seine Daten preiszugeben oder auf eine Leistung zu verzichten, die im wirtschaftlichen, sozialen und kulturellen Bereich für die Existenz, die freie Entfaltung der Persönlichkeit oder die Teilhabe am gesellschaftlichen Leben notwendig ist. Mit digitalen Zugangshürden werden in Deutschland Millionen von Menschen aus der Inanspruchnahme von (Infrastruktur-)Leistungen der Daseinsvorsorge ausgeschlossen, die diese Voraussetzungen nicht erfüllen wollen oder können.

Ob Unternehmen und Behörden ihre Geschäfts- oder Verwaltungsprozesse digitalisieren, ist keine Frage des Datenschutzes. Bei der Digitalisierung dieser Prozesse müssen sie aber den für sie geltenden Rahmen des Datenschutzrechts beachten.

Die Verarbeitung personenbezogener Daten im Rahmen von digitalen Zugangshürden kann nicht auf eine Einwilligung gestützt werden, wenn diese für die betroffenen Personen aufgrund einer Zwangssituation nicht freiwillig ist. Die Zulässigkeit der Datenverarbeitung fehlt auch dann, wenn sie für die Erfüllung des Hauptgegenstandes eines Vertrags, zur Wahrung berechtigter Interessen oder zum Erbringen einer Verwaltungsleistung nicht unbedingt erforderlich ist.

Bei der Digitalisierung ihrer Prozesse müssen Unternehmen und Behörden ihre Datenverarbeitungssysteme nach Art. 25 Abs. 1 und 2 DS-GVO so gestalten und digitalisieren, dass sie die Einhaltung der Grundsätze des Art. 5 Abs. 1 DS-GVO sicherstellen. Die Datenverarbeitung im Rahmen digitaler Zugangshürden wird jedoch in vielen Fällen auch gegen die Grundsätze von Treu und Glauben, der Zweckbindung, der Datenminimierung und der Speicherbegrenzung verstoßen und deswegen rechtswidrig sein.

Umgekehrt wird die Zulässigkeit und Rechtmäßigkeit digitaler Zugangshürden in den meisten Fällen erreicht werden können, wenn ein alternativer

Zugang zu der begehrten Leistung auch ohne Datenerhebung möglich ist. Unternehmen und Behörden sind daher aufgerufen, digitale Zugangshürden zu ihren analogen Leistungen zu überprüfen und durch zumutbare alternative Zugänge zu ergänzen.

Für die ausschließlich digitale Ausstellung von Sparpreistickets und die Notwendigkeit, hierfür ein E-Mail-Konto oder eine Mobilfunknummer anzugeben, machte die Deutsche Bahn ihr berechtigtes Interesse an Vervielfältigungs-, Übertragungs- und Einnahmeschutz geltend. Dieses Interesse rechtfertigt jedoch nicht die Erhebung von E-Mail-Adresse oder Mobilfunknummer. Das Ticket kann am Schalter auf Papier ausgedruckt werden. Auf das Ticket kann auch neben der Ticketnummer der Name des Kunden gedruckt werden. Bei der Ticketkontrolle kann dann durch Überprüfung der Ticketnummer und das Vorzeigen eines Ausweises oder einer Bahncard festgestellt werden, ob das Ticket vervielfältigt oder an eine unberechtigte Person übertragen worden ist. Wird das Ticket am Schalter bezahlt, besteht bei diesem Verfahren auch Einnahmeschutz. Aus diesem Grund ist die Erhebung und Speicherung dieser Daten nicht nur unzulässig, sondern verstößt auch gegen die Pflicht zur datenschutzgerechten Systemgestaltung nach Art. 25 Abs. 1 DS-GVO.

Mit dieser datenschutzrechtlichen Argumentation konnte ich z. B. bei der Deutschen Bahn erreichen, dass sie seit dem 15. Dezember 2024 für den Verkauf von Sparpreistickets keine Angaben mehr zu einem E-Mail-Konto oder einem Smartphone fordert und das Sparpreisticket auch auf Papier ausstellt.

11.4
Schwärzung in einer Scheidungsfolgenvereinbarung im Rahmen einer Bonitätsprüfung

Kreditinstitute dürfen Daten aus einer Trennungs- und Scheidungsfolgenvereinbarung zu Zwecken der Bonitätsprüfung verarbeiten. Betroffene haben jedoch das Recht, nicht bonitätsrelevante Daten in dieser Trennungs- und Scheidungsfolgenvereinbarung zu schwärzen.

Im Rahmen einer Beschwerde wurde mir folgender Sachverhalt zur Kenntnis gebracht: Die Betroffene hatte gemeinsam mit ihrem geschiedenen Ehemann Verbindlichkeiten bei einer in meinem Aufsichtsbereich ansässigen Bank. Nach der Scheidung traten die Kreditnehmer mit dem Wunsch an die Bank heran, die Verträge auf die Beschwerdeführerin umschreiben zu lassen. Im Rahmen der berechtigten Prüfung der Bank, ob der geschiedene Ehemann aus dem Vertragsverhältnis entlassen werden kann (Schuldhaftentlassung), ist diese als Kreditgeberin grundsätzlich berechtigt, die Bonität der zukünftig

alleinigen Schuldnerin zu überprüfen. In diesem Zusammenhang darf sie nach Art. 6 Abs.1 UAbs. 1 Buchts. f DS-GVO entsprechende bonitätsrelevante Unterlagen anfordern. Zu diesen gehört auch eine Trennungs- und Scheidungsfolgenvereinbarung, in welcher die geschiedenen Ehepartner diverse Regelungen, u. a. auch in finanziellen Angelegenheiten, treffen.

Die Betroffene erklärte sich einverstanden, die Vereinbarung zur Verfügung zu stellen, bestand aber auf der Möglichkeit, Schwärzungen bezüglich der geregelten Aspekte vornehmen zu dürfen, welche nicht bonitätsrelevant waren. Dieses lehnte die Bank hingegen mit der Begründung ab, dass bei geschwärzten Unterlagen nicht überprüft werden könne, ob nicht auch bonitätsrelevante Passagen unkenntlich gemacht worden seien.

Daher wandte sich die Betroffene an meine Behörde mit der Bitte um Prüfung der Rechtmäßigkeit der Datenerhebung der Bank sowie der Weigerung, Schwärzungen zu akzeptieren.

Zu klären war, aufgrund welcher Rechtsnorm die Daten durch die Bank erhoben werden dürfen. Da es für sie weder eine gesetzliche Pflicht zur Erhebung der Daten aus der Trennungs- und Scheidungsfolgenvereinbarung gibt, noch die Betroffene eingewilligt hat, kommt als Rechtsgrundlage nur Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in Betracht.

Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung

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

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

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

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

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

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

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

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

Die Prüfung der Bonität des verbleibenden Vertragspartners stellt ein berechtigtes Interesse im Sinne dieser Norm dar. Ein diese Interessen überwiegendes schutzwürdiges Interesse am Ausschluss der Erhebung von Daten zur Bonitätsprüfung ist grundsätzlich festzustellen, wenn Daten erhoben werden sollen, welche für die Erfüllung des Erhebungszweckes nicht erforderlich sind.

Das ist in der Regel dann der Fall, wenn aus diesen Daten keine Rückschlüsse auf die Bonität der Betroffenen gezogen werden können.

Da eine Trennungs- und Scheidungsfolgenvereinbarung in der Regel eine Vielzahl von nicht bonitätsrelevanten Informationen erhält, kann an der Erhebung dieser Daten kein berechtigtes Interesse der Bank festgestellt werden. Insofern kann die Erhebung nicht bonitätsrelevanter Daten nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden.

Die Bank hat daher die Betroffenen im Rahmen der Datenerhebung darauf hinzuweisen, dass Schwärzungen vorgenommen werden können, soweit hiervon keine Informationen zu vermögensrechtlichen Regelungen und einmaligen oder wiederkehrenden Zahlungsverpflichtungen betroffen sind.

Die Bank hat diese datenschutzrechtliche Anforderung entsprechend umgesetzt.

11.5
Ausweiskopien in Hotels

Familienurlaub, Geschäftsreise, Städtetrip – ein Hotelaufenthalt gewährt dem Betreiber detaillierte Einblicke in das private Lebensumfeld seiner Gäste. Dazu gehören beispielsweise Informationen über gesundheitliche Merkmale, etwaige Behinderungen, Freizeitaktivitäten, Begleitpersonen sowie sexuelle Orientierungen. Diese sensiblen Daten erfordern vom Hotelbetreiber einen besonders verantwortungsvollen Umgang, um das Recht der Gäste auf Datenschutz nach Art. 7 und 8 GRCh und auf informationelle Selbstbestimmung gemäß Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG zu gewährleisten.

Im laufenden Jahr erreichten mich vermehrt Beschwerden über den Umgang mit personenbezogenen Daten im Hotelgewerbe (zu Ausweiskopien im Beschäftigungsverhältnis s. Kap. 7.5). Hierbei konnten im Wesentlichen zwei Problemfelder identifiziert werden: das Anfertigen von Kopien der Personalausweise bzw. Passdokumente sowie eine unsichere Lagerung der erhobenen personenbezogenen Daten.

Anfertigung von Kopien von Personalausweisen und Passdokumenten

Oftmals behaupten Beherbergungsstätten gegenüber ihren Gästen, dass die Anfertigung von Kopien der Reisedokumente eine zwingende Vorrausetzung für das Zustandekommen des Beherbergungsvertrages sei. Folglich könnten die Reisenden nur übernachten, wenn sie sich bereit erklärten, Kopien ihre Dokumente anfertigen zu lassen.

Nach Art. 4 Abs. 2 DS-GVO umfasst der Begriff der „Verarbeitung" das „Erheben" und das „Erfassen" personenbezogener Daten. Eine solche Verarbeitung liegt bei der Anfertigung von Kopien folglich vor.

Eine Verarbeitung von personenbezogenen Daten für eine anstehende Übernachtung ist nach Art. 6 DS-GVO nur zulässig, wenn einer der nach Abs. 1 genannten Erlaubnistatbestände a bis f erfüllt ist. Für Beherbergungsstätten ist Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO einschlägig. Für die Abfrage von personenbezogenen Daten für einen Meldeschein könnten §§ 29 und 30 Bundesmeldegesetz (BMG) eine Pflicht begründen. Dass die Personalausweise kopiert werden können, könnte sich aus § 20 Abs. 2 Personalausweisgesetz (PAuswG) ergeben.

Zulässigkeit nach Bundesmeldegesetz

Gemäß § 29 BMG sind Hotels verpflichtet, bestimmte personenbezogene Daten von Gästen auf einem Meldeschein zu erfassen. Die Norm wird durch § 30 BMG ergänzt, in dem die zu erhebenden personenbezogenen Daten konkretisiert werden. § 30 Abs. 2 BMG verpflichtet die Hotels, das Datum der Ankunft und der voraussichtlichen Abreise, den Familiennamen sowie den Vornamen, das Geburtsdatum, die Staatsangehörigkeit(en), die Anschrift, die Anzahl der Mitreisenden und derer Staatsangehörigkeit(en) in den Fällen des § 29 Abs. 2 Satz 2 und 3 BMG sowie die Seriennummer des anerkannten und gültigen Passes oder Passersatzpapiers bei ausländischen Personen zu erfassen. Gem. § 30 Abs. 2 BMG haben die Leiter der Beherbergungsstätten bei ausländischen Personen die Angaben im Meldeschein mit denen des Identitätsdokumentes zu vergleichen. Ferner verpflichtet § 30 Abs. 4 BMG, die ausgefüllten Meldescheine für die Dauer von 12 Monaten nach dem Tag der Abreise des Gastes aufzubewahren.

Zulässigkeit nach PAuswG

Der Personalausweis gilt nach § 20 Abs. 1 PAuswG als Identifikationsnachweis und Legitimationspapier unter anderem gegenüber nicht öffentlichen Stellen, wie es Beherbergungsbetriebe darstellen. Problematisch ist, dass

eine Vorlagepflicht im Sinne des § 30 Abs. 2 BMG nur für ausländische Personen besteht. Eine Pflicht für deutsche Staatsbürger, den Personalausweis zu Legitimationszwecken vorzulegen, besteht folglich nicht. Hinsichtlich der teilweise geforderten Kopien der Personalausweise findet sich zwar in § 20 Abs. 2 PAuswG die Möglichkeit, mit Einwilligung des Personalausweisinhabers im Sinn des Art. 6 Abs. 1 UAbs. 1 Buchst. a i. V. m. Art. 7 DS-GVO eine Kopie anzufertigen. Für eine wirksame Einwilligung fehlt jedoch die notwendige Freiwilligkeit. Dieser steht das Koppelungsverbot nach Art. 7 Abs. 4 DS-GVO entgegen, wonach bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, dem Umstand in größtmöglichem Umfang Rechnung getragen werden muss, ob u. a. die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind. Für die Verfolgung überwiegender berechtigter Interessen nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO fehlt die Erforderlichkeit der Erstellung einer Kopie.

Mithin lässt sich festhalten, dass es bezüglich der Anfertigung von Kopien der Personalausweis- und Passdokumente an einer gesetzlichen Grundlage mangelt.

Aufbewahrung der Identitätsdaten

Gemäß Art. 5 Abs. 1 Buchst. c und e DS-GVO dürfen personenbezogene Daten nur dann verarbeitet werden, wenn dies dem Zweck angemessen und auf das unbedingt notwendige Maß beschränkt ist. Zweck der Datenerhebung in Beherbergungsbetrieben ist die Erfüllung gesetzlicher Vorgaben (Meldepflicht, steuerliche Abgaben, ausländerrechtliche Bestimmungen). Die Kopien der Ausweisdokumente aufzubewahren, ist nicht angemessen, da diese noch eine Vielzahl weiterer personenbezogener Daten enthalten, die nach § 30 BMG nicht erforderlich sind. Hierzu gehören beispielsweise die Augenfarbe und die Körpergröße des Ausweisinhabers sowie das Lichtbild.

Einige Beschwerden hatten ferner die Verwahrung von ausgefüllten Meldescheinen und weiteren Unterlagen an den Rezeptionen und Empfangstresen zum Inhalt. Beschwerdegegner waren hierbei sowohl kleinere Beherbergungsbetriebe als auch größere Häuser. Beschwerdeführer bemängelten in manchen Fällen, dass gerade in Zeiten einer unbesetzten Rezeption Unterlagen offen und sichtbar auf dem Tresen lagen. Grundsätzlich gilt, dass Dokumente und Unterlagen mit personenbezogenen Daten nach Art. 5 Abs. 1 Buchst. f DS-GVO vor unberechtigter Einsicht von Dritten geschützt werden müssen.

In einem Fall hat für meine Behörde das zuständige Ordnungsamt Amtshilfe geleistet und vor Ort eine Inaugenscheinnahme durchgeführt. Der Grund

der Beschwerde war das offene Auslegen eines Ordners in einem Beherbergungsbetrieb mit den Meldescheinen i. S. d. § 30 BMG, so dass andere Gäste und fremde Personen Einblick in die ausgefüllten Meldescheine hatten. Der Sachverhalt wurde seitens des Ordnungsamtes bestätigt. Die Rezeption war teilweise unbesetzt, so dass der Ordner für jeden offen einsehbar war. Eine Mitarbeiterin des Ordnungsamtes konnte im Ordner ungehindert blättern und folglich die personenbezogenen Daten der bisherigen Gäste einsehen. Dies war auch jeder anderen Person möglich. Da hierbei Geburtsdatum, Name und Vorname, Anschrift sowie weitere personenbezogene Daten offen einsehbar waren, ordnete ich gegenüber dem Hotelbetreiber an, das Verfahren umgehend einzustellen. Der Beschwerdegegner bestätigte mir daraufhin die Einstellung des beanstandeten Verfahrens und eine zukünftige datenschutzkonforme Handhabe mit den Meldescheinen.

12. Gesundheitsbereich

Im Gesundheitsbereich werden Gesundheitsdaten verarbeitet, die aufgrund ihrer Sensitivität und ihres Diskriminierungspotenzials nach Art. 9 DS-GVO einen besonderen Schutz erfordern. Die informationelle Selbstbestimmung des Patienten wird gestärkt durch sein Recht auf Auskunft über seine Gesundheitsdaten. Dieses umfasst auch ein Recht des Patienten auf kostenlose Kopie der Patientenakte, das auch in den Berufsordnungen der Gesundheitsberufe zu berücksichtigen ist (Kap. 12.1). Der Schutz der Gesundheitsdaten ist in besonderer Weise gefährdet, wenn Krankenhäuser geschlossen werden und niemand mehr für den Schutz verantwortlich ist (Kap. 12.2). Daher bedarf es ausdrücklicher Regelungen für die Letztverantwortung für die Aufbewahrung von Patientenakten (Kap. 12.3). Ein umfangreicher Missbrauch von Gesundheitsdaten wäre auch bei dem Cyberangriff auf das Universitätsklinikum Frankfurt am Main möglich gewesen (Kap. 12.4). Nutzt eine Blutspendeeinrichtung mit Einwilligung der betroffenen Personen zu deren Identifikation einen Handvenenscanner, sollte sie stets auch ein alternatives Verfahren anbieten, bei dem keine biometrischen Daten verarbeitet werden (Kap. 12.5). Auch bei den Datenerhebungen im Rahmen von Schuleingangsuntersuchungen ist der besondere Schutz von Gesundheitsdaten zu gewährleisten (Kap. 12.6).

12.1
Recht des Patienten auf kostenlose Kopie der Patientenakte

In seinem Urteil vom 26. Oktober 2023 (C-307/22) stellte der EuGH fest, dass Patientinnen und Patienten einen aus Art. 15 DS-GVO resultierenden Anspruch auf eine unentgeltliche erste Kopie ihrer Akte haben. Ich habe daraufhin auf eine Entschließung der DSK hingewirkt, in der auch die Heilberufskammern dazu aufgefordert werden, die entsprechenden Kostenregelungen in ihren Berufsordnungen zu ändern und das Urteil des EuGH zu berücksichtigen.

Am 26. Oktober 2023 hat sich der EuGH zum Verhältnis des Rechts auf Einsicht in die Patientenakte aus § 630g BGB zum Recht auf Kopie personenbezogener Daten aus Art. 15 Abs. 3 DS-GVO geäußert. Im Ergebnis muss die erste Kopie der Patientenakte unentgeltlich zur Verfügung gestellt werden. Durch eine nationale Regelung wie § 630g Abs. 2 Satz 2 BGB darf dem Patienten keine Kostenlast hierfür auferlegt werden. Der Verantwortliche kann jedoch für alle weiteren Kopien ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangen.

Allerdings enthalten auch die Berufsordnungen der Heilberufskammern entsprechende Regelungen zur Kostenerstattung für die Herausgabe von Kopien aus der Patientenakte (§ 10 Abs. 2 a. E. Musterberufsordnung der Bundesärztekammer; § 12 Abs. 4 Musterberufsordnung der Bundeszahnärztekammer; § 11 Abs. 1 der Musterberufsordnung der Psychotherapeutenkammer). Damit gibt es derzeit Satzungen, die der DS-GVO widersprechen und die Rechtsprechung des EuGH missachten.

Im Sinne eines möglichst einheitlichen Rechtsrahmens war daher aus meiner Sicht auch im Berufsrecht darauf hinzuwirken, dass keine Regeln bestehen bleiben, die nicht mit Unionsrecht vereinbar sind. Soweit dies die Regelungen des § 630g BGB anbelangt, hat der Bundesgesetzgeber bereits Bestrebungen zur Anpassung unternommen (Referentenentwurf des Bundesministeriums der Justiz: Entwurf eines Gesetzes zur Änderung des Bürgerlichen Gesetzbuchs – Einsichtnahme in die Patientenakte und Vererblichkeit bei Persönlichkeitsrechtsverletzung, https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2024_Einsichtnahme_Patientenakte.html?nn=110518). Auch auf Landesebene sollte mithin eine entsprechende Anpassung erfolgen, um Missverständnisse und eine Einschränkung der Betroffenenrechte zu vermeiden.

Da sowohl von der Landesärztekammer Hessen, als auch von der Psychotherapeutenkammer Hessen auf meine entsprechende Nachfrage die Rückmeldung einging, dass eine Anpassung der Berufsordnungen erst in weiter zeitlicher Ferne erfolge, habe ich auf eine Entschließung der DSK zur kostenlosen Kopie der Patientenakte und Änderung der Berufsordnungen der Heilberufskammern hingewirkt, https://www.datenschutzkonferenz-online.de/media/en/2024-09-11_Entschliessung_DSK_Patientenakte.pdf.

Die Entschließung vom 11. September 2024 stellt nochmals ausdrücklich klar, dass das Recht auf kostenlose Erstkopie der Patientenakte durch eine nationale Regelung nicht eingeschränkt werden kann. Darüber hinaus fordert die DSK die Heilberufskammern darin dazu auf, die berufsrechtlichen Regelungen zeitnah an die Vorgaben aus der DS-GVO anzupassen. Zudem wird darauf hingewiesen, dass die bestehenden berufsrechtlichen Regelungen, die für die Bereitstellung einer Erstkopie eine Kostenpflicht für den Patienten oder die Patientin vorsehen, keine Anwendung finden. Abschließend fordert die DSK die Heilberufskammern dazu auf, ihre Kammermitglieder über die Entscheidung des EuGHs zu informieren und zu einem rechtskonformen Vorgehen anzuhalten.

12.2
Krankenhausschließungen in Hessen

Anfragen und Hinweise im Hinblick auf Krankenhausschließungen und damit einhergehende herrenlose Patientenakten erhielt ich leider auch wieder in diesem Berichtszeitraum. Zwischenzeitlich konnte ich erreichen, dass sich auch die DSK zu diesem wichtigen Thema positioniert.

Verlassene Kliniken

Im Berichtsjahr war ich erneut mit zwei verlassenen Kliniken befasst, in denen nach ihrer Schließung weiterhin Patientendaten vorhanden waren. Es handelte sich um eine ehemalige Klinik für Rehabilitation (Reha-Klinik) und eine ehemalige Parkinson-Klinik.

Im Fall der Reha-Klinik wies mich die örtliche Polizei darauf hin, dass sich Unbefugte durch eine unverschlossene Hintertür Zugang zu den Räumlichkeiten der Klinik verschafften und dort Patientenakten offen zugänglich lagerten.

Bei den in der Klinik noch aufbewahrten Patientendaten handelte es sich um besonders sensible Gesundheitsdaten, die dringend vor unberechtigten Zugriffen geschützt werden mussten. Ebenso musste sichergestellt sein, dass Patientinnen und Patienten auf Verlangen Einsicht in ihre Behandlungsdokumentation nehmen können.

Die Verantwortlichen müssen nach Art. 5 Abs. 1 Buchst. f DS-GVO insbesondere durch geeignete technische und organisatorische Maßnahmen eine angemessene Sicherheit personenbezogener Daten gewährleisten.

In dieser Angelegenheit konnte ich darauf hinwirken, dass die Hintertür wieder abgeschlossen wurde und dadurch unbeteiligte Dritte nicht mehr ohne Weiteres in die Räumlichkeiten eindringen konnten.

Um hier eine langfristige Lösung zu erreichen, habe ich das im Berichtsjahr für das Thema Gesundheit zuständige Ministerium für Soziales und Integration eingeschaltet und über die Situation informiert.

Im Fall der verlassenen Parkinson-Klinik kontaktierte mich die Insolvenzverwalterin der Klinik und teilte mir mit, dass das Insolvenzverfahren mangels Masse aufgehoben werde. Es stelle sich nun die Frage, durch wen die weitere Aufbewahrung der Patientenakten erfolgen sollte. Auch hier wurde das Ministerium für Soziales und Integration eingebunden. Ich habe die Insolvenzverwalterin darauf hingewiesen, dass neben der Landesärztekammer Hessen auch die Hessische Krankenhausgesellschaft oder der Landesverband der Privatkliniken in Hessen e. V. Ansprechpartner für dieses Thema sein können.

Bewertung und Handlungsbedarf

Es hat sich in der Vergangenheit gezeigt, dass leerstehende Klinikgebäude als sogenannte „Lost Places“ regelmäßig unberechtigte Personen anziehen, die dort Filmaufnahmen anfertigen und diese im Internet veröffentlichen. Dadurch besteht für die betroffenen Personen das Risiko der Offenlegung personenbezogener Gesundheitsdaten gegenüber einer Vielzahl Dritter.

Häufig fehlt es bei der Schließung von Krankenhäusern an einem verantwortlichen Ansprechpartner, der sich um eine sichere Aufbewahrung der Patientendaten, die Erfüllung von Auskunftsrechten und die Löschung der Patientendaten nach Ablauf der Aufbewahrungsfristen kümmert (siehe zur Rechtslage in der Insolvenz von Krankenhäusern Roßnagel/Gierich, Patientenakten in Klinik-Insolvenzen, Zeitschrift für Datenschutz (ZD) 2025, Heft 3, 123 ff.).

Ich habe schon in der Vergangenheit auf einen Handlungsbedarf für die genannten Konstellationen hingewiesen (siehe hierzu meinen 44. und 49. Tätigkeitsbericht). Mit der Novellierung des Hessischen Krankenhausgesetzes (HKHG) im Jahr 2022 wurde in § 12 Abs. 5 HKHG eine wichtige Neuregelung getroffen. Danach sind hessische Krankenhäuser, die dem HKHG unterliegen, dazu verpflichtet, Konzepte für die sichere Aktenverwahrung im Falle ihrer Insolvenz zu erstellen und bereitzuhalten (s. auch https://datenschutz.hessen.de/datenschutz/gesundheitswesen/schutz-der-patientendaten-bei-schliessung-von-krankenhaeusern).

Für die beiden hier geschilderten Fällen konnte diese Regelung allerdings nicht weiterhelfen, da private Reha-Kliniken nicht dem Anwendungsbereich des HKHG unterfallen und die Insolvenz der Kliniken bereits vor Inkrafttreten der Neuregelung erfolgte.

DSK-Entschließung

Die DSK hat sich auf meine Initiative ebenfalls diesem Thema gewidmet und in ihrer Entschließung „Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern“ die datenschutzrelevanten Herausforderungen für Klinikbetreiber und Insolvenzverwalter dargestellt (https://datenschutzkonferenz-online.de/media/en/2024-05-15_DSK-Entschliessung_Krankenhausschliessung.pdf). Die DSK hat hierin auch denkbare Lösungsansätze aufgezeigt, die auf Landes- und Bundesebene weiterverfolgt werden sollten.

12.3
Letztverantwortung für die Aufbewahrung von Patientenakten

Im Hinblick auf die bevorstehende Evaluierung des Hessischen Gesetzes über das Berufsrecht und die Kammern der Heilberufe (Heilberufsgesetz) habe ich gegenüber der Landesärztekammer Hessen und dem Hessischen Ministerium für Gesundheit eine neue Regelung angeregt. Hiernach sollen die Heilberufskammern in Fällen von Praxisschließungen die Letztverantwortung für die Aufbewahrung der Patientenakten tragen.

Aus meinem Zuständigkeitsbereich sind mir Fälle bekannt, in denen Arztpraxen oder Medizinische Versorgungszentren (MVZ) kurzfristig und oftmals für die Patientinnen und Patienten unerwartet ihre Tätigkeit einstellten. Damit war zugleich auch oft die Aufbewahrung der Patientendokumentationen nicht mehr hinreichend gewährleistet. Dies hatte zur Folge, dass für die Patientinnen und Patienten der jeweiligen Einrichtung auch die Wahrnehmung von Betroffenenrechten, insbesondere die Akteneinsicht gemäß Art. 630g BGB und die Auskunft gemäß Art. 15 DS-GVO, nicht mehr möglich oder zumindest stark erschwert war. Ich sah daher in der bevorstehenden Evaluierung des Heilberufsgesetzes eine Gelegenheit, für solche Konstellationen eine gesetzliche Lösung zu schaffen und damit die Patientenrechte zu stärken.

Die neue Regelung soll bekräftigen, dass ein Kammermitglied beim Ausscheiden aus einer eigenen Niederlassung oder bei deren Schließung für die sichere Verwahrung der Patientendokumentationen Sorge tragen muss. Insbesondere jedoch – und dies ist in Hessen bislang nicht geregelt – sollen die Heilberufskammern in solchen Fällen die Letztverantwortung für die Aufbewahrung der Patientenakten tragen.

Solche Regelungen bestehen bereits in Baden-Württemberg, Rheinland-Pfalz und Sachsen.

§ 4 Abs. 1 HBKG BW

Die Kammern haben bei der Wahrnehmung ihrer Aufgaben die Interessen des Gemeinwohls und die Rechte der Patienten zu beachten. Sie haben Patientenunterlagen für die Dauer der Aufbewahrungspflicht in Obhut zu nehmen und den Patienten Einsicht zu gestatten, sofern dies nicht durch das verpflichtete Kammermitglied oder dessen Rechtsnachfolgerin oder -nachfolger gewährleistet ist. Gegenüber den Verpflichteten besteht in diesem Fall ein Anspruch auf Erstattung der Kosten, welche im Zusammenhang mit der Aufbewahrung der Patientenakten entstehen. Die Kammern können andere Kammermitglieder oder Dritte mit der Erfüllung dieser Aufgabe betrauen, des Weiteren können die Kammern gemeinsame Einrichtungen zur Erfüllung dieser Aufgabe errichten oder nutzen.

§ 7 Abs. 3 SächsHKaG

Die Kammern haben Patientenakten nach § 20 Absatz 1 Satz 2 Nummer 2 aufzubewahren, wenn ein Mitglied oder dessen Rechtsnachfolger nicht in der Lage ist, diese ordnungsgemäß zu verwahren. Sie können andere Mitglieder oder geeignete Dritte mit der Erfüllung dieser Aufgabe betrauen sowie gemeinsame Einrichtungen zur Erfüllung dieser Aufgabe errichten oder nutzen. Die Kammern oder von diesen nach Satz 2 Beauftragte können von dem Mitglied oder dessen Rechtsnachfolger Kostenerstattung verlangen. § 1936 des Bürgerlichen Gesetzbuches bleibt unberührt.

§ 22 Abs. 2 HeilBG

Die Kammermitglieder haben beim Ausscheiden aus einer eigenen Niederlassung oder bei deren Schließung dafür zu sorgen, dass die in Ausübung ihres Berufs gefertigten medizinischen und pflegerischen Aufzeichnungen und sonstigen dort vorhandenen Patientenunterlagen nach den Vorschriften der Schweigepflicht und des Datenschutzes untergebracht und nur für Berechtigte zugänglich gemacht werden. Kommt ein Kammermitglied dieser Pflicht nicht nach, ist die Kammer verpflichtet, die Unterlagen im Rahmen der Verwaltungsvollstreckung zu verwahren und zu verwalten. Die Kammern können auch gemeinsame Einrichtungen zur Aufbewahrung und Verwaltung errichten oder nutzen; das Nähere regelt die Satzung.

Ob und wann eine solche Regelung vom Hessischen Gesetzgeber umgesetzt wird, ist noch nicht bekannt.

Um die Betroffenenrechte von hessischen Patientinnen und Patienten zu stärken, sollte den Beispielen aus Baden-Württemberg, Sachsen und Rheinland-Pfalz gefolgt werden. Ich habe dies auch noch einmal so gegenüber der Landesärztekammer Hessen kommuniziert und für den Lösungsansatz geworben. Auf diese Weise haben die Patientinnen und Patienten eine feste Anlaufstelle, falls Kammermitglieder ihren berufsrechtlichen Pflichten nicht mehr nachkommen können oder wollen.

12.4
Cyberangriff auf das Universitätsklinikum Frankfurt am Main

Krankenhäuser sind für Ransomware-Angriffe ein interessantes Ziel: Unzählige hochsensible Patientendaten können verschlüsselt und auch exfiltriert werden. Die Rückgabe oder Löschung dieser Daten erfolgt dann meist nur gegen die Zahlung eines höheren Geldbetrages. Glück im Unglück hatte diesbezüglich das Uniklinikum Frankfurt. Der Ransomware-Angriff Ende 2023 konnte rechtzeitig erkannt und unterbunden werden, bevor Daten verschlüsselt oder exfiltriert wurden. Dennoch stellte der Angriff das Klinikum im Berichtszeitraum vor große Herausforderungen.

Der Cyberangriff und seine Folgen

In Hessens größtem Krankenhaus wurden am Freitag, den 6. Oktober 2023, im Rahmen einer Routinekontrolle des Netzwerks Unregelmäßigkeiten entdeckt. Es zeigte sich, dass sich unberechtigte Personen Zugang zu bestimmten IT-Systemen verschafft hatten und wahrscheinlich einen möglichen Ransomware-Angriff vorbereiteten (siehe 52. Tätigkeitsbericht, Kap. 14.6, S. 223f.). Umgehend wurden daher die entsprechenden Notfallprozesse initiiert, ein Krisenstab eingerichtet und externe qualifizierte IT-Sicherheitsdienstleister eingebunden. Das Uniklinikum entschloss sich außerdem, die gesamte IT-Infrastruktur vom Internet zu trennen, um den Angreifern den Zugang zu entziehen. Die internen IT-Systeme und -Dienste wurden dabei weiter betrieben, um die Patientenversorgung sicherstellen zu können. Durch die Trennung vom Internet waren jedoch die Websites und E-Mail-Adressen des Uniklinikums nicht mehr zu erreichen und auch aus dem Uniklinikum selbst konnte nicht mehr auf das Internet zugegriffen werden. Alltägliche Dinge wie das Rechnungswesen, Gehaltszahlungen, Logistik und Bestellungen waren nicht mehr möglich.

Das Uniklinikum informierte neben weiteren Aufsichtsbehörden auch mich gemäß Art. 33 DS-GVO über den schweren IT-Sicherheitsvorfall und die dadurch verursachte Verletzung des Schutzes personenbezogener Daten. Im Rahmen der Meldung gemäß Art. 33 DS-GVO stand ich im Austausch mit der verantwortlichen Stelle, die mir über den Sachverhalt und die gewonnenen Erkenntnisse berichtete. Es wurde vermutet, dass die erfolgten Angriffsmaßnahmen einen Ransomware-Angriff vorbereiten sollten. Dieser wurde offenbar noch in der Phase der Ausbreitung von Schadsoftware erkannt und rechtzeitig unterbunden. Die von den beauftragten qualifizierten Sicherheitsdienstleistern durchgeführten forensischen Analysen ergaben glücklicherweise keine Hinweise darauf, dass Daten von Patientinnen oder Patienten exfiltriert oder vernichtet worden waren. Dementsprechend hatte der Vorfall durch die potenzielle Verletzung der Vertraulichkeit der personenbezogenen Daten keine hohen Risiken für die betroffenen Patientinnen und Patienten zur Folge.

Als Lehre aus dem Vorfall entschloss sich das Uniklinikum, die eigene IT-Infrastruktur neu zu konzipieren und aufzubauen. Daher wurde dem üblichen Vorgehen gefolgt, dass die bisherigen IT-Systeme und Dienste in einer getrennten „roten Zone“ betrieben wurden, die weiter vom Internet getrennt waren. Die neue IT-Infrastruktur wird dabei in einer sogenannten „grünen Zone“ aufgebaut. Das Uniklinikum richtete IT-Dienste wie E-Mail und Zahlungsdienste, die umgehend benötigt wurden, temporär in einer „grauen Zone“ ein, bis diese in der grünen Zone neu aufgebaut und integriert werden

konnten. Die Behandlung und Analyse des eigentlichen Vorfalls und der anschließende Wiederaufbau der IT beschäftigte das Uniklinikum und die eingebundenen externen IT-Dienstleister noch das Jahr 2024.

Auswirkungen von Ransomware-Angriffen im Gesundheitsbereich

Kommt es bei einer Einrichtung aus dem Gesundheitsbereich, wie beim hier betrachteten Fallbeispiel einer Klinik, zu einem schweren IT-Sicherheitsvorfall, beispielsweise einem Ransomware-Angriff, führt dieser in der Regel auch zu Verletzungen des Schutzes personenbezogener Daten im Sinne der DS-GVO und zu potenziell hohen Risiken für die betroffenen Personen. Unmittelbare konkrete Schäden für Patientinnen und Patienten können dabei aus der Nichtverfügbarkeit oder Veränderung der verarbeiteten Gesundheitsdaten und damit ggf. auch der Medizingeräte entstehen. Lebenserhaltende Maßnahmen oder Operationen könnten beeinträchtigt oder verzögert werden. Sofern sich Daten nicht wiederherstellen lassen, müssen u. U. bereits durchgeführte Untersuchungen wiederholt werden. Auch die Organisation der angegriffenen Einrichtung ist in der Regel schwer getroffen und muss entsprechend aufwendig umgestellt werden.

Neben der Verfügbarkeit und Integrität führen insbesondere Ransomware-Angriffe häufig auch zu einer Verletzung der Vertraulichkeit der verarbeiteten Gesundheitsdaten. Während sich die Angreifer in der angegriffenen IT-Infrastruktur bewegen, kann es zur Einsichtnahme in personenbezogene Daten kommen. Häufig werden auch Daten der Patientinnen und Patienten sowie der Beschäftigten von den Angreifern exfiltriert und auf eigene Datenspeicher kopiert. Die Veröffentlichung der Daten oder die Androhung der Veröffentlichung ist dabei Teil der Erpressung der verantwortlichen Stelle. Es kommt auch vor, dass exfiltrierte Daten von den Angreifern an Dritte verkauft werden. Potenzielle Schäden aus einer Veröffentlichung können je nach Daten vielfältig sein und sich ggf. auch erst nach Jahren manifestieren.

Kommt es zu einem Vorfall, wie hier betrachtet, und damit zu Verletzungen des Schutzes personenbezogener Daten, führt dies oftmals auch zu immateriellen Schäden für die verantwortliche Stelle, die im Imageschaden und im Vertrauensverlust gegenüber der betroffenen Einrichtung bestehen. Die DS-GVO sieht in Art. 82 DS-GVO weiterhin auch eine Haftung der verantwortlichen Stellen für materielle und immaterielle Schäden vor, die den betroffenen Personen entstehen. Sie können ihre Ansprüche auf Schadensersatz gegenüber der verantwortlichen Stelle vor den Zivilgerichten geltend machen.

Vorbeugen ist besser als heilen

Im Fallbeispiel des Angriffs auf das Uniklinikum Frankfurt konnten durch die frühzeitige Erkennung des Angriffs an einem Freitag und der sofortigen Reaktion der verantwortlichen Stelle schlimmere Schäden vermieden werden. Durch die Trennung der IT-Infrastruktur vom Internet kam es zwar zu Beeinträchtigungen und organisatorischen Herausforderungen, allerdings war die Verfügbarkeit der verarbeiteten personenbezogenen Daten weiterhin gewährleistet, der Betrieb konnte weitestgehend fortgeführt und die Versorgung der Patientinnen und Patienten sichergestellt werden.

Durch den Vorfall sind der verantwortlichen Stelle erhebliche Kosten und Aufwände entstanden. Als ein Teil davon kann die Notwendigkeit gesehen werden, für die Sicherheit der Verarbeitung personenbezogener Daten gemäß Art. 32 DS-GVO wieder ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Der Vorfall hat der verantwortlichen Stelle zudem wertvolle Anregungen für die Neukonzeption der IT-Infrastruktur gegeben.

Das Uniklinikum Frankfurt geht vorbildlich offen mit dem Vorfall um und informiert andere Gesundheitseinrichtungen über die gemachten Erfahrungen in verschiedenen Gremien und Foren. Gerade im Gesundheitsbereich besteht die Erwartung, dass Gesundheitsdaten besonders gut geschützt werden. Über geeignete technische und organisatorische Maßnahmen müssen entsprechende Einrichtungen daher hinreichend sicherstellen, dass es gar nicht erst zu solchen Vorfällen kommen kann. Mir sind leider auf Grund der Komplexität und Individualität der jeweiligen Umstände der Gesundheitseinrichtungen Grenzen bei der Beratung und Unterstützung gesetzt. Insbesondere für Krankenhäuser als Teil der kritischen Infrastrukturen (KRITIS) erfolgt eine Regulierung durch das BSI-Gesetz (BSIG) und die KRITIS-Verordnung (KritisV). Für den Blickwinkel der IT-Sicherheit stellt dementsprechend auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) verantwortlichen Stellen Informationen zur Verfügung.

Fazit

In den letzten Jahren nehmen die mir gemäß Art. 33 DS-GVO gemeldeten Verletzungen des Schutzes personenbezogener Daten auf Grund von Angriffen auf IT-Systeme und -Dienste stetig zu. Dies betrifft konkret auch den Gesundheitsbereich. Elektronische Gesundheitsakten, vernetzte Medizingeräte und die zunehmende papierlose Organisation stellen hierfür Faktoren und Gründe dar. Ich habe daher gegenüber dem zuständigen Ministerium auf Landesebene mehrfach die Bildung eines neuen Gremiums angeregt, das Konzepte zur Vorbeugung und zum Umgang mit Cyberangriffen im Gesundheitsbereich erarbeitet. In dem Gremium sollten die wesentlichen

Stakeholder aus dem Gesundheitsbereich zusammenkommen. Ein Hauptziel dieses Zusammenschlusses wäre es, bestehendes Wissen zu aktuellen und vergangenen Cyberangriffen zu teilen. Durch ein gemeinsames Lernen in diesem Bereich könnte so idealerweise das Sicherheitsniveau für alle Beteiligten erhöht werden.

12.5
Handvenenscanner in einer Blutspendeeinrichtung

Nutzen Verantwortliche zu Identifikationszwecken ein biometrisches Verfahren auf Grundlage der Einwilligung der betroffenen Personen, sollten sie stets ein alternatives Verfahren anbieten, bei dem keine biometrischen Daten nach Art. 4 Nr. 14 DS-GVO verarbeitet werden. Insbesondere wenn eine Einwilligung in die Verarbeitung biometrischer Daten Voraussetzung für den Zugang zu Dienstleistungen der Verantwortlichen ist, kann ansonsten nicht von der Freiwilligkeit der Einwilligung nach Art. 4 Nr. 11, Art. 7 Abs. 4 DS-GVO ausgegangen werden. Den betroffenen Personen muss in solchen Fällen vielmehr eine alternative Verfahren zur Identifizierung angeboten werden, damit sie eine Wahlmöglichkeit haben.

Handvenenscan zur Identifizierung

Ein Unternehmen in Hessen, das Blutplasma von Spendern sammelt, überprüfte vor jeder Spende die Identität der Spender. Hierzu bediente man sich eines Verfahrens des Handvenenscannens: Bei der erstmaligen Registrierung von Spendern wurden diesen jeweils eine Ausweiskarte ausgestellt. Auf dieser wurde eine digitale Repräsentation (ein sogenanntes „Template“) ihrer Handvenen gespeichert, die mittels eines berührungslosen Infrarotsensors erfasst wurden. Dieses Verfahren beruht darauf, dass das Muster der menschlichen Handvenen ähnlich einmalig ist wie das eines Fingerabdrucks und somit bei der Verifikation ihrer Identität eine ausreichend hohe Einzigartigkeit sicherstellt. Da es sich dabei um Daten zu physiologischen Merkmalen der Personen handelt, umfasst dies eine Verarbeitung von biometrischen Daten nach Art. 4 Nr. 14 DS-GVO.

Vor einer Spende sollten die Spender dann ihre Hand jeweils wieder erneut auf den Sensor auflegen, der dann durch Abgleich von Handvenen-Template auf der Karte einerseits und dem „live“ gewonnenen Handvenen-Abbild andererseits überprüfte, ob es sich bei der vorstelligen Person um den ursprünglich registrierten und mittels Karte ausgewiesenen Spender handelte.

Eine Spenderin beschwerte sich darüber, dass das Unternehmen zur wiederkehrenden Identifikation der Spender kein alternatives Verfahren, das keine Verarbeitung biometrischer Daten voraussetzt, anbot.

Das Unternehmen teilte mir in dem Beschwerdeverfahren mit, dass die betroffenen Personen nur dann als Spender registriert werden können, wenn sie ihre Einwilligung zur Verarbeitung biometrischer Daten zur Identifikation mittels Handvenenscanner erteilen. Der Einsatz des Handvenenscanners sei sehr sicher und könne die Anforderungen aus dem Gesetz zur Regelung des Transfusionswesens an die eindeutige Identifikation von Spendern bestmöglich erfüllen.

Datenschutzrechtliches Erfordernis einer alternativen Methode

Hinsichtlich der Freiwilligkeit der Einwilligung nach Art. 4 Nr. 11 und Art. 7 Abs. 4 DS-GVO bestanden erhebliche Zweifel, da das Unternehmen kein alternatives Verfahren zur Identifikation der Spender ohne Verarbeitung biometrischer Daten angeboten hat.

Es kann nur dann davon ausgegangen werden, dass eine betroffene Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte und freie Wahl hat, also in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden (s. DSK Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf mit Verweis auf Erwägungsgrund 42 DS-GVO sowie EDSA-Leitlinien 05/2020 zur Einwilligung https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf). Nach dem sogenannten Koppelungsverbot aus Art. 7 Abs. 4 DS-GVO ist hierbei auch zu berücksichtigen, ob die Erfüllung eines Vertrages von einer Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich ist.

Eine Blutplasma-Spende war bei dem Unternehmen ohne Einwilligung in die Identifikation mittels Handvenenscan nicht möglich, sondern von der entsprechenden Einwilligung abhängig. Die Verarbeitung der biometrischen Daten mittels Handvenenscanner war aber nicht erforderlich zur Durchführung einer Blutspende als Erfüllung des Vertrages, da sich auch andere, datensparsamere Verfahren zur Identifikation anbieten.

Als alternatives Verfahren zur Prüfung der Spenderidentität kam hier insbesondere die Sichtung eines Ausweisdokuments in Betracht. Dieses Verfahren wird auch von der Richtlinie zur Gewinnung von Blut und Blutbestandteilen und zur Anwendung von Blutprodukten der Bundesärztekammer zur Identifikation der Spender genannt (vgl. Ziffer 2.2.4.1 BAEK Richtlinie zur Gewinnung von

Blut und Blutbestandteilen und zur Anwendung von Blutprodukten – Richtlinie Hämotherapie, https://www.bundesaerztekammer.de/fileadmin/user_upload/BAEK/Themen/Medizin_und_Ethik/Richtlinie-Haemotherapie-2023_neu2.pdf).

Auch die EDSA-Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte fordern bei der Authentifizierung mittels biometrischer Daten stets ein alternatives Verfahren, das keine Verarbeitung biometrischer Daten erfasst (https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_de.pdf, Rn. 86). Diese EDSA-Leitlinien beziehen sich unmittelbar nur auf die Verarbeitung biometrischer Daten mittels Videoüberwachung, die entsprechende Schlussfolgerung kann aber auch auf die Verarbeitung mittels Handvenenscanner übertragen werden.

Nach der Verpflichtung zur datenschutzgerechten Gestaltung der Datenverarbeitungssysteme des Art. 25 Abs. 1 DS-GVO ist das alleinige Vorhalten einer Identifikationslösung problematisch, da der Verantwortliche den Grundsatz der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DS-GVO durch geeignete technische und organisatorische Maßnahmen umsetzen muss. Er darf also auch aus diesem Blickwinkel keine Verarbeitung personenbezogener Daten in einem Umfang durchführen, der über das notwendige Maß hinausgeht.

Personalausweis als Alternative

Nachdem ich das Unternehmen auf die erheblichen Zweifel bezüglich der Freiwilligkeit der Einwilligung in die Verarbeitung biometrischer Daten hingewiesen habe, hat es den Prozess zur Spenderidentifikation geändert und ein alternatives Verfahren hinzugefügt. Spender können sich nun auch per Sichtkontrolle des Personalausweises identifizieren lassen. Somit haben sie die Wahlmöglichkeit zwischen einem Verfahren, das biometrische Daten verarbeitet, und einem Verfahren, das ohne die Verarbeitung biometrischer Daten auskommt. Aufgrund der umfassenden Einsicht für die Problematik seitens des Unternehmens und der zeitnahen Bereitstellung einer datenschutzfreundlicheren Alternative konnte ich vom Ergreifen aufsichtsbehördlicher Abhilfemaßnahmen in diesem Fall absehen.

12.6
Datenerhebungen im Rahmen von Schuleingangsuntersuchungen

Im Berichtszeitraum habe ich das Hessische Landesamt für Gesundheit und Pflege zu den im Kontext der Schuleingangsuntersuchungen verwendeten Unterlagen beraten. Hierbei konnte ich sowohl für eine bessere Verständ-

lichkeit und Transparenz sorgen als auch dafür, dass sehr sensible und nicht erforderliche Daten nicht mehr abgefragt werden.

Die Schuleingangsuntersuchung ist eine staatliche Pflichtuntersuchung. Sie dient ausschließlich dazu, die gesundheitliche Schulfähigkeit des Kindes festzustellen. Im Rahmen der Schuleingangsuntersuchung werden vom schulärztlichen Dienst der hessischen Gesundheitsämter zahlreiche Daten schulpflichtiger Kinder erhoben. Die Betroffenen sind dabei zur Mitwirkung verpflichtet. Dies ergibt sich aus § 71 Abs. 1 Hessisches Schulgesetz (HSchG) und aus § 2 der Verordnung über die Zulassung und die Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege.

§ 71 HSchG

(1) Soweit zur Vorbereitung einer Entscheidung nach diesem Gesetz schulärztliche oder schulpsychologische Untersuchungen sowie sonderpädagogische Überprüfungen erforderlich werden, sind die Kinder, Jugendlichen und volljährigen Schülerinnen und Schüler verpflichtet, sich untersuchen zu lassen und an wissenschaftlich anerkannten Testverfahren teilzunehmen. In begründeten Einzelfällen kann durch die Schulaufsichtsbehörde eine Untersuchung nach Satz 1 angeordnet werden.

(2) Kinder und Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler haben die für die Untersuchungen erforderlichen Angaben zu machen. Kinder, Jugendliche und volljährige Schülerinnen und Schüler dürfen dabei in der Regel nicht befragt werden über Angelegenheiten, die ihre oder die Persönlichkeitssphäre ihrer Eltern oder Angehörigen betreffen.

(3) Jugendliche, ihre Eltern und volljährige Schülerinnen und Schüler sind über die Untersuchungen und Testverfahren vorher näher zu informieren. Ihnen ist Gelegenheit zur Besprechung der Ergebnisse und zur Einsicht in die Unterlagen zu geben.

(4) Für Untersuchungen im Rahmen der Schulgesundheitspflege gelten Abs. 1 bis 3 entsprechend. Dabei können auch röntgenologische Untersuchungen sowie perkutane und intrakutane Tuberkuloseproben angeordnet werden.

(5) Die nähere Ausgestaltung der Schulgesundheitspflege und die Zulassung der für sie erforderlichen Untersuchungen erfolgt durch Rechtsverordnung.

(6) Diese Vorschriften gelten auch für die Schulen in freier Trägerschaft.

§ 2 SchulGesPflV

(1) Schulärztliche Untersuchungen finden anlässlich der Einschulung statt und sind danach in jährlichen Abständen bis zum Ende der Schulausbildung zulässig. Einschulung im Sinne des Satz 1 ist auch die erstmalige Aufnahme an einer Schule im Geltungsbereich des Hessischen Schulgesetzes in der Fassung vom 1. August 2017, soweit nicht eine Einschulungsuntersuchung in einem anderen Land erfolgt ist. Die Untersuchungen dienen der Gesunderhaltung, Entwicklungsbeurteilung und der Krankheitsfrüherkennung und schließen eine Beratung zur Veranlassung notwendiger Folgemaßnahmen und eine Impfberatung ein.

Aus besonderem Anlass sind schulärztliche Untersuchungen zulässig, wenn und soweit Anhaltspunkte für die Annahme vorliegen, dass eine Krankheit der Schülerin oder des Schülers den Schulbesuch oder die Gesundheit der Mitschülerinnen und Mitschüler gefährdet.

(2) Die schulärztlichen Untersuchungen können neben funktions- und entwicklungsdiagnostischen Untersuchungen auch körperliche Untersuchungen erfassen, soweit dies nach dem Stand der Erkenntnisse der medizinischen Wissenschaft zur sachgerechten Erreichung des Untersuchungsziels notwendig und geeignet erscheint. Invasive und mit stofflichen Belastungen verbundene Untersuchungsverfahren sind im Rahmen von Untersuchungen aus besonderem Anlass nach Abs. 1 Satz 4 unzulässig, es sei denn, es handelt sich um röntgenologische und immunologische Untersuchungen zur Feststellung einer Tuberkuloseerkrankung.

(3) Im Rahmen landeseinheitlicher Impfprogramme sowie von Modellprojekten können mit Zustimmung des Hessischen Ministeriums für Soziales und Integration und des Hessischen Kultusministeriums auch Schutzimpfungen angeboten und mit schriftlicher Einwilligung der in § 100 Abs. 1 des Hessischen Schulgesetzes in der Fassung vom 1. August 2017 genannten Personen durchgeführt werden.

Die zuständigen Gesundheitsämter dürfen nur solche personenbezogenen Daten erheben, die auch für die Durchführung der Untersuchung erforderlich sind. Darüberhinausgehende Daten dürfen nur auf freiwilliger Basis erhoben werden. Dazu erhalten die Erziehungsberechtigten bereits im Vorfeld Fragebogen und Informationsunterlagen.

Das im Jahr 2023 gegründete Hessische Landesamt für Gesundheit und Pflege ist auf mich zugekommen und hat um Beratung bei der Anpassung der bisher eingesetzten Unterlagen gebeten. Für die Abfrage von erforderlichen Informationen im Rahmen der Schuleingangsuntersuchung sollte ein landesweit einheitlicher Erhebungsbogen entwickelt werden.

Welche Daten im Einzelfall wirklich erforderlich sind, ist oft schwer zu beurteilen. Hier kam es bei meiner Beratung insbesondere auf die Frage an, welche Angaben zur Beurteilung der Schulfähigkeit unerlässlich sind.

In konstruktiven Gesprächen mit dem Landesamt konnte ich erreichen, dass in dem von den Eltern auszufüllenden Fragebogen einige Fragen gestrichen oder geändert wurden und das Ausfüllen des Fragebogens mit teilweise sehr sensiblen Angaben freiwillig bleibt. Hier ging es vor allem um Angaben zur Schwangerschaft und Geburt, Fragen zum familiären Umfeld des Kindes und Informationen zu behandelnden Ärzten sowie aktuellen und früheren Erkrankungen.

Zudem habe ich empfohlen, die Informationen zur Datenverarbeitung gemäß Art. 13 und 14 DS-GVO, die dem Elternanschreiben beigefügt werden sollten, in einigen Punkten zu überarbeiten.

Durch mein Einwirken konnten sowohl das Verfahren als auch die verwendeten Unterlagen für die Betroffenen transparenter gestaltet werden. Der freiwillige Fragebogen für die Erziehungsberechtigten wurde darüber hinaus hinsichtlich des Umfangs datenschutzfreundlicher ausgestaltet.

13. Wissenschaft und Forschung

Der Zweck der „wissenschaftlichen Forschung" erfährt von der DS-GVO mehrere Bevorzugungen. Daher ist es sehr wichtig, diesen Begriff zu definieren und abzugrenzen. Dies hat die DSK in einem Positionspapier getan. Diese Klarstellungen führen zu einer einheitlichen Praxis im deutschen Datenschutzrecht (Kap. 13.1). Zum 1. Januar 2025 tritt ein neues Landesstatistikgesetz in Kraft. In diesem sind meine datenschutzrechtlichen Hinweise vollumfänglich berücksichtigt worden (Kap. 13.2).

13.1
Der Begriff der wissenschaftlichen Forschung

Die DSK hat unter meinem Vorsitz ein Positionspapier zum Begriff „wissenschaftliche Forschungszwecke" veröffentlicht. In diesem Positionspapier erläutert die DSK anhand von fünf Kriterien, wann Verarbeitungsvorgänge zu wissenschaftlichen Forschungszwecken erfolgen und dadurch von den entsprechenden Privilegierungen und Einschränkungen der DS-GVO profitieren. Durch diese für den Forschungsbereich wichtigen Klarstellungen können die forschungsrelevanten Bestimmungen der DS-GVO einheitlich angewendet werden.

Hintergrund

Wissenschaftliche Forschung ist für eine Wissensgesellschaft von enormer Bedeutung und kann neben ideellen Vorteilen auch dazu beitragen, Gesundheit, Wachstum und Wohlstand zu sichern. Viele Gebiete der wissenschaftlichen Forschung sind auf die Nutzung personenbezogener Daten angewiesen.

Die DS-GVO erkennt die Bedeutung wissenschaftlicher Forschung an und privilegiert Verarbeitungen zu Zwecken der wissenschaftlichen Forschung durch Ausnahmen von datenschutzrechtlichen Grundsätzen und Einschränkungen von Rechten der betroffenen Personen (z. B. Art. 5 Abs. 1 Buchst. b und e DS-GVO, Art. 14 Abs. 5 Buchst. b DS-GVO und Art. 17 Abs. 3 Buchst. d DS-GVO).

Bisher war es für Verantwortliche nicht einfach zu bestimmen, was unter dem Begriff der „wissenschaftlichen Forschungszwecke" im Sinne der DS-GVO zu verstehen ist und welche Datenverarbeitungen von den entsprechenden Privilegierungen und Einschränkungen profitieren.

Um diese Bewertung zu erleichtern und für mehr Rechtssicherheit zu sorgen, hat die DSK ein Positionspapier zum Begriff „wissenschaftliche Forschungszwecke" veröffentlicht (https://datenschutzkonferenz-online.de/

media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf). Der Arbeitskreis Wissenschaft und Forschung der DSK, dessen Vorsitz ich ausübe, hat das Positionspapier für die DSK erarbeitet.

Kriterien

Nach dem Positionspapier der DSK müssen die folgenden fünf Kriterien erfüllt sein, damit wissenschaftliche Forschungszwecke im Sinne der DS-GVO vorliegen:

I. Methodisches und systematische Vorgehen
II. Erkenntnisgewinn
III. Nachprüfbarkeit
IV. Unabhängigkeit und Selbstständigkeit
V. Gemeinwohlinteresse

Denn nur wenn diese Kriterien gegeben sind, sind die Einschränkungen des Rechts auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) und des Rechts auf Datenschutz nach Art. 8 GRCh zugunsten der Forschungsfreiheit nach Art. 5 Abs. 3 GG und Art. 13 GRCh gerechtfertigt. Die DSK hat sich bei der Bestimmung der Kriterien an der Rechtsprechung des Bundesverfassungsgerichts orientiert (BVerfG, BVerfGE 35, 79, 112 f.; BVerfGE 47, 327, 367), da der EuGH zu dieser Frage noch keine Entscheidungen getroffen hat und die Grundrechte der Charta nach ihrem Art. 52 Abs. 4 im Einklang mit den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ausgelegt werden müssen.

Die Bedeutung der einzelnen Kriterien lässt sich dem Positionspapier entnehmen. Anhand von zwei Beispielfällen möchte ich die Anwendung der Kriterien verdeutlichen.

Beispielfall 1: Entwicklung des autonomen Fahrens

Auch bei der Entwicklung des autonomen Fahrens können Automobilhersteller bei der Verarbeitung personenbezogener Daten wissenschaftliche Forschungszwecke im Sinne der DS-GVO verfolgen. Ob dies tatsächlich der Fall ist, kann aber nur in einer Einzelfallbeurteilung anhand der im DSK-Positionspapier genannten Kriterien festgestellt werden.

Eine Beachtung der Methodik und Standards der jeweiligen Fachdisziplinen bei der Entwicklung des autonomen Fahrens (Ingenieurswesen, Elektrotechnik etc.) spricht für ein methodisches und systematisches Vorgehen (Kriterium I).

Bei Vorhaben, die im vorwettbewerblichen Bereich die Machbarkeit oder einen Demonstrator zum Ziel haben, ist ein wissenschaftlicher Erkenntnisgewinn (Kriterium II) eher zu vermuten als bei Vorhaben, die bereits unmittelbar eine Produktzulassung zum Ziel haben. Eine Einordnung des Vorhabens als „Produktentwicklung" bzw. „Vorserienentwicklung" spricht in diesem Zusammenhang mangels wissenschaftlichen Erkenntnisgewinns gegen wissenschaftliche Forschungszwecke, wohingegen eine „experimentelle Entwicklung" von Systemen des autonomen Fahrens eher hiervon erfasst ist.

Im Rahmen des Kriteriums der Nachprüfbarkeit (Kriterium III) wird man von Entwicklungsvorhaben der Automobilindustrie verlangen, dass die Durchführung und die Ergebnisse des Forschungsvorhabens nach wissenschaftlichen Standards zu dokumentieren sind und im Fall der Verwertung der Ergebnisse auch der Öffentlichkeit zur Diskussion gestellt werden. Hierbei kann es z. B. ausreichend sein, dass ein künstliches neuronales Netz als computerimplementierte Erfindung patentiert wird.

Das Kriterium der Unabhängigkeit und Selbstständigkeit (Kriterium IV) liegt bei Vorhaben der Automobilindustrie dann vor, wenn nicht in einer weisenden Art lenkende Eingriffe in den Forschungsprozess stattfinden, die über eine bloße Kritik hinausgehen.

Das Kriterium des Gemeinwohlinteresses (Kriterium V) schließt nicht solche Vorhaben aus, die eine kommerzielle Vermarktung von Ergebnissen zum Ziel haben. Es müssen jedoch ein gesellschaftlicher Nutzen oder Gemeinwohleffekte vorliegen. Dies ist bei Vorhaben des autonomen Fahrens z. B. dann anzunehmen, wenn die Ergebnisse dazu beitragen, dass die Mobilität von älteren oder leistungseingeschränkten Menschen durch selbstfahrende Autos verbessert wird.

Beispielfall 2: Klinische Studie

In klinischen Studien werden die Wirksamkeit und Verträglichkeit neuer Medikamente und Behandlungen untersucht. Hierbei werden Gesundheitsdaten der Studienteilnehmerinnen und -teilnehmer verarbeitet. Ob dabei wissenschaftliche Forschungszwecke verfolgt werden, ist anhand der konkreten Studie zu untersuchen, kann aber in der Regel angenommen werden.

Die Beachtung des Prüfplans und der Regeln der „guten klinischen Praxis" (*good clinical practice* – GCP) sprechen für ein methodisches und systematisches Vorgehen (Kriterium I).

Klinische Studien sind außerdem die bekannteste Methode zur Erlangung neuer medizinischer Erkenntnisse (Kriterium II).

Im Rahmen des Kriteriums III (Nachprüfbarkeit) wird nicht verlangt, dass eine Veröffentlichung aller Forschungsergebnisse erfolgen muss, allerdings müssen die Durchführung und die Ergebnisse des Forschungsvorhabens nach wissenschaftlichen Standards dokumentiert werden und diese dürfen nicht von vornherein einer Geheimhaltungsabsicht unterliegen. Die Publikation der Studienergebnisse darf daher nicht von Beginn an ausgeschlossen werden, um systematisch eine kritische Überprüfbarkeit im Fachkreis (Peer Review) zu verhindern.

Das Kriterium IV verlangt Unabhängigkeit und Selbstständigkeit der Forschenden, insbesondere auch gegenüber dem Sponsor einer Studie. Sollte der Sponsor einer klinischen Studie, z. B. ein Pharmaunternehmen, Einfluss auf das Ergebnis nehmen oder das Ergebnis bereits vorwegnehmen, fehlt es an der nötigen Unabhängigkeit und Selbstständigkeit des Forschenden und es werden keine wissenschaftlichen Forschungszwecke im Sinne der DS-GVO verfolgt.

Das Kriterium V (Gemeinwohlinteresse) schließt nicht aus, dass auch Vorhaben mit wirtschaftlicher Motivation und finanziellen Interessen wissenschaftliche Forschungszwecke im Sinne der DS-GVO verfolgen können, wenn die Ergebnisse der Allgemeinheit zugutekommen (sollen). Bei der Forschung an neuen Medikamenten im Rahmen klinischer Studien verfolgen Pharmaunternehmen kommerzielle Interessen. Zugleich kann bei klinischen Studien zu neuen Medikamenten aber regelmäßig von einem gesellschaftlichen Nutzen ausgegangen werden, z. B. aufgrund der Bekämpfung oder Vorbeugung von Krankheiten durch den sicheren und bedarfsgerechten Einsatz neuer Medikamente.

Fazit

Das Positionspapier der DSK zum Begriff „wissenschaftliche Forschungszwecke“ schafft Klarheit für den Forschungsbereich und gibt den Verantwortlichen Hilfestellung bei der Bestimmung, ob ihre Verarbeitungsvorgänge wissenschaftliche Forschungszwecke verfolgen. Es kann auch dazu beitragen, im EDSA ein gemeinsames Verständnis des Begriffs „wissenschaftliche Forschungszwecke“ zu entwickeln.

13.2
Änderung des Hessischen Landesstatistikgesetzes

Das Hessische Landesstatistikgesetz, zuletzt geändert durch Gesetz vom 19. September 2016 (GVBl. S. 158), wird zum Ablauf des 31. Dezember 2024 außer Kraft treten (§ 23 HLStatG). Ich habe daher im Rahmen der erforderlichen Evaluierung eine Stellungnahme zum vierten Gesetz zur Änderung des Hessischen Landesstatistikgesetzes abgegeben. Meine Hinweise wurden im Gesetzesvorhaben vollumfänglich berücksichtigt.

Anmerkungen zur geplanten Einschränkung des Auskunftsrechts

Der Gesetzesentwurf sieht in dem neu eingefügten § 2a eine Einschränkung des Auskunftsrechts aus Art. 15 DS-GVO vor. Die Vorschrift orientiert sich am Wortlaut des § 24 Abs. 2 HDSIG:

> *§ 2a HLStatG*
>
> *Das Recht*
>
> *1. auf Auskunft nach Art. 15,*
> *2. auf Berichtigung nach Art. 16,*
> *3. auf Einschränkung der Verarbeitung nach Art. 18 und*
> *4. auf Widerspruch nach Art. 21*
>
> *der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates vom 27. April 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 Nr. L 119 S. 1, Nr. L 314 S. 72, 2018 Nr. L 127 S. 2, 2021 Nr. L 74 S. 35) ist insoweit beschränkt, als dieses Recht voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich macht oder ernsthaft beeinträchtigt und die Beschränkung des Rechts für die Erfüllung dieser Zwecke notwendig ist. Das Recht auf Auskunft nach Art. 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.*

Ich habe darauf hingewiesen, dass zumindest in der Gesetzesbegründung näher ausgeführt werden sollte, wann das Hessische Statistische Landesamt personenbezogene Daten für Zwecke der wissenschaftlichen Forschung verarbeitet und wann ein „unverhältnismäßiger Aufwand“ angenommen werden kann.

Die Voraussetzungen für den Ausschluss des Rechts auf Auskunft nach Artikel 15 DS-GVO wurden daraufhin in der Gesetzesbegründung wie folgt präzisiert:

„Das Statistische Landesamt betreibt insbesondere im Rahmen der methodischen Weiterentwicklung von Statistiken, im Sinn des gesetzlichen Auftrags nach § 2 Abs. 2 Ziffer 2 HLStatG, wissenschaftliche Forschung und führt in diesem Bereich Kooperationen mit Hochschulen durch. Beispiele solcher gemeinsamen Forschungsarbeiten finden sich aktuell in den Bereichen „Fernerkundung", „Geoinformation" und „Neue digitale Daten". Ein „unverhältnismäßiger Aufwand" kann insbesondere dann angenommen werden, wenn ein Forschungsvorhaben mit besonders großen Datenmengen arbeitet oder eine Vielzahl von Auskunftsersuchen vorliegen. Auch für den Fall, dass aufgrund der Art der Speicherung der Daten und der Datenkategorie das Auffinden der betroffenen Person im Datenbestand wesentlich erschwert wird, kann ein unverhältnismäßiger Aufwand vorliegen." (Gesetzesbegründung, Stand 28. September 2023) zu Nr. 3)

Anmerkungen zur geplanten Streichung des Anhörungsverfahrens nach § 6 HLStatG

§ 6 HLStatG regelt die Vergabe statistischer Arbeiten an Dritte. § 6 Abs. 1 Satz 2 sieht dabei eine Anhörung des HBDI vor der Übertragung der Arbeiten vor.

§ 6 HLStatG

(1) Bei der Durchführung von amtlichen Statistiken kann das Statistische Landesamt Arbeiten an Dritte übertragen, sofern sichergestellt ist, dass die Vorschriften zum Schutz personenbezogener Daten und der statistischen Geheimhaltung eingehalten werden. Der Hessische Datenschutzbeauftragte ist vor der Übertragung zu hören. Soweit die Übertragung an nicht öffentliche Stellen erfolgt, ist sicherzustellen, dass der Dritte sich der Kontrolle des Statistischen Landesamtes und des Hessischen Datenschutzbeauftragten unterwirft. § 5 gilt für die Personen, die zur Erledigung der übertragenen Arbeiten eingesetzt werden, entsprechend.

(2) Gemeinden, Landkreise, sonstige Gemeindeverbände und Zweckverbände können unter den in Abs. 1 genannten Voraussetzungen einzelne Arbeiten an Dritte übertragen. Der örtliche Datenschutzbeauftragte ist vor der Übertragung zu hören.

Der Gesetzesentwurf sah zunächst die Streichung und Ersetzung der Norm vor. Dies wurde damit begründet, dass die Auftragsdatenverarbeitung in Art. 28 DS-GVO geregelt sei. Diese Regelung komme unmittelbar zur Anwendung. Eine die DS-GVO wiederholende Regelung sei zudem nicht zulässig.

Dem habe ich widersprochen. Auch wenn Art. 28 DS-GVO unmittelbar Anwendung findet, ist es dem nationalen Gesetzgeber auf Grundlage der Öffnungsklauseln des Art. 6 Abs. 3 und Abs. 2 DS-GVO möglich, spezifischere Bestimmungen zur Auftragsverarbeitung im öffentlichen Bereich zu treffen. Die Vorgaben des § 6 HLStatG, als weitere konkretisierende Maßnahmen, können daher bestehen bleiben. Mit dem Wegfall der Vorschrift könnten private Stellen als Auftragsverarbeiter außerhalb meines Zuständigkeitsbereichs

beauftragt werden, deren Tätigkeit nicht mehr von mir unmittelbar überprüft werden kann. Die Streichung der Regelung hätte eine Abschwächung des bisherigen Datenschutzniveaus und eine Einschränkung meiner Befugnisse bedeutet. Von einer Streichung wurde im Ergebnis abgesehen.

Anmerkungen zur geplanten Regelung zur Nutzung von „Webscraping“

Der Gesetzentwurf sieht nun im bisher aufgehobenen § 3 eine Regelung zum sog. „Webscraping“ vor:

> *§ 3 HLStatG*
>
> *Das Statistische Landesamt darf zu Zwecken der Statistikerstellung und zur methodischen Weiterentwicklung der Statistik allgemein zugängliche Daten durch den Einsatz automatisierter Abrufverfahren erheben.*

Der Bedarf für die Normierung wird wie folgt begründet:

> „Die Nutzung von Webscraping im Rahmen von ‚Neuen Digitalen Daten‘ soll ausdrücklich erlaubt werden, um künftig schneller aktuelle Daten bereitstellen zu können. Um testen zu können, ob neue digitale Datenquellen für die amtliche Statistik geeignet sind, bedarf es eines besseren Zugangs zu Daten für Eignungsprüfungen, als dies aktuell der Fall ist. Gegenwärtig sind die statistischen Ämter hier nämlich auf die Kooperationsbereitschaft einzelner Unternehmen und Institutionen angewiesen, denn eine ausdrückliche Erlaubnisnorm für den Einsatz von Webscraping gibt es bislang nicht. Um neue digitale Daten nach positiver Eignungsprüfung in die amtliche Statistikproduktion überführen zu können, sind rechtliche Regelungen darüber hinaus zwingend erforderlich. Sobald das Verfahren flächendeckend eingesetzt und getestet wurde, kann nämlich nicht mehr lediglich von einer Weiterentwicklung der Methoden gesprochen werden, so dass es aus Gründen der Rechtssicherheit einer entsprechenden gesetzlichen Verankerung bedarf. Eine entsprechende Regelung führt zudem auch zur Entlastung von Auskunftspflichtigen.“ (Gesetzesbegründung zu Nr. 4, Stand 28.09.2023)

Diese Neuregelung wurde von mir ausdrücklich begrüßt. Mit dieser neuen Rechtsgrundlage wird die bisher unsichere Rechtslage beendet. Es ergaben sich insoweit in der Vergangenheit datenschutzrechtliche Fragen hinsichtlich der Erhebung personenbezogener Daten und deren weiterer Verarbeitung mit dieser Methode.

14. Technik und Organisation

Die Umsetzung des Datenschutzrechts setzt geeignete Techniken für Verantwortliche und betroffene Personen sowie passende und leistungsfähige Organisationsstrukturen und -verfahren voraus. Diese Voraussetzungen zu ermöglichen, zu überprüfen und durchzusetzen, ist eine wichtige Aufgabe jeder Datenschutzaufsichtsbehörde. Soweit dies möglich, beraten wir z. B. zur Auswahl, zur Gestaltung und zum Einsatz von Software und IT-Diensten (Kap. 14.1), zu angemessenen technischen und organisatorischen Maßnahmen entsprechend der Empfehlungen des EDSA (Kap. 14.2), zum Löschen und Vernichten nicht mehr benötigter Daten (Kap. 14.3) sowie zu software-gestützter Schwärzung von PDF-Dateien (Kap. 14.4). Zur technischen Überprüfung von Websites kommen neue Prüftools zum Einsatz (Kap. 14.5). Überprüft wurden z. B. der Software-Einsatz bei hessischen Gesundheitsämtern (Kap. 14.6). Datenschutzverletzungen sind mir als Aufsichtsbehörde zu melden (Kap. 14.7). Eine wichtige Ursache für Datenschutzverletzungen kann in unangemessenen und nicht notwendigen Berechtigungen bei Android-Apps liegen (Kap. 14.8). Auffällig oft wurden Fehladressierung von E-Mails aus der Hessischen Landesverwaltung gemeldet (Kap. 14.9)

14.1
Software und IT-Dienste als Beratungsgegenstand

Mich erreichen häufig Anfragen, die auf meine grundlegende Beurteilung einer bestimmten Software oder eines bestimmten IT-Dienstes gerichtet sind. Derartige Anfragen kann ich aus unterschiedlichen Gründen in aller Regel nicht wie von den Anfragenden gewünscht beantworten. In diesem Kapitel gehe ich näher auf die Hintergründe ein und stelle den Bezug zu meinem Beratungsangebot her.

Hintergrund

Eine wichtige Aufgabe meiner Behörde ist, wie in Art. 57 Buchst. b, c und d DS-GVO angedeutet, die Beratung von datenschutzrechtlich Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO und Auftragsverarbeitern gemäß Art. 4 Nr. 8 DS-GVO. Auf den hierbei in der Abteilung für technischen und organisatorischen Datenschutz meiner Behörde verfolgten Beratungsansatz bin ich bereits in meinem 52. Tätigkeitsbericht zum Datenschutz in Kap. 14.2 *Beratung zum technisch-organisatorischen Datenschutz* näher eingegangen.

Besonders die beratende Unterstützung im Rahmen von IT-Projekten bildet hierbei einen wichtigen Schwerpunkt. Dies gilt vor allem auch deshalb, weil im Rahmen von derartigen Projekten häufig das Fundament für die Verarbeitung

personenbezogener Daten gelegt wird. Gerade hier können richtungsweisende Weichen für einen datenschutzrechtskonformen und darüber hinaus auch datenschutzfreundlichen Einsatz von IT gestellt werden. Gleichzeitig können Fehler vermieden werden, die ansonsten zu datenschutzrechtlichen Verstößen führen können und deren nachgelagerte Behebung mindestens mit erheblichen Aufwänden und Verzögerungen verbunden wäre. Dementsprechend begrüße ich es sehr, wenn sich Verantwortliche und Auftragsverarbeiter bei Beratungsbedarf in IT-Projekten möglichst frühzeitig an mich wenden. Weiterführende Informationen zur Bedeutung einer frühzeitigen, durchgängigen und umfassenden Integration des Datenschutzes in IT-Projekte können u. a. in Kap. 3.2 *Digitale Souveränität und erfolgreiche Digitalisierungsprojekte* meines 50. Tätigkeitsberichts zum Datenschutz gefunden werden.

Vielfach erreichen mich Anfragen von Verantwortlichen und Auftragsverarbeitern, die von mir eine dahingehende Einschätzung wünschen, ob eine bestimmte Software oder ein bestimmter IT-Dienst datenschutzrechtskonform eingesetzt werden kann. Häufig enthält eine solche Anfrage keine oder nur äußerst allgemeine Angaben zu etwaigen Einsatzszenarien. Nicht selten sind die betroffenen Softwareprodukte und IT-Dienste jedoch für unterschiedliche Zwecke einsetzbare Systeme, z. B. für Textverarbeitung, Videokonferenzen oder Cloud-basierte Kollaboration. Zusammengenommen kann die Antwort in aller Regel nur lauten: „Es kommt darauf an." Worauf es ankommt und warum die Beantwortung dieser Frage durch den Fragesteller selbst erfolgen muss, werde ich im Folgenden erläutern. Hierbei gehe ich als Voraussetzung davon aus, dass die avisierte Verarbeitung personenbezogener Daten rechtmäßig erfolgen kann und insbesondere die Anforderungen des Art. 6 DS-GVO erfüllt sind. Eine diesbezügliche rechtliche Betrachtung wird in diesem Beitrag nicht weiter erfolgen.

Anforderungen an die Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten durch datenschutzrechtlich Verantwortliche muss den Anforderungen der DS-GVO genügen. Zur Umsetzung dieser Anforderungen und zum Nachweis müssen Verantwortliche gemäß Art. 24 Abs. 1 DS-GVO geeignete technische und organisatorische Maßnahmen (TOM) ergreifen.

Bei der Ausgestaltung und Nutzung der zur Verarbeitung personenbezogener Daten eingesetzten Technik müssen Verantwortliche gemäß Art. 25 DS-GVO ihre Systeme so gestalten, dass sie die Grundsätze des Datenschutzes gemäß Art. 5 Abs. 1 DS-GVO wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufnehmen, um den Anforderungen der DS-

GVO zu genügen. Auch sind Verantwortliche gemäß Art. 5 Abs. 2 DS-GVO hinsichtlich der Einhaltung dieser Anforderungen rechenschaftspflichtig.

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");

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung");

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit");

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung");

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"); (…)

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht").

Neben dem Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 DS-GVO müssen Verantwortliche und zusätzlich auch Auftragsverarbeiter gemäß Art. 32 DS-GVO ein besonderes Augenmerk auf die Sicherheit der Verarbeitung personenbezogener Daten richten. Hierzu müssen sie gemäß Art. 32 Abs. 1 DS-GVO geeignete technisch-organisatorische Maßnahmen (TOM) umsetzen.

In Art. 24, 25 und 32 DS-GVO werden jeweils Rahmenbedingungen vorgegeben, unter deren Berücksichtigung die Systemgestaltung, die Konfiguration, die Auswahl und die Umsetzung der jeweiligen TOM erfolgen müssen.

Art. 24 Abs. 1 DS-GVO

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um (…)

Art. 25 Abs. 1 DS-GVO

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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen (…).

Art. 32 Abs. 1 DS-GVO

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 (…).

Bei der Systemgestaltung der Ergreifung und Umsetzung von TOM muss folglich immer der konkrete Kontext der geplanten Verarbeitung personenbezogener Daten berücksichtigt werden, insbesondere hinsichtlich der zur Verarbeitung einsetzbaren Technik, der Spezifika und Rahmenbedingungen der Verarbeitung selbst sowie der Risiken für Rechte und Freiheiten der von der Verarbeitung ihrer Daten betroffenen Personen. Auch reicht es nicht aus, dass Verantwortliche und Auftragsverarbeiter einmalig einen datenschutzrechtskonformen Zustand herstellen. Sie müssen diesen auch aufrechterhalten und hierzu geeignete Prozesse zur regelmäßigen und anlassbezogenen Überprüfung, Evaluation, Bewertung und ggf. Anpassung der Systemgestaltung und der ergriffenen TOM etablieren.

Dokumentationen der Verarbeitungstätigkeiten

Gemäß Art. 4 Nr. 2 DS-GVO ist der Begriff der „Verarbeitung“ personenbezogener Daten wie folgt definiert

Art. 4 Nr. 2 DS-GVO

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

Vor dem Hintergrund der bisherigen Ausführungen müssen von Verantwortlichen folglich für Verarbeitungsvorgänge bzw. für Vorgangsreihen unter Berücksichtigung des jeweiligen Verarbeitungskontextes Gestaltungsmaßnahmen und TOM ergriffen werden, um die Anforderungen der DS-GVO zu erfüllen. Die isolierte Betrachtung einzelner Vorgänge dürfte zu feingranular, ineffizient und ggf. sogar ineffektiv sein. Stattdessen sollten zusammengehörige Verarbeitungsvorgänge auch zusammengefasst und in ihrem gemeinsamen Kontext betrachtet werden. Hierbei sollten allerdings die Spezifika der einzelnen Verarbeitungsvorgänge bei der Betrachtung nicht außer Acht gelassen werden.

Für die zielführende Zusammenfassung von Verarbeitungsvorgängen zur gemeinsamen Betrachtung sieht Art. 30 DS-GVO ein Verzeichnis der Verarbeitungstätigkeiten vor. Verantwortliche und Auftragsverarbeiter müssen ein solches Verzeichnis führen, das für sämtliche Verarbeitungstätigkeiten in ihrer jeweiligen Zuständigkeit separate Einträge mit gesetzlich vorgegebenen Mindestinformationen enthält.

In Erwägungsgrund 82 DS-GVO ist als Zweck des Verzeichnisses der Verarbeitungstätigkeiten der Nachweis der Einhaltung der DS-GVO genannt. Auch wird explizit darauf hingewiesen, dass die zuständige Datenschutzaufsichtsbehörde Verarbeitungsvorgänge anhand des Verzeichnisses kontrollieren können soll. Dies muss bei der Führung des Verzeichnisses entsprechend berücksichtigt werden.

ErwGr 82 DS-GVO

Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen. Jeder Verantwortliche und jeder Auftragsverarbeiter sollte verpflichtet sein, mit der Aufsichtsbehörde zusammenzuarbeiten und dieser auf Anfrage das entsprechende Verzeichnis vorzulegen, damit die betreffenden Verarbeitungsvorgänge anhand dieser Verzeichnisse kontrolliert werden können.

Mit Art. 30 DS-GVO ist folglich ein Rahmen zur Dokumentation und zum Nachweis der datenschutzrechtskonformen Ausgestaltung von Verarbeitungstätigkeiten gegeben. Der Begriff der Verarbeitungstätigkeit selbst ist jedoch in der DS-GVO nicht definiert. Hierzu kann das Standard-Datenschutzmodell (SDM) der DSK (https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/) herangezogen werden, das auch vom IT-Planungsrat und vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen wird. In Version 3.1 des SDM wird in Kapitel D2.1 auf die Zusammenhänge zwischen elementaren Verarbeitungsvorgängen, Vorgangsreihen und Verarbeitungstätigkeiten eingegangen. Hierbei wird eine Analogie zu in den in anderen Kontexten verwendeten Begriffen „Verfahren“ und „Geschäftsprozess“ auf der einen und „Verarbeitungstätigkeiten“ auf der anderen Seite für den Fall hergestellt, dass personenbezogene Daten verarbeitet werden.

Rolle von Software und IT-Diensten

Der Begriff „Software“ ist nicht einheitlich definiert. Für die Betrachtung in diesem Beitrag wird davon ausgegangen, dass es sich bei Software um ein Programm oder eine zusammengehörige Menge von Programmen handelt. Ergänzt wird Software um Dokumentationen und sonstige Informationen, die der Konfiguration, dem Betrieb und der Nutzung von Software dienen.

Software selbst kann folglich nicht unmittelbar für Verarbeitungstätigkeiten eingesetzt werden. Hierzu muss zunächst ein Betriebskonzept festgelegt und umgesetzt werden. Abhängig von der konkreten Ausgestaltung der betrachteten Software stehen Verantwortlichen hierzu verschiedene Optionen zur Verfügung. So können sie eine Software bspw. in ihrer eigenen IT-Infrastruktur selbst „on premise“ betreiben. Dieses Betreibermodell dürfte Verantwortlichen grundsätzlich das höchste Maß an Kontrolle bieten. Auch dürfte der Gestaltungsspielraum hinsichtlich des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 DS-GVO und allgemein hinsichtlich der Ausgestaltung von TOM tendenziell am größten sein. Auf der anderen Seite müssen Verantwortliche bei diesem Betreibermodell alle erforderlichen personellen und infrastruk-

turellen Ressourcen für den Betrieb selbst vorhalten und bereitstellen. Als alternatives Betreibermodell kann auf Auftragsverarbeiter zurückgegriffen werden, welche die jeweilige Software gemäß den Vorgaben des Verantwortlichen bereitstellen. So können Verantwortliche sich die Expertise und die Ressourcen des jeweiligen Auftragsverarbeiters zunutze machen, müssen sich aber gleichzeitig auf das Angebot des Auftragsverarbeiters einstellen. Schließlich können Verantwortliche mittlerweile auch häufig auf weitgehend standardisierte Cloud-basierte Angebote zurückgreifen. So sind etwa standardisierte Software-as-a-Service-Angebote (SaaS) für Büro-Anwendungen, Videokonferenzsysteme oder Kollaborationswerkzeuge am Markt verfügbar. Gerade beim letzteren Betreibermodell verschwimmen die Grenzen zwischen Software und IT-Dienst oder -Service.

Nicht unerwähnt bleiben darf in diesem Zusammenhang, dass im Rahmen der Nutzung von Software in Form von Anwendungen und IT-Diensten sowie beim Rückgriff auf IT-Dienste von Auftragsverarbeitern eine umfassende Betrachtung der Verarbeitung personenbezogener Daten erfolgen muss. Mit zunehmender Vernetzung und i. d. R. dauerhafter Verbindung heutiger IT-gestützter Arbeitsplätze mit dem Internet ist bspw. eine mehr oder minder regelmäßige Kommunikation zwischen Anwendungen und IT-Diensten auf der einen und ihren Anbietern auf der anderen Seite nicht unüblich. Die Gründe hierfür sind vielfältig und reichen von Lizenzprüfungen und der Prüfung des Vorliegens von Updates über die Einbindung von Cloud-basierten Diensten bis hin zur Übermittlung von Informationen zu Programmabstürzen und Diagnosedaten zur Produktverbesserung. All diese und etwaige weitere Verarbeitungen personenbezogener Daten müssen entweder unterbunden oder datenschutzrechtskonform ausgestaltet werden.

Einsatz als Mittel zur Verarbeitung personenbezogener Daten

Vor dem Hintergrund der vorangegangenen Ausführungen sind Dienste und Anwendungen Mittel zur Verarbeitung personenbezogener Daten. Sie stellen maßgebliche Teile des Fundaments dar, auf dem aufbauend TOM ergriffen und letztendlich personenbezogene Daten verarbeitet werden. In Erwägungsgrund 78 DS-GVO wird in diesem Zusammenhang auf die besondere Rolle von Herstellern von Produkten, Diensten und Anwendungen hingewiesen. Sie werden aufgefordert, insbesondere bei der Entwicklung und Gestaltung sicherzustellen, dass Verantwortliche und Auftragsverarbeiter bei der späteren Nutzung ihren datenschutzrechtlichen Pflichten überhaupt nachkommen können.

Hersteller oder Anbieter legen durch die Ausgestaltung von Software und IT-Diensten somit maßgeblich den Rahmen zur Erfüllung datenschutzrecht-

licher Pflichten gemäß der Art. 24, 25 und 32 DS-GVO für nutzende Verantwortliche fest. Umgekehrt nehmen Verantwortliche bereits bei der Auswahl von Software und IT-Diensten wesentliche Weichenstellungen vor. In Bezug auf Art. 25 Abs. 1 DS-GVO handelt es sich hierbei um Festlegungen der Mittel zur Verarbeitung personenbezogener Daten. Weitergehende Erläuterungen hierzu und eine Einordnung in den übergeordneten Kontext der Digitalen Souveränität können in Kap. 2 *Digitale Souveränität und Datenschutz* meines 51. Tätigkeitsberichts zum Datenschutz gefunden werden.

Ausgehend vom Betrachtungsgegenstand einer einzelnen Verarbeitungstätigkeit besteht diese im Wesentlichen aus einer Folge einzelner Verarbeitungsvorgänge oder Vorgangsreihen. Zur Durchführung dieser dienen die bereits im Zusammenhang mit Art. 25 DS-GVO referenzierten Mittel der Verarbeitung. IT-Systeme und Dienste sowie Anwendungen stellen hierbei nur eine Teilmenge der eingesetzten Mittel dar. Eine differenzierte Betrachtung der Struktur von Verarbeitungstätigkeiten, der Ebenen der Verarbeitung personenbezogener Daten und der Rolle von Anwendungen, IT-Diensten und IT-Systemen findet sich in Kap. D2 des DSM, Version 3.1.

Aus der Perspektive eines einzelnen Dienstes oder einer einzelnen Anwendung kann es umgekehrt sein, dass dieser oder diese für mehrere unterschiedliche Verarbeitungstätigkeiten zum Einsatz kommt. Besonders häufig ist dies bei Anwendungen der Fall, die vielfältig nutzbare Basisfunktionalitäten bereitstellen, z. B. Büroanwendungen wie Textverarbeitungen und Tabellenkalkulationen. Auch Kommunikationsinfrastrukturen wie E-Mail-Dienste und Videokonferenzsysteme sowie Dienste zur Datei- und Dokumentenverwaltung werden von datenschutzrechtlich Verantwortlichen häufig für unterschiedlichste Zwecken zur Verarbeitung personenbezogener Daten eingesetzt.

Gerade am Beispiel des Kommunikationsmediums E-Mail lässt sich verdeutlichen, dass für die Nutzung einer solchen Infrastruktur in unterschiedlichen Kontexten unterschiedliche Anforderungen zu erfüllen und unterschiedliche Rahmenbedingungen zu berücksichtigen sind. Sollen bspw. innerhalb einer Organisation sensible personenbezogene Daten per E-Mail übermittelt werden, für die ein hohes Schutzniveau hinsichtlich Vertraulichkeit zu gewährleisten ist, so muss hierzu höchstwahrscheinlich eine wirksame Inhaltsverschlüsselung etabliert werden. Die hierzu nötigen infrastrukturellen Maßnahmen dürften organisationsintern umsetzbar sein. Demgegenüber dürfte der Einsatz einer Inhaltsverschlüsselung beim Versand allgemeiner Newsletter mit unverfänglichen und nicht personenspezifischen Inhalten nicht unbedingt erforderlich sein. Auch dürfte die Umsetzung einer entsprechenden Infrastruktur für jeden einzelnen Empfänger nicht in jedem Fall praktikabel sein. Weiterführende Ausführungen zum Einsatz von E-Mail für die Übermittlung personenbezogener

Daten können dem Kap. 14.1 *Übermittlung personenbezogener Daten per E-Mail* meines 49. Tätigkeitsberichts zum Datenschutz entnommen werden.

Für Betriebsmittel wie Anwendungen und IT-Dienste, die im Rahmen mehrerer verschiedener Verarbeitungstätigkeiten eingesetzt werden, bietet sich zunächst eine von den einzelnen Verarbeitungstätigkeiten losgelöste Betrachtung an. In deren Rahmen könnten zunächst die Spezifika, Rahmenbedingungen und sonstigen relevanten Aspekte zentral, konsistent und redundanzfrei dokumentiert und fortgeschrieben werden. Auch könnten relevante Bezüge zu weiteren Bereichen aufrechterhalten und verwaltet werden, etwa zu IT-Betrieb und Informationssicherheit. Bezogen auf Verarbeitungstätigkeiten, in deren Kontext das betrachtete Betriebsmittel zum Einsatz kommt, sollten sodann entsprechende Referenzen in beiden Richtungen vorgehalten werden. Hierdurch wird es möglich, im Falle relevanter Änderungen und bei Handlungsbedarf die Reichweite zu ermitteln und umfassend zu reagieren. Die Festlegung der konkreten TOM erfolgt auf Ebene der Verarbeitungsvorgänge, insbesondere wenn vorgangsspezifische Maßnahmen erforderlich sind. Eine entsprechende Dokumentation sollte zur Umsetzung der Nachweispflicht erfolgen.

Die Frage nach einem datenschutzrechtskonformen Einsatz

Die Ausgangsfrage nach dem etwaigen datenschutzrechtskonformen Einsatz einer Software oder eines IT-Dienstes kann folglich nicht losgelöst von den Verarbeitungstätigkeiten beantwortet werden, zu deren Umsetzung die jeweilige Software oder der jeweilige IT-Dienst eingesetzt werden soll. Auch sind die spezifischen Eigenschaften der Software oder des IT-Dienstes sowie Rahmenbedingungen für den geplanten Einsatz zu berücksichtigen. Hinzu kommen rechtliche Fragestellungen.

Insgesamt kann ich die Frage nach einem etwaigen datenschutzrechtskonformen Einsatz einer Software oder eines IT-Dienstes daher in aller Regel nur an den Anfragenden zurückgeben. Die Ermittlung, Bewertung und Beurteilung aller relevanter Faktoren und Optionen sind ein komplexer Prozess, der im Rahmen von Einführungsprojekten zu den Kernaufgaben und letztendlich auch zur Kernverantwortung eines datenschutzrechtlich Verantwortlichen gehören. Die Übernahme dieser Aufgabe durch mich würde meiner Rolle als Aufsichtsbehörde widersprechen.

Auch allgemeine Aussagen zu einzelnen Softwareprodukten und IT-Diensten sind mir nicht möglich. Diese müssten unterschiedlichste Konstellationen berücksichtigen und detaillierte Annahmen zu Rahmenbedingungen des etwaigen Einsatzes unterstellen. Die Aufstellung, Prüfung, Bewertung und Beurteilung derartiger Einsatzszenarien würde die Kapazitäten meiner Behörde übersteigen. Dies gilt umso mehr, da die Einsatzszenarien und somit

die Aussagen zum Einsatz von Software oder IT-Diensten fortgeschrieben und aktuell gehalten werden müssten.

Eine Ausnahme hiervon stellten vermeintlich die Festlegung der DSK zum datenschutzrechtskonformen Einsatz von Microsoft 365 vom 24. November 2022 (https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf) und die zugehörige *Zusammenfassung der Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung* der *AG Microsoft-Onlinedienste* der DSK dar. Hierzu ist jedoch festzuhalten, dass gerade keine umfassende Betrachtung von Software und IT-Diensten erfolgt ist. Stattdessen hat sich die Arbeitsgruppe mit ausgewählten rechtlichen Fragestellungen auseinandergesetzt und bereits für diese festgestellt, dass eine datenschutzrechtskonforme Nutzung des Betrachtungsgegenstands unter den spezifischen Rahmenbedingungen nicht möglich sein dürfte. Eine derartige Negativaussage hinsichtlich des datenschutzrechtskonformen Einsatzes ist prinzipbedingt erheblich einfacher möglich als eine Positivaussage. Denn schließlich muss für eine Negativaussage nur mindestens ein Verhinderungsgrund vorliegen, während für eine Positivaussage die vollumfängliche Abwesenheit derartiger Gründe belegt werden müsste.

Fazit

Die Auswahl von Software und IT-Diensten im Rahmen der Festlegung der Mittel zur Verarbeitung personenbezogener Daten ist eine komplexe und nicht selten auch komplizierte Aufgabe. Hierbei müssen vielfältige Anforderungen aus unterschiedlichen Bereichen und vielschichtige Rahmenbedingungen berücksichtigt werden. Auch ist es mit der einmaligen Festlegung auf ein spezifisches Produkt und der nachfolgenden Ergreifung von Maßnahmen nicht getan. Stattdessen muss der datenschutzrechtskonforme Einsatz im Kontext aller betroffenen Verarbeitungstätigkeiten dauerhaft gewährleistet werden. Hierzu sind entsprechende Prozesse des Datenschutzmanagements zu etablieren, die eine regelmäßige und anlassbezogene Überprüfung, Evaluation, Bewertung und Umsetzung von Anpassungsbedarf sicherstellen.

Ich kann datenschutzrechtlich Verantwortlichen ihre Verantwortung bei der Festlegung der Mittel zur Verarbeitung personenbezogener Daten nicht abnehmen. Meine Mitarbeitenden stehen jedoch hinsichtlich des methodischen Vorgehens und in der Folge auch bei spezifischen Fragestellungen beratend zur Verfügung. Eine wesentliche Voraussetzung hierfür ist jedoch, dass ein anfragender Verantwortlicher im Rahmen des IT-Projekts durchgängig und in ausreichendem Umfang Datenschutzexpertise bereitstellen muss, um die datenschutzrechtlichen Anforderungen umzusetzen. Denn dies obliegt

dem Verantwortlichen selbst und ist nicht Teil der Beratung durch meine Mitarbeitenden.

Datenschutzrechtlich Verantwortliche sind jedoch nicht zwangsläufig auf sich allein gestellt. Gerade bei Software und IT-Diensten, die ein breites Spektrum an Einsatzszenarien unterstützen, ist zu erwarten, dass nicht selten mehrere Verantwortliche vor ähnlichen Herausforderungen stehen. Hier würde es sich anbieten, dass nicht jeder Verantwortliche einzeln „das Rad neu erfindet". Hier könnte es lohnenswert sein, Kooperationsmöglichkeiten zu prüfen und ggf. Synergien zu nutzen. Diesen Ansatz spreche ich nicht selten auch im Rahmen meiner Beratung an, insbesondere im öffentlichen Bereich.

14.2
Angemessene technische und organisatorische Maßnahmen

Im Rahmen meiner aufsichtsbehördlichen Begleitung von gemeldeten Datenschutzverletzungen fragen Verantwortliche häufig nach empfohlenen technischen oder organisatorischen Maßnahmen (TOM), um vergleichbare Vorfälle in Zukunft verhindern zu können. Eine konkrete Auskunft ist im Rahmen der Begleitung grundsätzlich nicht möglich, da die Antwort immer von den jeweiligen Umständen und Umgebungen abhängt. Hilfe zur Selbsthilfe können aber die Leitlinien 01/2021 des EDSA geben, in der u. a. empfehlenswerte Maßnahmen für eine Auswahl an typischen Vorfällen zusammengefasst sind, die Verantwortliche kennen und berücksichtigen sollten. Weitere Quellen können auch das Standard-Datenschutzmodell oder der IT-Grundschutz des BSI sein.

Der Bedarf an Empfehlungen

Durch Datenschutzverletzungen können Risiken für die Rechte und Freiheiten natürlicher Personen entstehen. Um dies zu vermeiden, verpflichtet die DS-GVO Verantwortliche und Auftragsverarbeiter, mittels technischer und organisatorischer Maßnahmen ein angemessenes Schutzniveau zu gewährleisteten. Kommt es dennoch zu einer Verletzung des Schutzes personenbezogener Daten, so muss ein Verantwortlicher mit Sitz in Hessen diese gem. Art. 33 Abs. 1 DS-GVO meiner Behörde melden, sofern mindestens ein Risiko für Rechte und Freiheiten betroffener Personen besteht. Als Teil seiner Meldung muss ein Verantwortlicher u. a. darlegen, wie es zu dem Vorfall kommen konnte. Gerade bei schweren Vorfällen in Zusammenhang mit der Informationstechnik (IT), wie etwa Angriffe auf IT-Systeme oder Dienste, zeigt sich häufig, dass vermeidbare Defizite bei den bisher getroffenen technischen und organisatorischen Maßnahmen die Vorfälle begünstigten oder überhaupt erst ermöglichten.

In meinem 52. Tätigkeitsbericht habe in Kap. 14.4 erläutert, wie meine Behörde Verantwortliche bei der Behandlung von Datenschutzverletzungen begleitet. Ein wichtiger Aspekt ist sicherzustellen, dass die Verantwortlichen bzw. deren Auftragsverarbeiter aus einem Vorfall lernen und die bisher getroffenen Maßnahmen überprüfen, bewerten, evaluieren sowie bei Bedarf anpassen und ergänzen. Dies ist notwendig, um ein dem Risiko angemessenes Schutzniveau herstellen zu können. Im Dialog mit den Verantwortlichen kommen verständlicherweise häufig die Fragen auf, welche technischen und organisatorischen Maßnahmen angemessen und ausreichend sind und welche Empfehlungen ich allgemein geben würde.

Anforderungen zu technischen und organisatorischen Maßnahmen

Die Anforderung an die Verarbeiter von personenbezogenen Daten, mittels geeigneter technischer und organisatorischer Maßnahmen eine angemessene Sicherheit der Verarbeitung zu gewährleisten, gehört gem. Art. 5 Abs. 1 Buchst. f DS-GVO bereits zu den Grundsätzen der Verarbeitung von personenbezogenen Daten. Die Verantwortung für die Umsetzung geeigneter Maßnahmen wird im Art. 24 DS-GVO dem Verantwortlichen zugewiesen. Sie trifft ebenso Auftragsverarbeiter, so dass Art. 28 DS-GVO Vorgaben für Zuständigkeiten und vertragliche Regelungen enthält. Die Anforderungen an den Verantwortlichen und den Auftragsverarbeiter, die Sicherheit der Verarbeitung zu gewährleisten, werden im Art. 32 DS-GVO wie folgt konkretisiert:

Art. 32 Abs. 1 und 2 DS-GVO

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

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

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

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

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

(2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte

Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

Durch die Erfassung und weitere Verarbeitung von personenbezogenen Daten entstehen Risiken für natürliche Personen, wenn z. B. die Vertraulichkeit der Daten verletzt wird, also die Daten unberechtigten Dritten zugänglich werden. Bei der Bewertung des Risikos werden sowohl die Schwere eines möglichen Schadens als auch die Wahrscheinlichkeit des Auftretens berücksichtigt. Das Ziel bei der Auswahl und Umsetzung geeigneter technischer und organisatorischer Maßnahmen ist es, die Wahrscheinlichkeit und die Schwere eines möglichen Schadens soweit zu reduzieren, dass ein angemessenes Schutzniveau für die personenbezogenen Daten gewährleistet ist. Dabei sollen die Maßnahmen dem Stand der Technik entsprechen.

Der technologische Fortschritt impliziert in diesem Zusammenhang, dass sich der Stand der Technik ebenfalls weiterentwickelt. Dementsprechend müssen auch die Eignung und Angemessenheit von technischen und organisatorischen Maßnahmen regelmäßig und anlassbezogen überprüft werden. Neue Technologien und Erkenntnisse, entdeckte Schachstellen und sich verändernde Bedrohungsszenarien machen eine kontinuierliche Kontrolle und Anpassung notwendig. Diesem Umstand wird mit Maßnahmen an Verantwortliche und Auftragsverarbeiter in Art. 32 Abs. 1 Buchst. d DS-GVO Rechnung getragen. Mittels eines geeigneten Verfahrens sollen die Verantwortlichen und Auftragsverarbeiter regelmäßig die Wirksamkeit der umgesetzten Maßnahmen überprüfen, bewerten und evaluieren. Ist im Ergebnis ein dem Risiko angemessenes Schutzniveau nicht mehr gewährleistet, sind Anpassungen notwendig, um die Anforderung des Art. 32 DS-GVO wieder zu erfüllen.

Die DS-GVO ist technikneutral formuliert. Sie schreibt Verantwortlichen und Auftragsverarbeitern vor, dass diese ein dem Risiko angemessenes Schutzniveau gewährleisten müssen, aber nicht mittels welcher spezifischen Maßnahmen dies erfolgen muss oder kann. Daher kann die Frage, welche konkrete Ausgestaltung technischer und organisatorischer Maßnahmen für einen Anwendungsfall geeignet und angemessen ist, nicht pauschal beantwortet werden. Eine vollständige Prüfung und abschließende Bewertung von getroffenen Maßnahmen oder auch die konkrete Empfehlung von geeigneten Maßnahmen im Rahmen von Art. 33-Verfahren oder Beratungen zu konkreten Lösungen sind daher durch meine Behörde grundsätzlich nicht möglich.

Für die Auswahl der technischen und organisatorischen Maßnahmen nennt die DS-GVO u. a. in den Art. 24, 25 und 32 DS-GVO konkret Aspekte, die

zu berücksichtigen sind. Hierzu gehören generell die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung personenbezogener Daten und der damit einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen. Nach Art. 32 Abs. 1 DS-GVO sind für die Gewährleistung eines dem Risiko angemessenen Schutzniveaus auch der Stand der Technik und die Implementierungskosten zu berücksichtigen. Durch die Umsetzung der Maßnahmen sollen Verantwortliche nach Art. 24 Abs. 1 DS-GVO sicherstellen, dass die Verarbeitung gemäß dieser Verordnung erfolgt und sie dafür auch den Nachweis erbringen können. Dabei müssen nach Art. 24 Abs. 2 DS-GVO die technischen und organisatorischen Maßnahmen auch geeignete Datenschutzvorkehrungen umfassen, sofern diese in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten stehen. Weiterhin sind gemäß Art. 25 Abs. 1 DS-GVO Maßnahmen auszuwählen, die auf die Umsetzung der Datenschutzgrundsätze ausgelegt sind und die Rechte der betroffenen Personen schützen.

Die Empfehlungen des Europäischen Datenschutzausschusses

Der EDSA hat in seinen Leitlinien 01/2021 zu „Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten“ (Version 2.0) für eine Auswahl an typischen Fällen mögliche Risiken für betroffene Personen und die aus Sicht des Datenschutzes zu erwartende Reaktion von Verantwortlichen beispielhaft dargestellt und erläutert. Für die in den Leitlinien betrachteten Kategorien von Vorfällen gibt der EDSA auch Empfehlungen für technische und organisatorische Maßnahmen zur Vorbeugung oder Minderung der Auswirkungen dieser Vorfälle.

Die Aufzählungen an möglichen Maßnahmen des EDSA kann, wie zuvor dargestellt, nicht abschließend oder vollständig sein. Auch muss nicht jede dort genannte Maßnahme für jede Verarbeitungstätigkeit oder Konstellation angemessen sein. Um eine Anpassung der genannten Maßnahmen an den konkreten Einzelfall werden Verantwortliche und Auftragsverarbeiter nicht umhinkommen. Sie müssen dies unter Berücksichtigung ihrer jeweiligen Situation bewerten und entscheiden. Des Weiteren wird in den Leitlinien nur eine Auswahl an möglichen Kategorien von Vorfällen betrachtet. Häufige Fälle wie etwa kompromittierte E-Mail-Accounts werden zum Beispiel nicht betrachtet.

In den Leitlinien werden die Kategorien

– „Ransomware-Angriffe“,
– Angriffe auf Websites, Webserver und IT-Dienste über das Internet mit der Exfiltration von Daten,

– interne menschliche Risikoquellen,
– verlorene oder gestohlene Geräte und Papierdokumente sowie
– Fehler beim Versand von Post oder E-Mails

betrachtet.

Bei den Maßnahmen gibt es Überschneidungen zwischen den verschiedenen Kategorien. Teilweise können auch einzelne Empfehlungen mehrere Maßnahmen beschreiben, von denen gegebenenfalls nur eine Auswahl für eine Verarbeitungstätigkeit bzw. IT-Umgebung relevant ist. Ein gutes Bespiel dafür ist die erste Empfehlung in der Kategorie „Ransomware“:

> „Gewährleistung der Aktualität der Firmware, des Betriebssystems und der Anwendungssoftware auf den Servern, Client-Rechnern, aktiven Netzwerkkomponenten und allen anderen Rechnern im selben lokalen Netz (einschließlich Wi-Fi-Geräten). Sicherstellung, dass geeignete IT-Sicherheitsmaßnahmen vorhanden sind, dass sie wirksam sind und dass sie regelmäßig aktualisiert werden, wenn sich die Verarbeitung oder die Umstände ändern oder weiterentwickeln. Dazu gehört auch die Führung detaillierter Protokolle darüber, welche Patches zu welchem Zeitpunkt angewendet wurden.“

Über alle betrachteten Kategorien gibt es in der Leitlinie über 60 einzelne Empfehlungen mit teilweise mehreren Maßnahmen zur Vorbeugung von Vorfällen. Die betrachteten Kategorien werden in der Regel für alle datenverarbeitenden Stellen relevant sein. Das Ziel des EDSA ist es dabei, Verantwortlichen und Auftragsverarbeitern Ideen zur Vorbeugung zu geben und mögliche Lösungen aufzuzeigen. Im Kontext der gemäß Art. 33 DS-GVO an mich gemeldeten schweren Datenschutzverletzungen mit technischen Schwerpunkten verweise ich bei Fragen von Verantwortlichen nach möglichen Maßnahmen daher häufig auf diese Leitlinien. Ich empfehle den Verantwortlichen dabei zu überprüfen, ob die dort aufgeführten Maßnahmen bereits umgesetzt wurden. Bei den zum Zeitpunkt des Vorfalls nicht berücksichtigten Maßnahmen ist es ratsam, dass sich Verantwortliche die Frage stellen, warum dies bisher nicht geschehen ist und ob diese Maßnahmen für ihre Umstände geeignet wären. Im Rahmen der eigentlichen Vorgangsbearbeitung der mir gemeldeten schweren Datenschutzverletzungen mit technischen Schwerpunkten verweise ich ebenfalls auf die Leitlinien und fordere eine Begründung und Risikobewertung von Verantwortlichen, wenn diese Maßnahmen nach einem Vorfall nicht umgesetzt werden.

Weitere Quellen für mögliche technische und organisatorische Maßnahmen

Das Standard-Datenschutzmodell (SDM) der DSK stellt darüber hinaus eine Methodik zur Verfügung, um durch geeignete technische und organisatorische Maßnahmen die Risiken bei der Verarbeitung personenbezogener Daten so weit zu reduzieren, dass die rechtlichen Anforderungen der DS-GVO erfüllt werden können. Unter anderem werden zu den jeweiligen Gewährleistungszielen des SDM generische Maßnahmen genannt, die typischerweise zur Aufrechterhaltung der Gewährleistungsziele dienen können. Im Referenzmaßnahmen-Katalog des SDM werden zu diesem Zweck weitere Maßnahmen in Bezug auf typische Verarbeitungstätigkeiten dargestellt. Diesen Maßnahmen, die in Form von Bausteinen veröffentlicht werden, wird auch seitens der DSK eine Einschätzung mitgegeben, wie kritisch die jeweilige Maßnahme für die Gewährleistung der Anforderungen der DS-GVO in den typischen Verarbeitungssituationen ist.

Bei den Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung von personenbezogenen Daten gibt es eine signifikante Schnittmenge mit den Maßnahmen, die aus dem Bereich der IT-Sicherheit kommen. Für diese Schnittmenge kann zusätzlich auf die Veröffentlichungen des BSI verwiesen werden und hier insbesondere auf die dort entwickelte Vorgehensweise des IT-Grundschutzes. Das IT-Grundschutz-Kompendium, bestehend aus den IT-Grundschutz-Bausteinen, kann auch eigenständig als ergänzende Quelle von möglichen Maßnahmen genutzt werden. Bei der Verwendung von Quellen oder Vorgaben aus dem Bereich IT-Sicherheit muss allerdings immer beachtet werden, dass deren Anforderungen oder Empfehlungen nur eine Schnittmenge mit den Anforderungen des Datenschutzes bilden. Daher können für die Erfüllung von letzteren in der Regel weitere, möglicherweise auch konträre Maßnahmen notwendig sein. Die Maßnahmen aus den beiden Bereichen Datenschutz und IT-Sicherheit müssen dementsprechend mittels eines integrierten Vorgehens in Einklang gebracht werden. Auch unterscheidet sich die Sichtweise auf mögliche Risikoquellen, Bedrohungen und Schadenspotenziale sowie die Risikobewertung zwischen der IT-Sicherheit und dem Datenschutz. Dies muss berücksichtigt werden. Diese Unterschiede resultieren aus der unterschiedlichen Zielsetzung. Während die IT-Sicherheit Risiken bezüglich der eigenen Organisation betrachtet, liegt der Fokus des Datenschutzes auf den Risiken für die Rechte und Freiheiten natürlicher Personen. Das hat Auswirkungen sowohl auf die Ausgestaltung des Risikobegriffs als auch auf die technischen und organisatorischen Maßnahmen. Diese sind zum Teil die gleichen, hängen aber vom Einzelfall ab. Daher sind separate Risikobetrachtungen notwendig.

Fazit

Eine pauschale Antwort auf die Frage, welche technischen und organisatorischen Maßnahmen allgemein geeignet und hinreichend sind, um die Anforderungen der DS-GVO zu erfüllen, ist nicht möglich. Dies ist immer von der jeweiligen Situation und Verarbeitungstätigkeit abhängig. Es gibt aber unterschiedliche Quellen, die typische Maßnahmen aufführen und bei der Auswahl geeigneter Maßnahmen unterstützen. Diese Quellen sollten Verantwortliche kennen und angemessen berücksichtigen.

14.3
Löschen und Vernichten

Das Thema Löschen und Vernichten ist im Rahmen der Beratung im technischen und organisatorischen Datenschutz in unterschiedlichen Ausprägungen immer wieder von besonderer Bedeutung. Mit diesem Beitrag biete ich Verantwortlichen einen Einblick in dieses wichtige Thema und skizziere zur Veranschaulichung zwei konkrete Fälle aus dem Berichtszeitraum.

Beratungsanfragen und allgemeine Antworten

Die Verarbeitung personenbezogener Daten nach Art. 4 Nr. 2 DS-GVO muss gemäß den Grundsätzen aus Art. 5 Abs. 1 DS-GVO erfolgen. Hierzu zählt insbesondere auch der Grundsatz der Speicherbegrenzung nach Art. 5 Abs. 1 Buchst. e DS-GVO. Ferner haben betroffene Personen gemäß Art. 17 Abs. 1 DS-GVO gegenüber datenschutzrechtlich Verantwortlichen gemäß Art. 4 Nr. 7 DS-GVO das Recht auf unverzügliche Löschung ihrer Daten, falls mindestens eine der in Art. 17 Abs. 1 DS-GVO genannten Voraussetzungen erfüllt ist und keine Ausnahme des Art. 17 Abs. 3 DS-GVO eingreift. Nähere Informationen hierzu können dem *Kurzpapier Nr. 11 Recht auf Löschung / „Recht auf Vergessenwerden“* der DSK (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf) entnommen werden. Die Umsetzung des Grundsatzes der Speicherbegrenzung und die Gewährleistung des Rechts auf Löschung stehen bei der Verarbeitung personenbezogener Daten häufig in engem Zusammenhang. Immer wieder erreichen mich aus unterschiedlichen Bereichen Beratungsanfragen zu diesem Themenkomplex. Dies nahm ich im Berichtszeitraum zum u. a. Anlass, den Beitrag „*Löschen und Vernichten von Daten, aber wie?*“ (https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/loeschen-und-vernichten-von-daten-aber-wie) auf meiner Website zu veröffentlichen.

Löschen von Daten

Mit dem Begriff „Löschen“ bezeichnet man in der Informationstechnik (IT) im Allgemeinen den Vorgang des Entfernens von Daten (s. auch Roßnagel, in: Simitis/Hornung/Spiecker genannt Döhmann, 2. Aufl. 2025, Art. 4 Nr. 2 DS-GVO, Rn. 30). Die Anforderungen an die konkrete Ausgestaltung eines technisch wirksamen Löschverfahrens hängen maßgeblich von den jeweiligen Rahmenbedingungen ab. Hierbei sind je nach Szenario unterschiedliche Faktoren zu berücksichtigen, wie etwa

– die zugrundeliegenden Speichermedien,
– das eingesetzte Betriebssystem,
– das verwendete Dateisystem,
– hierauf aufbauende Datenbankmanagementsysteme sowie
– Verfahren zur Datensicherung.

Die einzelnen Löschschritte müssen aufeinander abgestimmt sein und sollten sich gegenseitig ergänzen. Gleichzeitig müssen aber auch Wechselwirkungen und Einflüsse ganzheitlich und umfassend betrachtet werden.

Grundsätzlich muss bei der Löschung von Daten auf Datenträgern sichergestellt werden, dass die zu löschenden Daten nicht wiederhergestellt werden können. Gängige Betriebssysteme berücksichtigen bei der Löschung von Daten bzw. Dateien allerdings ggf. nur Einträge im Inhaltsverzeichnis des zugrundeliegenden Dateisystems. Hierdurch werden dann ggf. nur Verweise auf Datenblöcke entfernt und Bereiche auf darunterliegenden Speichermedien zum Überschreiben freigegeben. Ein tatsächliches Entfernen der zu löschenden Daten durch ein wirksames Überschreiben findet hierbei jedoch nicht statt. Auch bei der Formatierung eines Speichermediums können ggf. Daten zurückbleiben, z. B. bei einer sogenannten „Schnellformatierung“. Im Ergebnis sind die Daten in beiden dargestellten Szenarien weiterhin vorhanden und können nicht selten mit entsprechenden Hilfsmitteln wiederhergestellt werden. Dementsprechend ist die technische Wirksamkeit der Löschung nicht gegeben. Weitere Informationen zu dieser Thematik können bspw. dem Beitrag „*Daten auf Festplatten, Datenträgern und Smartphones sicher löschen*“ (https://www.bsi.bund.de/dok/6599236) auf der Website des BSI entnommen werden.

Bereits bei der erstmaligen Speicherung von Daten und in der Folge bei der weiteren Verwaltung können ggf. Maßnahmen ergriffen werden, die eine spätere Löschbarkeit begünstigen. So kann bspw. eine durchgängige wirksame Verschlüsselung von gespeicherten Daten zu einer Verringerung des Widerherstellungsrisikos für gelöschte Daten beitragen.

Vernichten von Datenträgern

Mit „Vernichtung“ wird das Entfernen von Daten durch die Zerstörung des Datenträgers mittels eines Verfahrens bezeichnet, das eine Widerherstellung der Daten mit hinreichender Sicherheit verhindert (s. auch Roßnagel, in: Simitis/Hornung/Spiecker genannt Döhmann, 2. Aufl. 2025, Art. 4 Nr. 2 DS-GVO, Rn. 33). Verbreitete Verfahren sind in diesem Zusammenhang das Schreddern von Papierakten, CDs oder DVDs oder das Entmagnetisieren von Festplatten. Auch hier ist ein besonderes Augenmerk auf die Wirksamkeit des eingesetzten Verfahrens zu richten. Mit der technischen Normreihe „*DIN 66399 Büro- und Datentechnik – Vernichtung von Datenträgern*“ des Deutschen Instituts für Normung e. V. (DIN) stehen entsprechende Standards zur Verfügung.

Datenschutzrechtliche Perspektive

Aus datenschutzrechtlicher Perspektive handelt es sich bei der Löschung und Vernichtung von personenbezogenen Daten um eine Verarbeitung gemäß Art. 4 Nr. 2 DS-GVO. Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO müssen daher die bereits angeführten Grundsätze für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 DS-GVO auch beim Löschvorgang einhalten. Im Sinne des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen gemäß Art. 25 DS-GVO müssen hierzu geeignete technische und organisatorische Maßnahmen (TOM) ergriffen werden. Darüber hinaus müssen Verantwortliche und deren etwaige Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DS-GVO zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 DS-GVO ebenfalls TOMs ergreifen.

Hilfestellungen

Zur Ermittlung und Festlegung der erforderlichen TOM auf Basis eines risikobasierten Ansatzes empfehlen die DSK, der IT-Planungsrat und das BSI als Werkzeug das Standard-Datenschutzmodell (SDM) der DSK (https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V31.pdf). Eine spezifische Hilfestellung für das Thema Löschen und Vernichten im Zusammenhang mit dem SDM veröffentlichte die DSK mit dem gleichnamigen SDM-Baustein 60 „*Löschen und Vernichten*“ (https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_L%C3%B6schen_und_Vernichten_V1.0a.pdf).

Auch für den Bereich der Informationssicherheit sind Prozesse und Verfahren für das wirksame Löschen von Daten und Vernichten von Datenträgern um-

zusetzen. Der Baustein CON.6 „*Löschen und Vernichten*“ des BSI IT-Grundschutz-Kompendiums (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2023.pdf) kann hier eine Orientierung bieten.

Beispiele aus dem Berichtszeitraum

Im Berichtszeitraum gab es im Zusammenhang mit der Löschung von Daten unterschiedliche Beratungsanfragen datenschutzrechtlich Verantwortlicher. Zwei dieser Anfragen werde ich im Folgenden kurz skizzieren.

Bei einem Verantwortlichen werden wiederbeschreibbare Speichermedien wie USB-Sticks regelmäßig zur Weitergabe personenbezogener Daten verwendet. Empfänger der Speichermedien waren hierbei zum Teil betroffene Personen selbst. Es wurden aber auch Speichermedien an berechtigte Dritte weitergegeben. Nach der Nutzung wurden die Speichermedien zur Vernichtung an den Verantwortlichen zurückgegeben. Es stellte sich nun die Frage, ob eine Wiederverwendung der Speichermedien möglich sei. Zur Beantwortung dieser Frage musste der Verantwortliche den gesamten Nutzungszyklus der Speichermedien auf der einen und die Risiken für die Rechte und Freiheiten der betroffenen Personen auf der anderen Seite in den Blick nehmen. Hierauf aufbauend waren die Verschlüsselung der Daten auf den Datenträgern und die nach Rückgabe der Datenträger zur Anwendung gebrachten Löschverfahren von besonderer Relevanz. Auch wurde dem Verantwortlichen zur Etablierung eines Verfahrens zur regelmäßigen Überprüfung der ergriffenen Maßnahmen geraten.

Im Rahmen eines weiteren Beratungsfalls erreichte mich die Anfrage eines Verantwortlichen, der eine Web-basierte Plattform eines Dienstleisters zur Durchführung von Bewerbungsverfahren für Stipendien einsetzte. Bei dieser Plattform stellte sich überraschend heraus, dass die vollständige Löschung von Bewerbungen nicht umgesetzt war. Dementsprechend stellte sich die Herausforderungen, eine Speicherbegrenzung gemäß Art. 5 Abs. 1 Buchst. e DS-GVO auf andere Weise umzusetzen. Der Verantwortliche entschloss sich im Laufe der weiteren Beratung, die bisher eingesetzte Plattform nicht weiter nutzen zu wollen und sie zu ersetzen. Für eine Übergangsphase etablierte er als Abhilfemaßnahme einen manuellen Prozess, bei dem die Daten von Bewerbenden so weit, wie es die Plattform ermöglichte, gelöscht wurden. Die nach Abschluss dieses kleinschrittigen Prozesses verbliebenen Daten wurden mit Standardwerten überschrieben. Derartige Verfahren zur Problembehebung sind i. d. R. aufwändig, fehleranfällig und für den dauerhaften Regelbetrieb wenig geeignet.

Diese beiden exemplarischen Fälle verdeutlichen das breite Spektrum an Fragestellungen im Zusammenhang mit dem Thema Löschen und Vernichten. Ich ermutige Verantwortliche, sich aktiv mit diesem Thema zu befassen und sich den vielschichtigen Herausforderungen zu stellen.

14.4 Software-gestützte Schwärzung von PDF-Dateien

PDF-Dokumente sind aus dem Arbeitsalltag öffentlicher und nicht öffentlicher Stellen kaum mehr wegzudenken. Bestimmte Anwendungsfälle erfordern die Veränderung solcher Dokumente, um vertrauliche Informationen zu schwärzen. Im Folgenden wird beschrieben, woran sich die Wirksamkeit einer solchen Schwärzung bemisst und welche Verhaltensweisen angesichts der Möglichkeit einer ungeplanten Unwirksamkeit solcher Schwärzungen angezeigt sind.

Das Portable Document Format

Beim Portable Document Format (PDF) handelt es sich um ein sehr weit verbreitetes Format für digitale Dokumente. Es wurde mit dem Ziel entwickelt, Dokumente plattformübergreifend einheitlich und möglichst druckecht darzustellen. Die zugrundeliegende Hardware, das verwendete Betriebssystem und auch die zur Anzeige verwendeten Software sollten dementsprechend keinen Einfluss auf die Darstellung haben.

Die Möglichkeit zur inhaltlichen Bearbeitung von Dokumenten im PDF-Format lag demgegenüber bei der Spezifikation des Formats nicht im Fokus. In der Folge sind Anwendungsprogramme, mittels derer PDF-Dateien inhaltlich verändert werden können, weniger verbreitet als solche, die einen ausschließlich lesenden Umgang mit PDF-Dateien ermöglichen.

Schwärzen in PDF-Dokumenten

Bestimmte – teilweise auch kostenfrei verfügbare – Anwendungsprogramme ermöglichen jedoch, PDF-Dateien derart zu verändern, dass damit speziellen Anwendungsfällen Rechnung getragen wird. Ein solcher Anwendungsfall ist das sogenannte „Schwärzen“ von Schriftstücken. Dies kann überall dort erforderlich werden, wo ein Umgang mit vertraulichen Informationen erfolgt. Der Begriff des Schwärzens geht auf die wirksame Unkenntlichmachung von vertraulichen Teilbereichen physischer Dokumente zurück, z. B. in Papierakten. Hierzu werden die entsprechenden Bereiche schwarz dargestellt, so dass der ursprüngliche Inhalt nicht mehr erkennbar ist. Im Rahmen einer Schwärzung muss hierbei sichergestellt werden, dass der geschwärzte Inhalt nicht wieder sichtbar gemacht werden kann. So ist das einfache Markieren

oder Überschreiben eines relevanten Bereiches mittels eines blickdichten schwarzen Textmarkers in aller Regel ungeeignet. Hier kann ein verdeckter Bereich häufig mittels einfacher Verfahren wieder sichtbar gemacht werden.

Mit fortschreitender Digitalisierung entstand zunehmend der Bedarf, auch Teilbereiche von digitalen Dokumenten – wie PDF-Dokumente – unkenntlich zu machen. Der bereits verwendete Begriff der Schwärzung wurde für diesen Vorgang übernommen.

Für den Datenschutz ist das Entfernen von personenbezogenen oder personenbeziehbaren Daten aus Schriftstücken von besonderer Bedeutung. Allgemein kann etwa im behördlichen Kontext die Herausgabe von Schriftstücken erforderlich sein, in denen personenbeziehbare Daten enthalten sind, die bestimmten Empfängern gegenüber nicht offengelegt werden dürfen. In solchen Fällen kann ein entsprechend geeignetes Anwendungsprogramm genutzt werden, um diese Daten durch Schwärzen unkenntlich zu machen. In meiner Behörde ist das Schwärzen von Schriftstücken bspw. in den folgenden Fällen häufig erforderlich:

1. Akteneinsicht an Beteiligte in Verwaltungsverfahren (§ 29 HVwVfG).
2. Datenschutzrechtliche Auskunft über verarbeitete personenbezogene Daten an betroffene Personen (Art. 15 DS-GVO).
3. Informationszugang nach Informationsfreiheitsrecht (§ 80 HDSIG).

Technische Wirksamkeit der Schwärzung

Ein zentrales datenschutzrechtliches Ziel beim Schwärzen von Schriftstücken ist die Gewährleistung der Vertraulichkeit personenbezogener Daten gemäß Art. 5 Abs. 1 Buchst. f DS-GVO durch technische und organisatorische Maßnahmen nach Art. 25 Abs. 1 DS-GVO. Eine Schwärzung auf Ebene der Ansicht von PDF-Dokumenten erfolgt i. d. R. dadurch, dass schwarze oder weiße Bereiche anstelle der zu verbergenden Text- oder Bildbestandteile des Dokuments angezeigt werden. Hierbei ist zu beachten, dass die Text- oder Bildbestandteile bei der Schwärzung auch tatsächlich aus dem Dokument entfernt und nicht nur überlagert werden. Andernfalls wäre die Wirksamkeit der Schwärzung nicht sichergestellt, etwa wenn mittels einer Anwendung geschwärzte Bereiche wieder entfernt und die Text- oder Bildbestandteile wieder sichtbar gemacht werden könnten.

Es ist jedoch nicht ausreichend, bei einer Schwärzung lediglich die Anzeige eines Dokuments zu berücksichtigen. So bietet das PDF-Format bspw. die Möglichkeit, Daten aus einer Schrifterkennung (Optical Character Recognition, OCR) oder Meta-Daten in ein Dokument zu integrieren, ohne dass diese den Betrachtern angezeigt werden.

Dementsprechend muss im Rahmen einer Schwärzung sichergestellt werden, dass alle Teilbereiche eines Dokuments mit einbezogen werden. Idealerweise sollte bereits bei der Erstellung von Dokumenten sichergestellt werden, dass nur diejenigen Daten in Dokumente aufgenommen werden, die für den Verwendungszweck der Dokumente auch tatsächlich erforderlich sind.

Identifikation der Unwirksamkeit einer Schwärzung

Meine Behörde setzt selbst Anwendungs-Software ein, die unter Beachtung der genannten Anforderungen dafür genutzt wird, Schriftstücke im PDF-Format zu schwärzen. Diese Software wird durch die HZD zentral verteilt und auf den dienstlichen Rechnern der Hessischen Landesverwaltung bereitgestellt.

Im Anschluss an die Nutzung der Software erfolgt jeweils routinemäßig eine grundlegende Überprüfung der Ergebnisse hinsichtlich der Wirksamkeit der Schwärzung. Das heißt, es wird nach Erstellung der geschwärzten Datei noch mit anderen Programmen geprüft, ob Schwärzungen entfernt oder ggf. Text, der nur von ihnen überlagert wird, markiert und kopiert werden kann. Im Berichtszeitraum fiel in einem Fall bei der Überprüfung überraschenderweise auf, dass dies tatsächlich zutraf und die vorgenommene Schwärzung somit nicht wirksam war. Dieselbe Software war in der Vergangenheit erfolgreich eingesetzt worden, weshalb Bedienungsfehler wenig wahrscheinlich erschienen. Vielmehr bestand die Befürchtung, dass ein Softwarefehler vorlag, der im Rahmen eines Updates der Software unbemerkt geblieben war.

Um dies zu überprüfen, erfolgte ein Abgleich mit der offiziellen Versionshistorie der Software, die auf deren Website veröffentlicht war. Dort fand sich für die neuste veröffentlichte Version die Angabe einer Fehlerbehebung, die auch tatsächlich im Zusammenhang mit der Schwärzen-Funktion stand und auf deren Unwirksamkeit hinwies. Ferner enthielt die Versionshistorie die genaue Angabe, in welcher Version dieses Problem erstmalig aufgetreten war. Somit war genau bekannt, welche einzelne Version der Software eine unwirksame Schwärzung erzeugte. Die Software-Version, die auf den dienstlichen Rechnern im Einsatz war, war durch Bereitstellungsinformationen der HZD bekannt. Dadurch war erkennbar, dass auf diesen Rechnern noch die fehlerbehaftete Version im Einsatz war, während eine Version mit behobenem Fehler durch den Software-Entwickler bereits veröffentlicht worden war.

Daraufhin begann mit Unterstützung des behördlichen Datenschutzbeauftragten sowie des behördlichen IT-Sicherheitsbeauftragten eine Untersuchung der möglichen Folgen. Die Mitarbeitenden wurden über den Software-Fehler informiert. Sie wurden gebeten zu prüfen, ob von ihnen im Zeitraum, in dem die fehlerhafte Version im Einsatz war, Dokumente mit unwirksamer Schwärzung erstellt oder versandt worden waren. Dies war nicht der Fall.

Parallel zur internen Untersuchung ist meine Behörde auch auf die HZD zugegangen. Da diese für die Bereitstellung der PDF-Software auf den Dienstrechnern zuständig ist, sollte von dort aus auch eine Information der anderen betroffenen hessischen Dienststellen erfolgen, damit diese ebenfalls untersuchen konnten, welche Folgen der Software-Fehler bei ihnen jeweils hatte. In diesem Zusammenhang war auch von den Dienststellen zu prüfen, ob sie Meldungen gemäß Art. 33 DS-GVO oder § 60 HDSIG an mich abgeben mussten. Über die IT-Sicherheitsbeauftragten der einzelnen Dienststellen wurde diese Informationsverteilung erreicht. Die HZD führte zeitnah auch die Bereitstellung der neusten verfügbaren Version der betroffenen Software durch, in welcher der Fehler behoben war.

Fazit

Der Vorfall zeigt, dass die wirksame Schwärzung von PDF-Dokumenten nicht allein eine Frage der Darstellung am Bildschirm ist. Informationen – auch sensible personenbezogene Daten – können weiterhin in solchen Dokumenten vorhanden und somit auch extrahierbar sein. Verlassen sich datenschutzrechtlich Verantwortliche und Auftragsverarbeiter hier ausschließlich auf den ersten Eindruck der Darstellung, kann die Ungeeignetheit einer eingesetzten Software nicht erkannt werden oder ein Software-Fehler im Rahmen von Updates unentdeckt bleiben. Dies macht sowohl eine gründliche Softwareauswahl als auch regelmäßige Überprüfungen derselben erforderlich.

Ebenso essenziell ist ein Datenschutz-Management, das das zeitnahe Einspielen von Software-Aktualisierungen gewährleistet, insbesondere wenn diese sicherheitskritischen Schwachstellen oder datenschutzrelevante Fehler beheben. Zu einem angemessenen Datenschutz-Management gehören auch Prozesse zur Identifikation und zum Umgang mit Datenschutzvorfällen: Hier muss zunächst als Ausgangspunkt eine Abschätzung der möglichen Folgen durchgeführt werden, die auch die gesetzlichen Pflichten zur Abgabe von Meldungen von Verletzungen des Schutzes personenbezogener Daten (Art.33 DS-GVO) und zur Benachrichtigung betroffener Personen (Art. 34 DS-GVO) berücksichtigen und deren Umsetzung gewährleistet. Insbesondere im öffentlichen Bereich sollte stets auch der Blick über den eigenen Verantwortungsbereich hinaus erfolgen, um die Einbindung zuständiger Stelle und Gremien zu gewährleisten.

14.5
Einsatz neuer Prüftools zur technischen Prüfung von Websites

Websites sind ein im Rahmen meiner Aufsichtstätigkeit häufig wiederkehrender Gegenstand von Datenschutzprüfungen. Um den technischen Prüfprozess zu vereinfachen, hat meine Abteilung für technischen und organisatorischen Datenschutz ein Toolkit entwickelt, das verschiedene Prüf-Tools miteinander verbindet, um eine umfassende technische Analyse von Websites effizient zu ermöglichen.

Datenschutz bei Websites

Seit Inkrafttreten der DS-GVO gelten auch für Websites neue Anforderungen bezüglich der Verarbeitung personenbezogener Daten: Zu nennen sind insbesondere Einwilligungsvorbehalte für bestimmte Verarbeitungen etwa zu Werbezwecken, für die der Websitesverantwortliche kein überwiegendes berechtigtes Interesse geltend machen kann. Ferner gelten etwa für das Speichern von Informationen und den Zugriff auf Endeinrichtungen wie PCs oder Smartphones Anforderungen des TDDDG. Viele Websitesbetreiber haben daher ihre Online-Angebote angepasst und entsprechende Funktionalitäten ihrer Websites überarbeitet. Die Fortschreibung des Datenschutzrechts führte auch zu einem erhöhten öffentlichen Bewusstsein über potenzielle Datenschutzrisiken auf Websites und damit einhergehend einer steigenden Anzahl an eingehenden Datenschutzbeschwerden bei den Datenschutzaufsichtsbehörden.

Immer wieder muss ich daher Websites auf Indizien für etwaige Datenschutzverletzungen prüfen. Für den technischen Teil solcher Prüfungen gilt es, eine Vielzahl an verschiedenen Aspekten zu berücksichtigen, wie zum Beispiel:

– Ergeben sich Anzeichen für die Ausnutzbarkeit von Sicherheitslücken bei den verwendeten Anwendungskomponenten?
– Ist zur Übermittlung personenbezogener Daten eine angemessene Transportverschlüsselung eingerichtet?
– Wie ist das Speichern von Informationen auf Endeinrichtungen des Benutzers umgesetzt?
– Gibt es Anzeichen für Defizite bei der grundlegenden Konfiguration des Webservers?
– Gibt es Anzeichen dafür, dass personenbezogene Daten an Länder außerhalb der EU und des EWR – sogenannte Drittländer – übermittelt werden?
– Gibt es Domains mit ähnlichen Namen, die potenziell dem Zweck dienen, durch Fehleingaben an persönliche Daten der Nutzenden zu gelangen?

Werkzeuge für technische Prüfungen

Um diese und weitere Aspekte zu untersuchen, setze ich eine Reihe von unterschiedlichen Software-Werkzeugen ein. Im Rahmen der Nutzung hat es sich gezeigt, dass ihr manueller Einsatz für eine Vielzahl gleichartiger Prüfungen, die ebenfalls manuelle Auswertung und die verständliche Aufbereitung ihrer unterschiedlichen Ausgaben mit vergleichsweise hohen Aufwänden verbunden ist. Daher hat meine Abteilung für technischen und organisatorischen Datenschutz ein Toolkit entwickelt, das den Einsatz dieser Tools bündelt und ihre reihenweise Ausführung mittels weniger Steuerbefehle vereinfacht. Durch eine vereinheitlichte Bedienung und ein hohes Maß an Automatisierung konnte der Prüfprozess so erheblich effizienter gestaltet werden. Dadurch ist es mir möglich, auch große Mengen an Websites effizient auf Indizien für etwaige Verstöße gegen datenschutzrechtliche Vorgaben zu prüfen.

Ablauf einer automatisierten technischen Website-Prüfung

Das Toolkit nimmt einzelne Domain-Namen oder Listen von Domain-Namen entgegen. Die Websites mit diesen Domain-Namen werden dann automatisiert mittels eines Web-Browsers aufgerufen. Die bei diesem Aufruf entstehenden Verbindungs- und Inhaltsdaten werden dabei für die Prüfungswerkzeuge zugreifbar. In einem ersten Schritt werden die für den Endnutzer oberflächlich nicht sichtbar an dessen Browser übermittelten Kopfdaten beim Aufruf der Website unter dieser Domain ausgewertet. Es ist möglich, dass durch eine unerwünschte Konfiguration des Web-Servers, der diese Website bereitstellt, hierin Informationen enthalten sein können, die Aufschluss über eingesetzte IT-Systeme oder Software-Versionen mit etwaigen Sicherheitslücken geben. Dies kann als erstes Indiz für weitergehende Untersuchungen geeignet sein, die mögliche Schwächen bei der Sicherheit der Verarbeitung personenbezogener Daten gemäß Art. 32 Abs. 1 DS-GVO aufzeigen können.

Die IP-Adresse des Web-Servers wird mittels DNS-Auflösung abgefragt. Bei DNS handelt es sich um ein System weltweit verteilter Server, die einen Domain-Namen unter anderem IP-Adressen zuordnen. Dies geschieht teilweise in Abhängigkeit vom geografischen Ort einer solchen Abfrage, um weltweit einen effizienten Verbindungsaufbau zwischen Anfragendem und Server zu ermöglichen. Mit der IP-Adresse des Web-Servers kann das Toolkit durch Abgleich entsprechender Datenbanken Informationen zum ungefähren Standort des Servers erhalten, was vor allem in Hinblick auf potenzielle Datenübermittlungen in Drittländer von Interesse ist. Bei solchen Datenübermittlungen sind die Vorgaben des fünften Kapitels der DS-GVO zu beachten, wodurch insbesondere Übermittlungen an Stellen in Ländern

ohne Angemessenheitsbeschluss der EU-Kommission zusätzliche Anforderungen erfüllen müssen.

Das Toolkit führt auch eine Prüfung der Transportverschlüsselung der Website durch. Dies geschieht durch Simulation unterschiedlicher Benutzerkonfigurationen (Betriebssysteme, Web-Browser, Software-Bibliotheken), die unterschiedliche Verschlüsselungsverfahren unterstützen. Dadurch ergeben sich Erkenntnisse in Hinblick auf die unterstützen TLS-Versionen, -Chiffren und -Protokolle sowie sonstige kryptographische Schwachstellen. Dies dient einem Abgleich mit den Vorgaben zur Sicherheit der Verarbeitung personenbezogener Daten aus Art. 32 DS-GVO.

Das Toolkit ermöglicht außerdem den simulierten Aufruf einer Website mittels eines Web-Browsers, um dadurch Indizien zu sammeln, die auf die potenzielle Verarbeitung personenbezogener Daten oder das Speichern von Informationen hinweisen, wie z. B. das Anlegen von Cookies – mit Blick auf § 25 TDDDG – oder der Aufbau von Datenverbindungen zu Drittanbietern. Der Aufruf der Websites findet ohne Nutzerinteraktion statt, wird automatisiert protokolliert (auch in Form von Screenshots) und gibt dadurch Hinweise auf den Umgang mit Einwilligungs-Bannern auf der Website.

Des Weiteren bietet das Toolkit auch die Möglichkeit, ähnlich lautende Webadressen zu ermitteln, die sich nur durch Buchstabendreher von der eigentlichen Webadresse unterscheiden und damit eine Gefahr durch sogenannte Typosquatting-Angriffe darstellen können (zu entsprechenden Risiken und meine Prüfungen siehe Kap. 4.6 und 14.6). Bei Typosquatting werden persönliche Daten abgegriffen, indem Nutzer durch Tippfehler auf einer ähnlich aussehenden Website landen und dort dann unbedarft ihre Daten angeben.

Abschließend bereitet das Toolkit die Untersuchungsergebnisse in verschiedenen Formaten auf und fasst diese in einem einfach verständlichen Prüfbericht zusammen, der auch zur Grundlage für die Zusammenarbeit meiner technisch und juristisch orientierten Referate dienen kann.

Das Toolkit ist speziell auch in Hinblick auf Prüfvorgänge entwickelt und optimiert worden, bei denen eine größere Anzahl an Websites überprüft werden muss. Dies wurde bereits anhand einer ersten Prüfung erprobt, mit der die Grundlage zur effektiven Sensibilisierung der Verantwortlichen für ihre datenschutzrechtlichen Pflichten geschaffen wurde.

Fazit

Im Ergebnis konnte die Verbindung unterschiedlicher Tools zu einem umfassenden Werkzeugkasten technischer Datenschutzprüfungen einen wichtigen

Beitrag dazu leisten, Datenschutzbeschwerden effizient zu bearbeiten und eigeninitiierte Prüfungen zweckgemäß zu gestalten.

14.6
Prüfung des Software-Einsatzes bei hessischen Gesundheitsämtern

Im Berichtszeitraum habe ich den Einsatz einer bestimmten Software in hessischen Gesundheitsämtern überprüft. Die Prüfung hat mir gezeigt, wie wichtig es ist, Software den Anforderungen und Gegebenheiten vor Ort anzupassen, um einen datenschutzkonformen Einsatz zu gewährleisten.

Hinweise auf Sicherheitslücken durch Medienberichte

Die Arbeit der hessischen Gesundheitsämter, die bei den Landkreisen besonders schützenswerte personenbezogene Daten verarbeiten, wird durch Fachanwendungen unterstützt. Aus diesem Grund fanden gegen Ende 2023 Medienberichte meine Aufmerksamkeit, die darauf hinwiesen, dass die Fachanwendung eines bestimmten Anbieters mit zahlreichen Sicherheitslücken ausgeliefert werde, die im Falle der Ausnutzung zu ernstzunehmenden Datenschutzverletzungen führen könnten. So erfolge dort etwa die Speicherung von Passwörtern in unsicherer Weise. Auch Zugriffsberechtigungen seien unzureichend implementiert, so dass die Vertraulichkeit der Verarbeitung personenbezogener Daten infrage stünde.

Der Software-Anbieter selbst hat seinen Sitz außerhalb Hessens. Daher fiel eine diesbezügliche Prüfung der zuständigen Landesdatenschutzaufsichtsbehörde zu. Im Vordergrund meiner eigenen Prüfung standen demgegenüber diejenigen hessischen Gesundheitsämter, die die betroffene Software im Einsatz hatten. Diese treffen beim Software-Einsatz grundsätzlich alle rechtlichen Pflichten eines Verantwortlichen im Sinne der DS-GVO, insbesondere die Pflichten, die Datenschutzgrundsätze wie die Vertraulichkeit durch geeignete technische und organisatorische Maßnahmen (TOM) gemäß Art. 25 DS-GVO umzusetzen und die Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO zu gewährleisten.

Da am Markt für solche Fachanwendungen mehrere Lösungen angeboten werden und die einzelnen Gesundheitsämter diese voneinander unabhängig entsprechend ihrer jeweiligen Anforderungen beschaffen, waren nicht alle hessischen Gesundheitsämter von meiner Prüfung betroffen. Aufgrund einer öffentlich einsehbaren Auskunft auf eine „FragDenStaat“-Anfrage eines Bürgers war mir bereits kurz nach den Presseberichten zu den vermeintlichen Sicherheitslücken bekannt, bei welchen fünf Gesundheitsämtern die Software des Anbieters im Einsatz war.

Prüfung

Bei der Erfüllung meiner gesetzlichen Aufgaben aus Art. 57 Abs. 1 DS-GVO bin ich grundsätzlich nicht auf Anlässe in Form von Eingaben oder Beschwerden angewiesen. Im vorliegenden Fall haben die medialen Berichte für mich einen dahingehend ausreichenden Anfangsverdacht erzeugt, dass möglicherweise relevante Datenschutzverstöße vorliegen könnten. Dies nahm ich zum Anlass, um eigeninitiativ eine darauf gerichtete Datenschutzüberprüfung gemäß Art. 58 Abs. 1 Buchst. b DS-GVO durchzuführen.

Hierzu habe ich zunächst diejenigen fünf Gesundheitsämter, welche diese Software nutzten, mit einem Fragebogen adressiert. Mit diesem habe ich u. a. die folgenden Fragen gestellt:

– In welchem Umfang und zur Verarbeitung welcher Kategorien personenbezogener Daten wird die Software genutzt?
– Wie werden die einzelnen, in den Berichten aufgeworfenen Sicherheitslücken bewertet und waren diese für das jeweilige Gesundheitsamt zutreffend?
– Welche Konsequenzen wurden aus der öffentlichen Diskussion dieser Sicherheitslücken gezogen?

Die Gesundheitsämter mussten ihre Stellungnahmen durch die Übermittlung geeigneter Dokumentationen wie z. B. von Verzeichnissen von Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DS-GVO, Darstellungen technischer und organisatorischer Maßnahmen und Berechtigungskonzepte belegen.

Nach dem in allen Fällen fristgerecht erfolgten Rücklauf der Fragebögen konnte ich eines der Gesundheitsämter direkt von einer tiefergehenden Prüfung ausschließen, da dieses die Software nur im Bereich der Wasserüberwachung einsetzte und hier nicht von einer relevant risikobehafteten Verarbeitung personenbezogener Daten ausgegangen werden musste.

In drei Fällen wurden schriftliche Rückfragen gestellt und beantwortet, da die ersten Stellungnahmen an einigen Stellen noch Raum für unterschiedliche Interpretationen gelassen hatten. Diese konnten jedoch jeweils durch vertiefende Rückfragen ausgeräumt werden.

In einem einzigen Fall schien der rein schriftliche Austausch nicht erfolgversprechend, da sich die Antworten des Gesundheitsamts auf ein Verhalten der Software bezogen, das ohne Inaugenscheinnahme nicht ohne weiteres nachzuvollziehen war. Aus diesem Grund wurde mit diesem Gesundheitsamt eine Videokonferenz anberaumt. Im Rahmen dieser Konferenz konnte das Gesundheitsamt meinen Mitarbeitenden mittels Bildschirmpräsentation die infrage stehende Funktionsweise der Software nachvollziehbar und zufriedenstellend erläutern.

Im Ergebnis konnte ich zusammenfassend feststellen, dass die behaupteten Sicherheitslücken zwar unter bestimmten Konstellationen hätten bestehen können. Diese Konstellationen lagen jedoch zum Großteil für die hessischen Gesundheitsämter nicht vor. Von wesentlichem Interesse war etwa die mangelhafte Implementierung von Zugriffsberechtigungen, so dass es möglich gewesen sein könnte, dass ein fachbereichsübergreifender unbefugter Zugriff auf personenbezogene Daten hätte stattfinden können. Dem waren die hessischen Gesundheitsämter jedoch von Anfang an zuvorgekommen, indem für unterschiedliche Fachbereiche auch unterschiedliche Instanzen der Software mit jeweils eigenen Datenbanken genutzt wurden, wodurch diese Möglichkeit nicht bestand. Sicherheitslücken, die für die hessischen Gesundheitsämter tatsächlich akut waren, wie etwa das Bestehen von Standard-Administratorenzugängen mit bekannten Zugangsdaten und weitreichenden Berechtigungen, waren bereits zeitnah nach Bekanntwerden durch die medialen Berichte behoben worden. Aus diesem Grund war es in keinem der fünf Fälle für mich erforderlich, Abhilfemaßnahmen gemäß Art. 58 Abs. 2 DS-GVO zu verhängen.

Ausblick

Im Berichtszeitraum habe ich das Projekt „Einheitliche Software für die hessischen Gesundheitsämter (DigiLGL)“ begleitet. Ziel des Projekts ist es, die fragmentierte und teils veraltete Software der hessischen Gesundheitsämter durch eine einheitliche und modulare Softwareinfrastruktur zu ersetzen. Die hessischen Gesundheitsämter als auch das im Jahr 2023 neu geschaffene Hessische Landesamt für Gesundheit und Pflege sollen durch die Modernisierungsmaßnahme allen fachlichen und übergreifenden Anforderungen wie beispielsweise Datenschutz, Datensicherheit und Kompatibilität zum Online-Zugangs-Gesetz gerecht werden. Darüber hinaus sollen damit auch die grundlegenden Anforderungen an eine moderne IT-Infrastruktur wie der Einsatz von Open-Source-Software, Open Data und die Anforderungen der gematik erfüllt werden.

Im Oktober 2024 sind erste Module der neuen Software im Gesundheitsamt Frankfurt in den Echtbetrieb gegangen.

14.7
Datenschutzverletzungen

Die Zahl der Meldungen von Datenschutzverletzungen stieg im Berichtsjahr auf 2.141 und damit auf den bisherigen Höchststand seit Einführung der Meldepflicht nach Art. 33 DS-GVO. Darunter waren auch 482 Meldungen über Cyberangriffe auf Stellen in Hessen. Ein Beispiel, der Cyberangriff auf das Universitätsklinikum Frankfurt am Main, wird in Kap. 12.4 beschrieben.

Überblick und Entwicklungen

Die Anzahl 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 stieg im Berichtsjahr 2024 erneut an und erreichte mit 2.141 Meldungen den Höchststand seit Beginn der Zählung mit dem Wirksamwerden der DS-GVO. Die Bearbeitung der Meldung von Datenschutzverletzungen stellte damit weiterhin einen großen Anteil der täglichen Arbeit meiner Behörde dar.

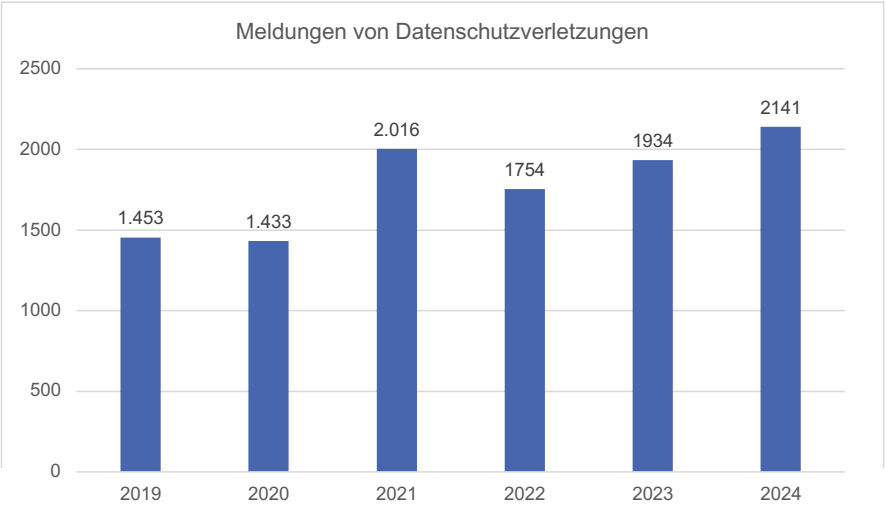


Abb. 1 Entwicklung der Anzahl der Meldungen von Datenschutzverletzungen beim HBDI seit Wirksamwerden der DS-GVO

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 2024 der Wirtschaftssektor einschließlich Kreditwirtschaft, Inkasso, Dienstleister, Handel und Gewerbe sowie die Bereiche Beschäftigtendatenschutz und Gesundheit.

Cyberangriffe auf Kommunen

Bereits in meinem letzten Tätigkeitsbericht hatte ich darauf hingewiesen, dass sich die Entwicklung der Cyberangriffe auf den Bereich der öffentlichen Verwaltung (und deren Dienstleister) dynamisch darstellt. Auch im Berichtsjahr 2024 ist die Anzahl erneut gestiegen.

Neben der Erbeutung einer hohen Anzahl von Daten der Bürgerinnen und Bürger rückt mehr und mehr in den Fokus, dass durch die höheren Angriffszahlen auch die Funktionsfähigkeit der Verwaltungen und damit die Zurverfügungstellung des kommunalen Angebots an die Bürgerinnen und Bürger eingeschränkt werden können.

Statistik unter dem Gesichtspunkt möglicher Nichtmeldungen (Dunkelziffer)

Im Rahmen der Meldungen von Cyberangriffen auf Auftragsverarbeiter stellten diese Listen mit betroffenen Verantwortlichen zur Verfügung. Im Laufe der Auswertungen wurde immer wieder festgestellt, dass Verantwortliche keine Meldungen abgeben. Dies führte im letzten Berichtsjahr zwangsläufig zu der Frage, wie hoch die Anzahl der Nichtmeldungen allgemein ist und wie die jährlich erhobene Statistik eventuell neu interpretiert werden müsste.

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.

Mit Blick auf die Cyberangriffe gerade auf Auftragsverarbeiter kann man jedoch die Tendenz ablesen, dass bei weitem nicht alle meldepflichtigen Vorgänge gemeldet werden. Ich empfehle weiterhin allen verantwortlichen Stellen und Auftragsverarbeitern ausdrücklich, ein funktionierendes und dynamisches 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 bzw. eindämmen und werden Meldepflichten eingehalten.

14.8 Unangemessene und nicht notwendige Berechtigungen bei Android-Apps

Bietet eine verantwortliche Stelle eine Dienstleistung in Form einer App für mobile Endgeräte an, so muss sie darauf bezogene, geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zu diesen Maßnahmen gehört auch die Prüfung, ob die von der App eingeforderten Berechtigungen notwendig und dem Zweck angemessen sind. Tun sie dies nicht, kann darin ein Datenschutzverstoß – insbesondere gegen die Vorschriften des Art. 5 Abs. 1 Buchst. c und f DS-GVO – liegen, da durch die Datenverarbeitung Verstöße gegen die Grundsätze der Datenminimierung und der Integrität und Vertraulichkeit der Verarbeitung vorliegen können.

Das Berechtigungssystem von Android-Apps

Mobile Apps sind aufgrund ihrer zahllosen Anwendungsfelder aus dem alltäglichen Leben nicht mehr wegzudenken: Vom Busfahrplan über die Wetter-App bis zur elektronischen Patientenakte werden zahlreiche Funktionen als mobile Anwendungen umgesetzt. Dabei werden zwangsläufig auch verschiedenste personenbezogene Daten verarbeitet, die unterschiedliche Schutzniveaus erfordern. Aus diesem Grund ist das Thema „mobile Apps“ auch für mich äußerst relevant.

Installiert der Nutzende eine App auf seinem mobilen Endgerät, so kann er mittels des Berechtigungssystems feststellen, welche Berechtigungen die Entwickler dieser App für sie als notwendig konfiguriert haben und somit durch die App angefordert werden. Das Android-Betriebssystem klassifiziert Berechtigungen hierbei grundsätzlich in die Kategorien „normale Berechtigungen“, „Signaturberechtigung“, „Laufzeitberechtigungen“ und die sogenannten „besonderen Berechtigungen“, die durch den Hersteller des mobilen Endgerätes spezifiziert werden. Nutzende können i. d. R. zumindest bei den „Laufzeitberechtigungen“ festlegen, ob sie dieser App den Zugriff auf diese Berechtigungen gestatten möchten.

Laufzeitberechtigungen – der Hersteller des Betriebssystems deklariert diese auch als „gefährliche Berechtigungen“ – ermöglichen einer App zusätzlichen Zugriff auf eingeschränkte Daten oder lassen die App Aktionen ausführen, die das System und andere Apps wesentlich beeinträchtigen können. Beispiele für solche Berechtigungen sind Zugriffe auf sensible Gerätefunktionen wie der Zugriff auf das Mikrofon oder die Kamera. Viele Laufzeitberechtigungen greifen zudem auch auf private Nutzerdaten zu, die potenziell vertrauliche

Informationen enthalten können. Beispiele hierfür sind Standort- und Kontaktdaten.

Dem Berechtigungssystem unter Android als zentralem Bestandteil des Betriebssystems kommt eine wichtige Rolle dabei zu, wesentliche Anforderungen des Datenschutzes zu gewährleisten. Aus Sicht der Nutzenden tritt das Berechtigungssystem primär durch die folgenden Funktionalitäten in Erscheinung:

– Sie können kontrollieren, auf welche personenbezogenen Daten (wie beispielsweise Bilder oder Kalendereinträge) Apps Zugriff erhalten.
– Sie werden in einem bestimmten Umfang darüber informiert, welche Daten von einer App verwendet werden und warum die App auf diese Daten zugreift.
– Eine App kann nur auf die Daten zugreifen und nur die Daten verwenden, die für eine bestimmte Aufgabe oder Aktion erforderlich sind, die Nutzende ausführen.

Datenschutzrechtliche Risiken

Verwendet eine App unangemessene und nicht notwendige Berechtigungen, so kann dieser Umstand für Nutzende erhebliche Risiken bergen, insbesondere wenn diese Berechtigungen beispielsweise von böswilligen Apps missbraucht werden. Die Beispiele für solche Risiken sind mannigfaltig. Aus technischer Sicht des Datenschutzes ergeben sich u. a. folgende Gefährdungen beim Einsatz von unangemessenen und nicht notwendigen Berechtigungen:

– Apps können auf private Informationen wie Kontakte, Kalender, Nachrichten oder Standort zugreifen und diese ohne Zustimmung des Nutzers speichern oder weitergeben und somit für unerwünschte Zwecke nutzen.
– Der Zugriff auf Telefonnummer, IMEI (Gerätekennung) oder IMSI (Subscriber Identity) kann genutzt werden, um ein Endgerät eindeutig zu identifizieren und Nutzerprofile für Tracking oder Werbung zu erstellen.
– Apps mit Standortberechtigungen können Bewegungsprofile erstellen, Nutzer überwachen und deren Aufenthaltsorte an Dritte übermitteln.
– Apps mit Zugriff auf Anruflisten oder SMS können vertrauliche Informationen wie Zwei-Faktor-Codes abfangen, um Konten zu übernehmen.
– Apps mit Speicherzugriff könnten personenbezogene Daten in der Form von privaten Fotos, Videos oder andere Dateien ohne Zustimmung des Nutzers weitergeben.

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 zu treffen, um ein dem Risiko angemessenes Schutzniveau in den von ihnen angebotenen Apps zu gewährleisten. Hierbei sind insbesondere die Grundsätze der Datenminimierung und der Integrität und Vertraulichkeit der Verarbeitung gemäß Art. 5 Abs. 1 Buchst. c und f DS-GVO zu beachten.

Beschwerde wegen einer App-Berechtigung

Im Berichtszeitraum erreichte mich eine Beschwerde über eine dem Zweck vermeintlich unangemessene und nicht notwendige Berechtigungsanforderung einer Onlinebanking-App. Der Beschwerdeführer teilte mir mit, dass die App eine Freigabe der „Telefon"-Berechtigung voraussetze, anderenfalls würde diese auf seinem mobilen Endgerät nicht funktionieren. Die verantwortliche Stelle, an die er sich zuvor mit diesem Anliegen gewandt habe, würde diese Berechtigung damit begründen, dass nur so ein Zugriff auf die Seriennummer des Endgerätes möglich sei. Dieser Zugriff sei aus sicherheitstechnischen Gründen erforderlich, um die Erstellung von Kopien der App und deren missbräuchlichen Einsatz zu verhindern. Aus Sicht des Beschwerdeführers sei diese Behauptung technisch jedoch nicht haltbar, da seit der Version 10 des Android-Betriebssystems nur noch ausdrücklich privilegierte Apps solche Hardware-Identifier auslesen könnten. Gleichzeitig erlaube es die „Telefon"-Berechtigung einer App jedoch, die Anrufhistorie zu lesen und auch die Handynummer, was aus Sicht des Beschwerdeführers für den Betrieb einer Onlinebanking-App nicht erforderlich sei. Dadurch würde gegen den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchst. c DS-GVO verstoßen. Durch möglichen Missbrauch dieser so gewonnenen Daten würde auch gegen den Grundsatz der Vertraulichkeit, der Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 Buchst. f DS-GVO verstoßen.

In dem vorliegenden Fall fordert die Onlinebanking-App die sogenannte „Telefon"-Berechtigung mit der Bezeichnung READ_PHONE_STATE an. Durch diese Berechtigung werden der App unter anderem die folgenden Zugriffe und Funktionen ermöglicht:

– Die App kann prüfen, ob ein Anruf aktiv ist, aussteht oder das Endgerät sich in einem Ruhezustand befindet.
– Die App kann Informationen über das Mobilfunknetz, wie beispielsweise den Netzbetreibernamen und die Art des Netzwerks, ermitteln.
– Die App kann feststellen, ob neue Voicemail-Nachrichten vorhanden sind oder ob Anrufweiterleitungen aktiviert sind.

– Die App kann in bestimmten Versionen des Android-Betriebssystems und dessen Programmbibliotheken Zugriff auf die Telefonnummer des Geräts, die IMSI und die IMEI nehmen.

Um Missbrauch beim Zugriff auf diese Informationen zu verhindern, werden seit der Version 10 von Android jedoch Zugriffe auf sensible Informationen wie die IMEI oder Telefonnummer durch das Betriebssystem selbst eingeschränkt. Apps benötigen ab dieser Android-Version die Berechtigung READ_PRIVILEGED_PHONE_STATE, diese ist jedoch nur für System-Apps verfügbar. Hervorzuheben ist auch, dass die Version 10 von Android im September 2019 veröffentlicht wurde und alle Endgeräte mit dieser oder einer neueren Version somit den Zugriff mittels READ_PRIVILEGED_PHONE_STATE einer App, die keine System-App ist, auf die IMSI oder IMEI verweigern. Der Marktanteil an Endgeräten mit der Android Version 9 oder älter liegt je nach Quelle bei einem Wert von deutlich unter 15 %. Somit ist der beabsichtigte Zweck der verantwortlichen Stelle kritisch zu hinterfragen, da er auf der überwiegenden Zahl der Android-Endgeräte mit einer aktuelleren Version ohnehin nicht erreicht werden kann. Daher ist die Berechtigung READ_PHONE_STATE, die zwar keinen Zugriff auf die gewünschten, aber dafür auf andere Informationen ermöglicht, nicht dem Zweck angemessen und ihr Setzen verstößt gegen den Grundsatz der Datenminimierung. Aus diesem Grund habe ich den Verantwortlichen auf die aus Datenschutzsicht überflüssige Berechtigung hingewiesen.

Prinzipien bei Entwicklung und Auswahl von Apps mit Blick auf deren Berechtigungen

Um Verstöße dieser Art zu vermeiden, sollten Entwickler also grundsätzlich bei der Entwicklung ihrer Apps und der Implementierung der angeforderten Berechtigungen zumindest die folgenden Prinzipien (sogenannte „Best Practices“) beachten. Diese können weiterhin auch von Verantwortlichen bei der Auswahl von Apps im Sinne einer datenschutzfreundlichen Konfiguration zur Orientierung herangezogen werden:

– Nach dem Prinzip der minimalen Rechte sollten Apps nur Berechtigungen anfordern, die für die vorgesehenen Aufgaben unbedingt nötig sind. Beispielsweise benötigt eine App zur Bearbeitung von Fotos keinen Zugriff auf das Telefonbuch oder den Kalender.
– Nach dem Prinzip der Vermeidung unnötiger sensibler Berechtigungen sollten Entwickler von Apps prüfen, ob es alternative Funktionalitäten zur Erreichung eines Zwecks gibt, die keine oder weniger invasive Berechtigungen benötigen. Beispielsweise reicht es für den Zugriff auf Bilddateien aus, die Android-Schnittstelle „Storage Access Framework“ zu nutzen,

anstatt den vollständigen Speicherzugriff mittels MANAGE_EXTERNAL_STORAGE anzufordern.

– Nach dem Prinzip der kontextbezogenen Berechtigungen sollten Apps Berechtigungen nur dann anfordern, wenn sie benötigt werden und beispielsweise nicht schon direkt beim Start der App. Eine App, die zur Erfüllung einer einzelnen, bestimmten Funktion Zugriff auf die Kamera benötigt, sollte den Zugriff auch nur anfordern, wenn der Nutzende diese Funktion aufruft.
– Nach dem Prinzip der Transparenz und Zweckbindung sollten Apps den Nutzenden darlegen, warum sie auf bestimmte Berechtigungen Zugriff benötigen. Dies ist beispielsweise im Berechtigungsdialog oder durch erklärende Texte in der App möglich.

Darüber hinaus sollten Entwickler regelmäßig Prüfungen ihrer Apps durchführen und kontrollieren, ob Funktionalitäten in Apps weiterhin die angeforderten Berechtigungen benötigen oder diese durch Programmänderungen oder Updates obsolet geworden sind. Verantwortliche sollten ihrerseits prüfen, ob die von Apps angeforderten Berechtigungen für die verfolgten Zwecke noch angemessen und erforderlich sind.

14.9 Fehladressierung von E-Mails aus der Hessischen Landesverwaltung

E-Mails werden verwendet, um ein enorm breites Spektrum an Daten auszutauschen, darunter nicht selten auch personenbezogene Daten. Wird eine E-Mail mit solchen Inhalten an den falschen Empfänger geschickt, etwa aufgrund eines Tippfehlers, kann dies eine Verletzung der Vertraulichkeit der Verarbeitung dieser personenbezogenen Daten darstellen. Hinsichtlich dieses Problems habe ich eine Überprüfung bei der Hessischen Landesverwaltung durchgeführt. Zu Typosquatting bei der Hessischen Polizei s. Kap. 4.6.

Typosquatting als Problem

Bei der Eingabe von Internetadressen in Browsern oder von Empfängeradressen in E-Mail-Clients machen Nutzerinnen und Nutzer im privaten, geschäftlichen oder behördlichen Umfeld leicht Tippfehler. Die so fälschlicherweise adressierte Domain muss nicht zwangsläufig auch tatsächlich registriert sein; die E-Mail würde dann ins Leere laufen und niemandem zur Kenntnis gelangen. In diesem Fall kann dies dem Absender regelmäßig auffallen, da dann eine entsprechende Fehlermeldung von dem verwendeten E-Mail-Client erzeugt werden sollte.

Möglich ist es jedoch auch, dass die Domain registriert ist und dort ein E-Mail-Server die eingehende falsch adressierte E-Mail annimmt. Die Folge ist dann zumindest, dass die E-Mail nicht an den eigentlich vorgesehenen Empfänger ausgeliefert wird. Für den Absender sieht es aber zunächst so aus, als sei die E-Mail erfolgreich ausgeliefert worden. Danach ist die Behandlung der E-Mail durch den unbeabsichtigten Empfänger ausschlaggebend. Im besten Fall stellt dieser den Fehlversand fest und informiert den Absender. Denkbar ist auch, dass er die E-Mail verwirft. Im schlechtesten Fall nutzt der Empfänger die empfangene E-Mail zum Ausspähen oder Missbrauch personenbezogener Daten. Möglich ist es sogar, dass er eine ganz bestimmte Domain in genau dieser Absicht registriert hat und darauf hofft oder es durch sein Vorgehen sogar provoziert, dass er auf diese Weise Zugriff auf vertrauliche Informationen erhält. Diese Art von Angriff wird dann auch als „Typosquatting“ bezeichnet (von engl. „typo“ = „Tippfehler“ und „squatting“ = etwas besetzen oder in Beschlag nehmen). Zu diesem Thema habe ich bereits einen Hinweis mit weitergehenden Informationen auf meiner Website veröffentlicht (https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/typosquatting-wenn-internetadressen-und-e-mails-durch-tippfehler-gefaehrlich-werden).

Verantwortliche sind gemäß Art. 5 Abs. 1 Buchst. f i. V. m. Art. 32 Abs. 1 DS-GVO verpflichtet, die Vertraulichkeit bei der Verarbeitung personenbezogener Daten auf Dauer zu gewährleisten. Hierbei muss auch mit menschlichen Fehlern wie dem Vertippen bei der Adresseingabe gerechnet werden. Es ist daher erforderlich, dass Verantwortliche diesen Fehlern durch geeignete technische und organisatorische Maßnahmen (TOM) begegnen. Hierzu können bspw. regelmäßige oder auch anlassbezogene Sensibilisierungen sowie das Zurverfügungstellen von digitalen Adressbüchern, die eine manuelle Eingabe seltener erforderlich werden lassen, dienen.

Ist es dennoch zu einer unbefugten Offenlegung personenbezogener Daten gekommen, müssen die Verantwortlichen prüfen, ob die Voraussetzungen einer melde- oder benachrichtigungspflichtigen Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 1 respektive Art. 34 Abs. 1 DS-GVO vorliegen und in diesem Fall entsprechend handeln. In jedem Fall ist eine geeignete Dokumentation gemäß Art. 33 Abs. 5 DS-GVO zu erstellen.

Datenschutzüberprüfung

Auch im behördlichen Umfeld kann das Thema der Fehladressierung von E-Mails relevant werden (s. zu Typosquatting bei der Polizei Kap. 4.6). So ist im Berichtszeitraum in einem Arbeitskreis der Hessischen Landesverwaltung zunächst bekanntgeworden, dass eine ganz bestimmte Domain

registriert war, deren Name dem einer offiziell durch das Land genutzten Domain stark ähnelte. Hierbei wurde bereits der Verdacht geäußert, dass es zum unbeabsichtigten Versand von E-Mails an E-Mail-Adressen dieser Domain gekommen sein könnte, insbesondere auch aus der Hessischen Landesverwaltung heraus. Da an diesem Arbeitskreis Vertreterinnen und Vertreter der meisten Ressorts teilnahmen, konnte so bereits an wichtigen Stellen ein erstes Bewusstsein für die Problematik geschaffen werden. In der Folge erreichten mich Meldungen über Verletzungen des Schutzes personenbezogener Daten gemäß § 60 HDSIG, da einige Ressorts selbst Untersuchungen dazu anstellten, ob es bei ihnen zu Fehlversendungen gekommen war.

Bei solchen Meldungen muss jedoch immer auch ein signifikantes Dunkelfeld angenommen werden. Meine Behörde ist bei Verantwortlichen darauf angewiesen, dass sie

1. eine Verletzung des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12 DS-GVO oder § 41 Nr.11 HDSIG zutreffend identifizieren,
2. eine solche Verletzung hinsichtlich ihrer Meldebedürftigkeit gemäß Art. 33 Abs. 1 DS-GVO respektive § 60 Abs. 1 HDSIG korrekt bewerten und
3. mir melden.

Dabei sind Fehler denkbar, die dazu führen, dass mir eine eigentlich meldepflichtige Datenschutzverletzung nicht gemeldet wird. Wegen der grundsätzlichen Bedeutung des Fehlversandes habe ich jedoch das Ziel verfolgt, einen besseren Überblick über das mögliche Dunkelfeld zu erhalten. Daher, und um angemessene, darauf gerichtete Maßnahmen ergreifen zu können, habe ich beschlossen, eine Datenschutzüberprüfung gemäß Art. 58 Abs. 1 Buchst. b DS-GVO durchzuführen.

Hierbei habe ich mich zunächst an die HZD gewandt, da diese die E-Mail-Infrastruktur der Hessischen Landesverwaltung betreibt. Der HZD fallen dabei gemäß § 1 Abs. 2 DV-VerbundG die Pflichten eines Auftragsverarbeiters i. S. d. Art. 28 DS-GVO zu. Ich forderte die HZD auf, mir eine statistische Aufschlüsselung der aus der Landesverwaltung heraus versandten E-Mails für den Prüfzeitraum von Januar bis Mai 2024 vorzulegen, aus der die Domains der Absender und Empfänger sowie jeweils die Anzahl der in diese Richtung versandten E-Mails hervorgehen (Beispiel: Die Domain datenschutz.hessen.de hat im Monat Februar an die Domain posteo.de 20 E-Mails versandt). Weil für den E-Mail-Versand die einzelnen Behörden als Verantwortliche nach DS-GVO und HDSIG gelten, konnte sich diese Darstellung in aggregierter Form auf die jeweiligen Domains beziehen und kam ohne Angabe der genauen, ggf. personenbezogenen, Absender-Adresse (z. B. max.mustermann@datenschutz.hessen.de) aus. Da zur Aufklärung möglicher Fehladressierungen

die Kenntnis von E-Mail-Inhalten nicht erforderlich war, mussten diese auch nicht in die Prüfung einbezogen werden. Die HZD stellte mir die gewünschten Daten anforderungsgerecht zur Verfügung.

Auswertung

Da der Gegenstand der Überprüfung mögliche Typosquatting-Domains waren, war zunächst festzulegen, welche Domains hierfür überhaupt infrage kämen, d. h. welche Domains möglicherweise imitiert würden. Drei Domains wurden hierfür ausgewählt:

1. „hessen.de“, die Domain der Hessischen Landesverwaltung. Sie könnte für Angreifer von Interesse sein, da nahezu alle Dienststellen der Landesverwaltung über eine Domain der Form „SUBDOMAIN.hessen.de“ (Bsp. datenschutz.hessen.de) verfügen, unter der sich ihre E-Mail-Adressen befinden. Durch Imitation dieser Domain könnte ein Angreifer also möglicherweise Zugriff auf Informationen oder personenbezogene Daten erhalten, die für die Landesverwaltung bestimmt sind.
2. „gmx.de“ und „gmx.net“, die E-Mail-Marke der 1&1 Mail & Media GmbH. Diese Domain steht exemplarisch für die E-Mail-Anbieter, die sich an Bürgerinnen und Bürger richten, die mit der Landesverwaltung per E-Mail kommunizieren möchten.
3. „europa.eu“ als Domain wichtiger EU-Institutionen wie der Europäischen Kommission oder dem Europäischen Parlament.

Für alle diese drei Ursprungs-Domains wurden sodann Listen von ihnen ähnelnden Domains generiert, die möglicherweise Typosquatting-Domains darstellen könnten. Zur Generierung dieser ähnlichen Domains wurden mehrere Verfahren genutzt:

1. Auslassung von Buchstaben (Beispiel: hessen.de wird zu hssen.de, hesen.de usw.)
2. Verdopplung von Buchstaben (Beispiel: hessen.de wird zu hhessen.de, heessen.de, hesssen.de usw.)
3. Einfügen von Bindestrichen an beliebiger Stelle (Beispiel: hessen.de wird zu hes-sen.de)
4. Levenshtein-Distanz: Dieses Verfahren berücksichtigt beliebige weitere Veränderungen von Zeichenketten, also Einfügungen, Löschungen oder Veränderungen. Dabei bezeichnet eine Levenshtein-Distanz von 1 genau eine solche Änderung (z. B. Löschung eines Buchstabens), eine Distanz von 2 zwei Änderungen (z. B. eine Löschung und eine Einfügung, zwei Löschungen usw.). Hiermit wurden weitere ähnliche Domains mit jeweils einer Levenshtein-Distanz von 1 generiert.

Es sind eine Vielzahl weiterer Verfahren möglich, bspw. das Austauschen von Buchstaben durch Homophone (gleich oder ähnlich klingende Buchstaben wie e und ä) oder Homoglyphen (gleich oder ähnlich aussehende Buchstaben oder Ziffern wie l, I, und 1); das Austauschen von Domain-Endungen, bspw. de und com oder auch die Kombination mehrerer Varianten. Im vorliegenden Fall wurden jedoch nur die oben gelisteten Verfahren berücksichtigt, um den Prüfauftrag realistisch zeitnah abschließen zu können.

Im nächsten Schritt wurde geprüft, ob die jeweiligen Domains auch tatsächlich im Internet existierten. Hierzu wurde für jede der mit den obigen Verfahren konstruierten Domains mittels einer Domain Name System (DNS)-Abfrage überprüft, ob diese Domain registriert war. Bei dem DNS handelt es sich um ein System, das registrierte Domain-Namen mit den dazugehörigen Adressen von Servern, die unter diesen Domains Inhalte anbieten, verknüpft. Domain-Namen, die dort nicht als registriert bekannt waren, wurden nicht weiter berücksichtigt. Sofern eine Domain registriert und mit einem Nameserver verknüpft war, erfolgte noch eine manuelle Betrachtung dieser Domain, um eine Einschätzung zu deren Verwendungszweck zu erhalten. Dies diente dazu, beispielhaft einen Überblick darüber zu erhalten, ob Variationen der geprüften Domains etwa besonders häufig von überprüfbar existierenden Unternehmen registriert waren. Denkbar wäre auch, dass der Betreiber in bestimmten Fällen eher schwierig zu ermitteln und ein Risiko bei Fehlversand dadurch schwerer zu bewerten wäre (etwa Baustellenseiten oder Domain Parking).

Nach diesem Prüfungsschritt lagen für jede der drei Ursprungs-Domains Listen mit ihnen ähnelnden Domains vor, die auch tatsächlich registriert waren. Die manuelle Betrachtung dieser Domains erlaubte den Ausschluss von der weiteren Auswertung. Die verbliebenen Domains konnten nun in Relation zu den Absender-Domains aus der E-Mail-Statistik gesetzt werden. Hierdurch war es möglich, genau aufzuschlüsseln, welche Behörde in welchem Monat an welche ähnelnden Domains wie viele E-Mails versandt hatte und welche die am häufigsten fälschlicherweise adressierten Domains waren.

Erkenntnisse der Überprüfung

Die Auswertung zeigte deutlich, dass es sowohl bei den Domain-Variationen von „hessen.de“ als auch von „europa.eu“ jeweils eine Domain gab, die deutlicher häufiger adressiert worden war als die anderen. Bei den Variationen von „gmx.de“ und „gmx.net“ zeigte sich ein heterogeneres Bild, was voraussichtlich schon auf die Kürze dieser Domain-Namen zurückzuführen ist: Möglichst kurze Domain-Namen gelten als prägnant und sind daher tendenziell beliebt. Außerdem gibt es zahlreiche Abkürzungen etwa von

Firmennamen, die in diesen Bereich fallen. Aus diesem Grund war es bei dieser Gruppe von Domains wesentlich schwieriger, eine Beurteilung vorzunehmen, ob es sich tatsächlich um unbeabsichtigte Falschschreibungen der Ursprungs-Domain-Namen durch die Absender handelte.

Fehladressierungen an Variationen von „europa.eu“ waren ausschließlich bei einer bestimmten Absender-Domain, also einer Behörde der Landesverwaltung, zu beobachten, was durch deren spezialisiertes Aufgabenfeld mit hohem Bezug zur Europäischen Union hinreichend erklärbar war. An die Variationen von „hessen.de“ wurden durch eine größere Anzahl von Absender-Domains bzw. Behörden fehladressiert. Einige Behörden stachen dabei zahlenmäßig hervor. Teilweise war ein Zusammenhang mit der Mitarbeiterzahl der jeweiligen Behörde zu vermuten. Positiv festzustellen war, dass über den Auswertungszeitraum eine Abnahme der absoluten Zahl der Fehladressierungen festgestellt werden konnte. Ich sehe dies als Indiz dafür, dass der Austausch im Arbeitskreis der Landesverwaltung bereits an wichtigen Stellen für ein Problembewusstsein gesorgt hat. Weniger stark ausgeprägt war dieser Effekt in den nachgeordneten Bereichen der größeren Ressorts, wie etwa bei den Schulen. Hier wäre anzuregen, dass zukünftig angemessene Maßnahmen eine Weitergabe der entsprechenden Informationen sichergestellt werden.

Ausgehend davon, wie häufig solche Fehladressierungen durch bestimmte Behörden vorgenommen worden waren, wurden die obersten 15 Behörden durch mich mit einem auf sie zugeschnittenen Sensibilisierungsschreiben kontaktiert. Hierin waren die bei der Auswertung aufgefallenen Fehladressierungen nach Monaten aufgeschlüsselt, Informationen zu dem Thema Typosquatting waren enthalten und den Verantwortlichen wurde nahegelegt, unter Einbindung ihrer behördlichen Datenschutzbeauftragten eine Sensibilisierung der Mitarbeitenden vorzunehmen. Mögliche Maßnahmen zur besseren Vermeidung von Fehladressierungen waren dabei insbesondere für die Varianten der Domain „hessen.de“ schnell ersichtlich: Die Bediensteten der Hessischen Landesverwaltung sind in dem E-Mail-Programm, das auf ihren Arbeitsplatzrechnern zum Einsatz kommt, in einem gemeinsamen Adressbuch gespeichert. Somit sollte beim Versand von E-Mails innerhalb der Landesverwaltung auf die manuelle Eingabe von Adressen, die anfällig für Tippfehler ist, zugunsten einer Auswahl des Empfängers aus dem Adressbuch möglichst verzichtet werden.

Auch wies ich die Verantwortlichen mit meinem Schreiben darauf hin, dass sie jederzeit mit einer Wiederholung dieser Prüfung rechnen müssen. Je nach Entwicklung und aktuellen Schwerpunkten ist es grundsätzlich auch denkbar, dass dabei das Augenmerk auf anderen Domains liegen könnte oder zusätzliche Methoden zur Überprüfung herangezogen werden.

Sofern es bei den verantwortlichen Stellen noch Rücksprachebedarf bei der Umsetzung wirksamer technischer und organisatorischer Maßnahmen zur besseren Vermeidung von Fehladressierungen gibt, die durch die Einbindung der eigenen Ressourcen, wie der behördlichen Datenschutzbeauftragten und des Datenschutzmanagements, nicht zu klären sind, stehe ich gerne beratend zur Verfügung.

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 personenbezogenen 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 nachzukommen, habe ich im Berichtsjahr im Rahmen zahlreicher Veranstaltungen für unterschiedliche Zielgruppen den Austausch mit der Öffentlichkeit gesucht (Kap. 15.1). Darüber hinaus haben meine Mitarbeitenden und ich im Rahmen von Schulungen (Kap. 15.2), Vorträgen und Podiumsdiskussionen (Kap. 15.3) sowie verschiedenen Veröffentlichungen (Kap. 15.4) datenschutzrechtliche Zusammenhänge erläutert. Diese Anstrengungen zur Öffentlichkeitsarbeit werden ergänzt durch Beiträge in elektronischen Medien (Kap. 15.5) und Kommunikationen mit der Presse (Kap. 15.6). Außerdem habe ich im Berichtsjahr als Vorsitzender der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die Datenschutzaufsichtsbehörden vielfach in der Öffentlichkeit vertreten.

15.1 Veranstaltungen

Die von mir durchgeführten Veranstaltungen dienten einerseits der Diskussion von Fachfragen mit Fachpublikum (z. B. Tagungen) und andererseits der Vorstellung meiner Aufgaben und Tätigkeiten in der Öffentlichkeit (z. B. Messen).

Wiesbadener Forum Datenschutz

Zum 26. Mal haben die Präsidentin des Hessischen Landtages Astrid Wallmann und ich am 7. März 2024 das Wiesbadener Forum Datenschutz veranstaltet. Die Fachtagung im Plenarsaal des Landtags trug den Titel „Der Europäische Gerichtshof als Gestalter des Datenschutzrechts“. Trotz teils erschwerter Anreise aufgrund eines Bahnstreiks haben sich etwa 150 Interessierte aus Wirtschaft, Wissenschaft und Politik im Hessischen Landtag eingefunden. Erörtert wurde das Thema in Vorträgen von Prof. Dr. Christoph Krönke von der Universität Bayreuth („Welche Rolle spielt der Europäische Gerichtshof in der Fortentwicklung des Datenschutzes?“), Prof. Dr. Anne Paschke von der Technischen Universität Braunschweig („Wie präzisiert der Europäische Gerichtshof die Zulässigkeit der Verarbeitung personenbezogener Daten?“), Prof. Dr. Tobias Herbst von der Hochschule für Polizei und öffentliche Verwaltung Nordrhein-Westfalen („Wie versteht der Europäische

Gerichtshof die Verantwortung des Verantwortlichen?“), Dr. Alexander Dix von der Europäischen Akademie für Informationsfreiheit und Datenschutz („Wie gestaltet der Europäische Gerichtshof die Rechte der betroffenen Person aus?“) und dem ehemaligen Hamburgischen Datenschutzbeauftragten Prof. Dr. Johannes Caspar („Welche Rolle weist der Europäische Gerichtshof den Aufsichtsbehörden zu? Eine Kritik des Begriffs der völligen Unabhängigkeit“).

CAST-Forum „Datenhunger Lernender Systeme“

Am 14. März 2024 veranstaltete ich im Rahmen des „Competence Center for Applied Security Technology (CAST)“ zusammen mit der Plattform Privatheit des BMBF eine Tagung zum Thema „Datenhunger Lernender Systeme – Datennutzung und Datenschutz im Rahmen Künstlicher Intelligenz“ in Darmstadt. Lernende Systeme wie Large Language Models (LLM) benötigen für ihr Training und ihre Überprüfung sehr viele Daten. Da sich unter den Trainingsdaten ebenso wie in den Ergebnissen, die LLM ausgeben, meist auch personenbezogene Daten befinden, stellen sich ethische und rechtliche Fragen hinsichtlich der Nutzung der Daten für berechtigte Zwecke und des Schutzes der durch die Datenverwendung betroffenen Personen. Die Tagung fragte danach, wie ein Ausgleich zwischen den Zielsetzungen der KI-Nutzung und den Zielen des Datenschutzes zu finden ist. Ausgangspunkt war eine sachliche Darstellung des Lernverfahrens und der für das Lernen der Systeme benötigten Daten (Dr. Stille, hessen.ai). Thematisiert wurden ethische Fragen wie nach der Transparenz des Lernprozesses und der befürchteten Diskriminierung durch die Anwendung von KI (Prof. Dr. Gehring, ZeVeDi). Soweit personenbezogene Daten verarbeitet werden, stellen sich Fragen, welchen datenschutzrechtlichen Anforderungen solche Systeme unterliegen und wie diese erfüllt werden können, ohne den Nutzen Lernender Systeme in Frage zu stellen (Prof. Dr. Kugelmann, LfDI Rheinland-Pfalz). Weitere wichtige Aspekte des Datenschutzes sind zum einen die Anforderungen an solche Systeme, wenn sie zur Unterstützung von Entscheidungen genutzt werden sollen (Dr. Philipp Richter, LfDI Rheinland-Pfalz), und zum anderen, wenn betroffene Personen ihre Rechte gegenüber den Betreibern Lernender Systeme geltend machen (Prof. Dr. Hornung, Universität Kassel). Eine mögliche Lösung der anstehenden Konflikte könnte darin bestehen, für das Anlernen solche Systeme anonyme Daten zu verwenden. Untersucht wurden daher die Anforderungen, die erfüllt sein müssen, um von einer anonymen Datenverarbeitung ausgehen zu können, die nicht mehr dem Datenschutzrecht unterliegt.

Dritter Datenschutztag Hessen & Rheinland-Pfalz

„Datenschutzbeauftragte auf Zukunftskurs“ – so lautete das Motto des 3. Datenschutztags Hessen & Rheinland-Pfalz, zu dem am 25. Juni 2024 mehr als 200 behördliche, kommunale und betriebliche Datenschutzbeauftragte in Frankfurt am Main zusammenkamen. Die Veranstaltung, die ich, wie schon in den Vorjahren, gemeinsam mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. und dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) Prof. Dr. Dieter Kugelmann ausgerichtet habe, war damit erneut ein voller Erfolg. Der 3. Datenschutztag Hessen & Rheinland-Pfalz bot insgesamt 17, zum Teil parallel stattfindende Keynotes, Fachvorträge und Podiumsdiskussionen. Ein besonderes Merkmal der Tagung ist seit der Premiere vor drei Jahren die Gelegenheit für die Teilnehmenden, sich nicht nur untereinander auszutauschen, sondern mit ihren Fragen auch direkt an die Fachleute aus den Aufsichtsbehörden heranzutreten. Das gilt sowohl für die Tagungspausen als auch für das interaktive Abschlusspanel „Die Aufsichtsbehörden beantworten Ihre Fragen“. Einen inhaltlichen Schwerpunkt der Keynotes und Fachvorträge bildete der Einfluss neuester technischer und gesetzgeberischer Entwicklungen auf die Arbeit der Datenschutzbeauftragten – allen voran der Einfluss Künstlicher Intelligenz und der KI-Verordnung, die sie reguliert.

Tag der offenen Tür im Hessischen Landtag

Am 28. und 29. September 2024 war ich mit meiner Behörde wieder beim Tag der offenen Tür im Hessischen Landtag präsent. Meine Mitarbeitenden stellten an einem Stand die Arbeit der Behörde vor und informierten zu vielfältigen Datenschutzthemen. Mit dabei waren Angebote für Jung und Alt wie Broschüren zu verschiedenen Datenschutzfragen, ein Glücksrad und ein Angelspiel für jüngere Besucherinnen und Besucher sowie Giveaways zur Steigerung der Aufmerksamkeit für den Datenschutz. Von sehr vielen der über 10.000 Besucher der Veranstaltung wurde mein Angebot sehr positiv aufgenommen, was sich in zahlreichen interessierten Gesprächen zeigte. Für Besucherinnen und Besucher, die ein konkretes Anliegen mit fachlichem Bezug mitbrachten, konnten Erstkontakte geknüpft oder vermittelt werden. Zudem habe ich im Rahmen der Veranstaltung wertvolle Rückmeldungen zu besonderen Informationsbedarfen für meine künftige Arbeit erhalten.

Künstliche Intelligenz, Datenschutz ... und Sex!?

Wie schon in den vergangenen Jahren fand auch im Berichtsjahr wieder eine Abendveranstaltung in Kooperation mit der Plattform Privatheit und dem Museum für Kommunikation Frankfurt statt. An der Veranstaltung am

17. Dezember 2024 mit dem Titel „Künstliche Intelligenz, Datenschutz … und Sex!?“ war erstmals auch die Hessische Landeszentrale für politische Bildung mit Informationsangeboten beteiligt. Die Veranstaltung fand im Museum für Kommunikation im Rahmen der dortigen Ausstellung „Apropos Sex“ statt. Im Mittelpunkt der Veranstaltung standen Internet- und KI-Angebote wie Chatbots, die auf intime sexuelle Interaktion ausgerichtet sind. Zu den datenschutzrechtlichen Fragen referierten Priv.-Dozent Dr. Christian Geminn und Dr. Maxi Nebel in ihrem Vortrag „Sichere Selbstoffenbarung? Rechtsfragen intimer Kommunikation mit menschähnlichen Systemen“ von der Universität Kassel sowie Prof. Dr. Jessica Heesen von der Universität Tübingen in ihrem Vortrag „Musternde Blicke. Wie KI Sexobjekte generiert“ zu den ethischen Aspekten. An der anschließenden Podiumsdiskussion unter der Leitung von Jan Eggers, KI-Koordinator des Hessischen Rundfunks, nahm außer den Referenten auch ich teil. Die Veranstaltung im Museum für Kommunikation Frankfurt stieß vor Ort auf großes Interesse, zudem wurde sie live gestreamt und ist auch nachträglich noch abrufbar.

15.2
Schulungen

Mitarbeitende meiner Behörde und ich selbst haben im Berichtszeitraum viele Schulungen veranstaltet, um über Datenschutzfragen zu informieren. Im Folgenden werden die wichtigsten Schulungsveranstaltungen aufgelistet.

Datum	Titel	Referenten
15.2.2024	Informationsfreiheit in Hessen	Stephanie Wetzstein
21.2.2024	Datenschutz in Gesundheitsberufen	Anna Sagel
22.2.2024	Datenverarbeitung durch Google, Facebook und Co.	Prof. Dr. Alexander Roßnagel
06.3.2024	Datenschutz bei der Verarbeitung von Personaldaten in öffentlichen Stellen in Hessen	Stephanie Wetzstein
11.3.2024	Grundlagenseminar zum Datenschutzrecht	Ines Walburg
19./20.3.2024	Datenschutz in Schulen – Basisseminar	Michael Sobota
20.3.2024	Datenschutz bei der Verarbeitung von Personaldaten in öffentlichen Stellen	Stephanie Wetzstein
22.3.2024	Datenschutz bei der Verarbeitung von Personaldaten in öffentlichen Stellen	Stephanie Wetzstein
26.3.2024	Datenschutz für Kommunen	Dr. Sebastian Rapp
16.4.2024	Praxiswissen Datenschutz: Datenschutz in Kommunen	Dr. Sebastian Rapp

17./18.4.2024	Datenschutz in Schulen – Basisseminar	Michael Sobota
17.4.2024	Informationsfreiheit in Hessen	Stephanie Wetzstein
18.4.2024	Datenverarbeitung durch Google, Facebook und Co.	Prof. Dr. Alexander Roßnagel
23./24.4.2024	Datenschutz in Schulen – Basisseminar	Michael Sobota
24.4.2024	Praxiswissen Datenschutz: Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten	Roman Mehner
25.4.2024	Praxiswissen Datenschutz: Datenschutz in Kommunen	Dr. Sebastian Rapp
30.4.2024	Datenschutz in Schulen – Basisseminar	Michal Sobota
6./7.5.2024	Datenschutz in Schulen – Basisseminar	Michael Sobota
14./15.5.2024	Der behördliche Datenschutzbeauftragte	Michael Sobota
16./17.5.2024	Der behördliche Datenschutzbeauftragte	Michael Sobota
16.5.2024	Datenschutz bei der Verarbeitung von Personaldaten in öffentlichen Stellen in Hessen	Stephanie Wetzstein
6.6.2024	Datenschutz für Kommunen	Dr. Sebastian Rapp
2.7.2024	Praxiswissen Datenschutz: Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten	Roman Mehner
3.7.2024	Praxiswissen Datenschutz: Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten	Roman Mehner
5./6.11.2024	Datenschutz in Schulen – Aufbauseminar	Michael Sobota
5.11.2024	Praxiswissen Datenschutz: Datenschutz in Kommunen	Dr. Sebastian Rapp
6.11.2024	Datenschutz bei der Verarbeitung von Personaldaten in öffentlichen Stellen	Stephanie Wetzstein
21./22.11.2024	Datenschutz in Schulen – Aufbauseminar	Michael Sobota

15.3
Vorträge und Podiumsdiskussionen

Mitarbeitende meiner Behörde und ich selbst haben im Berichtszeitraum viele Vorträge gehalten und an Podiumsdiskussionen teilgenommen, um über Praxisfragen des Datenschutzes, politische Entwicklungen, neue Entscheidungen und Datenschutzfragen zu informieren. Im Folgenden werden die wichtigsten Vorträge und Podiumsdiskussionen aufgelistet.

Datum	Vortragstitel	Veranstaltung	Vortragende
26.1.2024	Rechtliche Aspekte datengetriebener Modelle in der Umsetzung in die Versorgung	15. Opinion-Leader-Meeting der DGIM „Trends in Diagnose und Therapie internistischer Krankheitsbilder – kann eine Systemmedizin Realität werden?“, Collegium Glashütten	Prof. Dr. Alexander Roßnagel
6.2.2024	Datenschutz bei Internal Investigations, Umsetzung Hinweisgeberschutzgesetz und Meldewesen nach Whistleblowing und Lieferkettengesetz	BvD Regionalgruppe Frankfurt	Katja Horlbeck
27.2.2024	Die Durchsetzung von Datenschutz gegenüber Unternehmen und Verwaltung	Juristische Fakultät der Tokyo-Universität (mit Livestream), Tokyo	Prof. Dr. Alexander Roßnagel
28.2.2024	Erläuterung aktuell geltende Datenschutzregelung mit Drittstaaten insbesondere USA, Darstellung des Angemessenheitsbeschlusses, Regelung Datenschutz Verwaltung vs. Schulen bzgl. MS O365	AG EDV Rüsselsheim	Katja Horlbeck
28.2.2024	Durchsetzung der Datenschutz-Grundverordnung in der Europäischen Union und in Deutschland	Personal Information Protection Commission Japan (PPC, Datenschutzkommission), Tokyo	Prof. Dr. Alexander Roßnagel

29.2.2024	Die Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union und Deutschland im digitalen Zeitalter	Hitotsubashi-Universität (mit Livestream), Tokyo	Prof. Dr. Alexander Roßnagel
14.3.2024	Anonymisierung und anonyme Nutzung von Daten als Schlüsselfrage	CAST-Forum, „Datenhunger Lernender Systeme – Datennutzung und Datenschutz im Rahmen Künstlicher Intelligenz“, Darmstadt	Prof. Dr. Alexander Roßnagel
14.3.2024	Beschäftigtendatenschutz	Praxistage Datenschutz und Informationssicherheit des VNR Verlags für die Deutsche Wirtschaft AG	Katja Horlbeck
2.5.2024	Datenschutzbeauftragte und Datenschutzaufsichtsbehörden in Deutschland	Digitaldialog Indonesien – Deutschland	Lisa-Marie Lange
23.5.2024	Interessenkonflikte bei Datenschutzbeauftragten in öffentlichen Stellen	Deutsche Hochschule der Polizei, Fortbildungsseminar Rechts- und Anwendungsprobleme des öffentlichen Dienstrechts	Dr. Sebastian Rapp
27.5.2024	Beschäftigtendatenschutz	BvD Sonderseminar	Katja Horlbeck
28.5.2024	Panel: HR-Compliance & interne Ermittlungen – Ein 360-Grad Blick aus Sicht des betrieblichen Datenschutzes, Compliance und der aufsichtsbehördlichen Praxis	BvD-Verbandstage	Katja Horlbeck
28.5.2024	Betroffenenrechte – Umsetzung – Durchsetzung	BvD-Verbandstage	Maria Christina Rost
12.6.2024	Datenschutz im Parlament	Podiumsdiskussion der Stiftung Datenschutz „Datenschutz im Parlament“ in der Parlamentarischen Gesellschaft des Bundestages, Berlin	Prof. Dr. Alexander Roßnagel

24.6.2024	Anhörung zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes, BT-Drs. 20/10859, 24.6.2024	Ausschuss für Inneres und Heimat des Deutschen Bundestages, Berlin	Prof. Dr. Alexander Roßnagel
25.6.2024	Grundlagen für die Aufgabenerfüllung als Datenschutzbeauftragte	3. Datenschutztag Hessen & Rheinland-Pfalz	Prof. Dr. Alexander Roßnagel
25.6.2024	Technische Datenschutzprüfung – (k)ein Grund zur Panik?	3. Datenschutztag Hessen & Rheinland-Pfalz	Rouven Wachhaus/ Martin Meffert
25.6.2024	Aktuelle Fragestellungen aus der kommunalen und behördlichen Praxis	3. Datenschutztag Hessen & Rheinland-Pfalz	Dr. Sebastian Rapp
25.6.2024	#datenschutzskandal – Datenschutzrechtliche Fehltritte bei der Online-Präsenz vermeiden	3. Datenschutztag Hessen & Rheinland-Pfalz	Martin Buchter
25.6.2024	KI-Einsatz in der Verwaltung unter Berücksichtigung des Datenschutzes	3. Datenschutztag Hessen & Rheinland-Pfalz	Katja Horlbeck
25.6.2024	Datenschutz und Sicherheit bei Großveranstaltungen	3. Datenschutztag Hessen & Rheinland-Pfalz	Ines Walburg
25.6.2024	Einführung in die KI-Verordnung aus der Perspektive der Datenschutzaufsicht, Teil 1	BvD Regionalgruppe Frankfurt	Katja Horlbeck
8.7.2024	Datenschutz in der Gesundheitsberichterstattung	Landesarbeitsgemeinschaft Gesundheitsberichterstattung (LAG GBE)	Dr. Nils Gaebel
29.8.2024	Internationale Datentransfers	Digitaldialog Indonesien – Deutschland	Lisa-Marie Lange
31.8.2024	Anonymität in der Rechtsprechung des EuGH und in der Anwendung von KI-Systemen	Zweite Sommerklausur der DSK, Verwaltungsuniversität Speyer	Prof. Dr. Alexander Roßnagel
6.9.2024	Szenarien zur Ausgestaltung einer parlamentarischen Aufsichtsstelle	Veranstaltung „Meinungsaustausch DS-GVO / länderübergreifendes parlamentarisches Aufsichtsgremium“, Hessischer Landtag	Prof. Dr. Alexander Roßnagel

17.9.2024	Stellungnahme zu verbindlichen Beschlüssen in der DSK	Anhörung im Innenausschuss des Landtags Nordrhein-Westfalen	Prof. Dr. Alexander Roßnagel
26.9.2024	Cyberkriminalität, Datensicherheit und Datenschutz aus Sicht des HBDI	73. Jahrestagung des Verbands der Krankenhausdirektoren Deutschlands e. V. (VKD Hessen)	Dr. Nils Gaebel
7.10.2024	KI und Datenschutz	Treffen der Datenschutzbeauftragten der hessischen Landkreise	Silvana Hornjak
8.10.2024	Cyberkriminalität, Datensicherheit und Datenschutz aus Sicht des HBDI	e-Health-Kongress 2024 Rhein-Main und Hessen	Dr. Nils Gaebel
10.10.2024	Wahrnehmung von Betroffenenrechten im Beschäftigungsverhältnis – Dauerbrenner Auskunft	Datenschutztag des Arbeitgeberverbandes Chemie und verwandte Industrien für das Land Hessen e. V.	Katja Horlbeck
10.10.2024	Offener Austausch und Fragerunde mit dem HBDI	12. Kommunaler Datenschutztag 2024 der eKom21, Hanau	Prof. Dr. Alexander Roßnagel
18.10.2024	Datenschutz und Datennutzung	Zweite Digitalministerkonferenz, Futurium Berlin	Prof. Dr. Alexander Roßnagel
22.10.2024	Digitale Identitäten: Wie machen wir die Schlüssel der digitalen Zukunft sicher?, Podiumsdiskussion	Digitalgipfel der Bundesregierung, Kap Europa in Frankfurt	Prof. Dr. Alexander Roßnagel
29.10.2024	Regulierung – Motor oder Hemmschuh der Innovation, 29.10.24, Paneldiskussion	6. Frankfurter Regulierungskonferenz 2024, Frankfurt School of Finance & Management, Frankfurt	Prof. Dr. Alexander Roßnagel
31.10.2024	Einführung in die KI-Verordnung aus der Perspektive der Datenschutzaufsicht, Teil 2	BvD Regionalgruppe Frankfurt	Katja Horlbeck
1.11.2024	Podiumsdiskussion zum Thema KI	Stadt Frankfurt, Leitungskonferenz	Katja Horlbeck
4.11.2024	Rolle des Datenschutzkoordinators im Kontext des Beschäftigtendatenschutzrechts	BvD, Online Schulung „Qualifizierte:r Datenschutzkoordinator:in (BvD)“	Katja Horlbeck

5.11.2024	Datennutzung und Datenschutz – ein Widerspruch?	Treffen der Dozentinnen und Dozenten der Initiative „Datenschutz geht zur Schule“, Wiesbaden	Prof. Dr. Alexander Roßnagel
12.11.2024	Anhörung des Innenausschusses des Hessischen Landtag zum Gesetzentwurf der Fraktion der CDU und der Fraktion der SPD zum Gesetz zur Stärkung der inneren Sicherheit in Hessen	Hessischer Landtag, Wiesbaden	Prof. Dr. Alexander Roßnagel
19.11.2024	Grußwort zur Einführung von Maria Christina Rost als Landesbeauftragte für den Datenschutz Sachsen-Anhalt	Landtag Sachsen-Anhalt, Magdeburg	Prof. Dr. Alexander Roßnagel
21.11.2024	Datenschutz und Datennutzung	DGRI-Jahrestagung „Resilienz im digitalen Wandel“, Universität Kassel	Prof. Dr. Alexander Roßnagel
25.11.2024	Das Volkszählungsurteil des Bundesverfassungsgerichts und seine Bedeutung heute und morgen	IT-Kontrollkommission der Hessischen Gerichtsbarkeit, Hessisches Ministerium der Justiz, Wiesbaden	Prof. Dr. Alexander Roßnagel
25.11.2024	Aktuelles aus der Aufsichtsbehörde	Herbsttagung GDD Herfa Kreis Hessen	Martin Buchter
26.11.2024	KI-Einsatz im Beschäftigungsverhältnis	Baker McKenzie	Katja Horlbeck
4.12.2024	Blitzlicht Datenschutz 2024/25 – Rück- und Ausblick	BvD e. V.	Prof. Dr. Alexander Roßnagel

15.4 Publikationen

Mitarbeitende meiner Behörde und ich selbst haben im Berichtszeitraum viele datenschutzrechtliche Beiträge veröffentlicht. Diese Publikationen enthalten wichtige Antworten auf Fragen des Datenschutzes.

Im Folgenden werden die wichtigsten Vorträge und Podiumsdiskussionen aufgelistet.

Gaebel, N.: Cyberangriffe immer auf dem Radar haben!, Management & Krankenhaus 11/2024, 10.

Horlbeck, K.: Datenschutzrechtliche Herausforderungen der Verwaltungsdigitalisierung, BvD-News 01/2024, 56–61.

Rapp, S.: Interessenkonflikte bei Datenschutzbeauftragten in öffentlichen Stellen, Zeitschrift für Datenschutz (ZD) 2024, 193–197.

Rapp, S.: Datenschutz in Kommunen, KommJuR 2024, 401–422.

Roßnagel, A.: Kommentierung der Art. 2, 4 Nr. 2, 4 Nr. 6, 5, 6 Abs. 1 UAbs. 1 Buchst. c und 3, 6 Abs. 2, 6 Abs. 3, 6 Abs. 4, 40 und 41 sowie §§ 1, 3, 23, 24 und 25 BDSG, in: Simitis, S./Hornung, G./Spiecker gen. Döhmann, I. (Hrsg.), Datenschutzrecht, Kommentar zur DS-GVO und zum BDSG, 2. Aufl., Baden-Baden 2025.

Roßnagel, A.: TeleMediaR – Telekommunikations- und Multimediarecht, dtv-Textsammlung mit einer Einführung. (als Hrsg. zus. m. M. Geppert), Beck-Texte im dtv, 13. Aufl. München 2024, 1061 S.

Roßnagel, A.: Anmerkung zu EuGH vom 11.1.2024, C-231/22, Etat Belge, EuZW 2024, 265, Europäische Zeitschrift für Wirtschaftsrecht (EuZW), 35. Jg. (2024) Heft 4, 269–270.

Roßnagel, A.: Anmerkung zu EuGH vom 30.4.2024, C-470/21, La Quadrature du Net u. a. II, EuZW 2024, 657, Europäische Zeitschrift für Wirtschaftsrecht (EuZW), 35. Jg. (2024) Heft 14, 664–666.

Roßnagel, A.: Datenhunger lernender Systeme (Editorial), Datenschutz und Datensicherheit (DuD), 48. Jg. (2024), Heft 8, 485.

Roßnagel, A.: Festlegungen für die KI-Aufsicht, NJW 41/2024, 3.

Roßnagel, A.: Anonymisierung personenbezogener Daten und Nutzung anonymer Daten, Datenschutz und Datensicherheit (DuD), 48. Jg. (2024), Heft 8, 513–520.

Roßnagel, A.: IT-Sicherheitsinfrastrukturen und -dienste, in: Hornung, G./Schallbruch, M. (Hrsg.), IT-Sicherheitsrecht – Praxishandbuch, 2. Aufl. Baden-Baden 2024, 410–444.

Roßnagel, A./Geminn, C. L.: The GDPR Five Years on – A Retrospective from the Viewpoint of Consumers, European Journal of Consumer Law (EJCL) 2024, 109–129.

Roßnagel, A./Hansen M./Keber, T.: Souveränität und Datenschutz, Frankfurter Allgemeine Zeitung vom 6. Mai 2024, 6.

Roßnagel, A./Rost, C. M.: Geldbußen gegen juristische Personen. Klarstellungen durch zwei Entscheidungen des EuGH vom 5.12.2023, Zeitschrift für Datenschutz (ZD), 14. Jg. (2024), Heft 4, 183–189.

Roßnagel, A./Rost, C. M.: Der EuGH zu Scoring und automatisierte Entscheidungen, BvD-News 01/2024, 20–23.

Roßnagel, A./Wallmann, A.: Der Europäische Gerichtshof als Gestalter des Datenschutzrechts, Nomos Verlag, Reihe Wiesbadener Forum Datenschutz, neue Reihe Band 4, Baden-Baden 2024, 134 S.

15.5
Elektronische Medien

Aus Datenschutzgründen nutze ich keine sozialen Medien, deren wesentliche Zielsetzung es ist, Profile über Nutzer anzulegen und diese für Werbezwecke selbst zu nutzen oder an Dritte weiterzugeben. Die dadurch geringere Reichweite versuchen wir, über andere Mittel auszugleichen.

Homepage

Im Berichtsjahr haben wir intensiv über unsere Homepage im World Wide Web über praktische Fragen des Datenschutzes informiert. Auf der Website wurde im Berichtsjahr 28 Beiträge veröffentlicht und zahlreiche Bereiche inhaltlich aktualisiert.

Mastodon

Im Berichtsjahr haben wir unseren Mastodon-Account im Fediverse weitergepflegt und insgesamt etwa 40 Beiträge veröffentlicht und zahlreiche Anfragen beantwortet. Die Reichweite dieses Kommunikationskanals hat sich dabei im Jahresverlauf wie schon im Vorjahr kontinuierlich erhöht, was unter anderem auf die steigende Bekanntheit der Plattform zurückzuführen sein dürfte.

15.6
Presseanfragen und Pressemitteilungen

Im Berichtsjahr habe ich intensiven Kontakt mit der Presse gehalten. Presseorgane haben insgesamt 52 Presseanfragen an uns gerichtet, die wir alle behandelt haben. Meine Mitarbeitenden und ich haben zudem im Rahmen mehrerer Interviews in Presseorganen zu Datenschutzfragen Stellung genommen.

Im Jahr 2024 habe ich 16 Pressemitteilungen veröffentlicht. Auf besonderes Interesse sind meine Pressemitteilungen zur Deutschen Bahn (Kritik an der Vergabe von Sparpreistickets nur gegen Angabe eine E-Mail oder Mobilfunknummer im Oktober und Abkehr von dieser Praxis aufgrund unserer Kritik im Dezember) und zum Parkraumüberwacher Parkvision gestoßen.

16. Arbeitsstatistik

16.1 Zahlen und Fakten

Die statistische Auswertung der Arbeitsmengen in diesem Kapitel entspricht den formalen Anforderungen, die die Datenschutzkonferenz vorgibt, um bundeseinheitliche Aussagen 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 2023	Fallzahlen 2024
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).	3.520	**3.839**
Beratungen Anzahl von schriftlichen Beratungen. Dies umfasst summarisch Beratungen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. **Nicht:** (Fern-)mündliche Beratungen, Schulungen, Vorträge etc.	1.115	**1.171**
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	**741**
Abhilfemaßnahmen Anzahl der getroffenen Maßnahmen, die im Berichtszeitraum getroffen wurden.	171	**115**
(1) nach Art. 58 Abs. 2 a (Warnungen)	0	**0**
(2) nach Art. 58 Abs. 2 b (Verwarnungen)	31	**55**
(3) nach Art. 58 Abs. 2 c–g und j (Anweisungen und Anordnungen)	16	**13**

(4) nach Art. 58 Abs. 2 i (Geldbußen)	124 in Höhe von Insg. € 56.810	**47** in Höhe von Insg. € 544.986
(5) nach Art. 58 Abs. 2 h (Widerruf von Zertifizierungen)	0	**0**
Genehmigungsverfahren		
(1) BCR-Verfahren (Art. 58 Abs. 2j DS-GVO) mit deutscher oder europaweiter Federführung des HBDI	14	**16**
(2) Akkreditierungsverfahren (Art. 52 Abs. 2e DS-GVO) mit deutscher oder europaweiter Federführung des HBDI	1	**1**
Europäische Verfahren		
(1) Anzahl der Verfahren mit Betroffenheit (Art.56 DS-GVO	13	**289**
(2) Anzahl der Verfahren mit Federführung (Art. 56 DS-GVO)	4	**12**
(3) Anzahl der Verfahren gemäß Kap. VII DS-GVO (Art. 60 ff. DS-GVO)	1.062	**848**
Begleitung bei Rechtsetzungsvorhaben		
Anzahl der Beratungen in Rechtssetzungsverfahren	30	**15**

16.2
Ergänzende Angaben

Die nachstehenden Darstellungen erläutern und ergänzen die Zahlen und Fakten auch im Vergleich mit dem Vorjahr und den weiteren Arbeitsgebieten im Berichtsjahr. Insgesamt hält sich die Zahl der Fälle, die mir zur Kenntnis gelangen, neun Jahre nach dem Inkrafttreten und sieben 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:

Fachbebiete	2023				2024			
	Beschwerden	Beratungen	Hinweise	Eingaben insgesamt	Beschwerden	Beratungen	Hinweise	Eingaben insgesamt
Auskunfteien, Inkasso	456	6	0	**462**	503	4	2	**509**
Schule, Hochschule, Archive	146	109	8	**263**	140	136	13	**289**
e-Kommunikation, Internet	289	36	98	**423**	260	45	112	**417**
Beschäftigtendatenschutz	267	136	16	**419**	287	150	25	**462**
Videobeobachtung	232	88	219	**539**	295	87	306	**688**
Kreditwirtschaft	441	4	7	**452**	401	3	2	**406**
Handel, Handwerk, Gewerbe	167	21	8	**196**	236	17	8	**261**
Verkehr, Geodaten, Landwirtschaft	318	16	55	**389**	342	13	53	**408**
Gesundheit, Pflege	160	81	48	**289**	183	85	55	**323**
Betriebliche/ Behördliche DSB	5	187	0	**192**	6	188	0	**194**
Kommunen, Wahlen	97	139	0	**236**	88	131	7	**226**
Polizei, Justiz, Verfassungsschutz	152	90	34	**276**	196	93	32	**321**
Vereine, Verbände	111	32	8	**151**	105	27	8	**140**
Adresshandel, Werbung	313	4	18	**335**	367	5	9	**381**
Wohnen, Miete	71	36	10	**117**	114	30	17	**161**
Soziales	72	38	4	**114**	83	41	5	**129**
Versorgungsunternehmen	60	8	25	**93**	35	14	51	**100**
IT-Sicherheit, DV-Technik**	7	45	20	**72**	5	46	15	**66**
Versicherungen	76	9	3	**88**	41	9	14	**64**
Rundfunk, Fernsehen, Presse	42	6	10	**58**	43	4	3	**50**

Religionsgemeinschaften	7	1	0	**8**	1	4	0	**5**
Datenschutz außerhalb der EU***					2	10	1	**13**
Forschung, Statistik	5	12	0	**17**	8	17	0	**25**
Ausländerrecht	5	4	0	**9**	3	1	0	**4**
Steuerwesen	18	3	0	**21**	10	2	0	**12**
Zensus	1	0	0	**1**	1	0	0	**1**
Sonstige Themen <10 (z. B. Kammern, Glücksspiel)	2	4	2	**8**	84	9	3	**96**
Zwischensumme Beschwerden, Beratungen und Hinweise	3.520	1.115	593	**5.228**	3.839	1.171	741	**5.751**
Meldungen von Datenpannen*				**1.934**				**2.141**
Gesamtsumme dokumentierter Eingaben				**7.162**				**7.892**
Telefonische Beratungen und Auskünfte von mehr als 10 Minuten**				**3.576**				**3.084**
Gesamtsumme dokumentierter + telefonischer Eingaben				**10.738**				**10.976**

*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 Antworten auf Verständnisfragen zur DS-GVO u. Ä. sowohl zu allgemeinen Themen als auch zu spezifischen Fragestellungen. Exemplarisch werden derartige Telefonate im November, als Monat ohne besondere Vorkommnisse, gezählt und als Durchschnittswert hochgerechnet.

*** 2024 erstmals gesondert ausgewiesen

Abhilfemaßnahmen und Gerichtsverfahren

Abhilfemaßnahmen	Anzahl 2023	Anzahl 2024
(1) Warnungen (Art. 58 Abs. 2 a DS-GVO)	0	**0**
(2) Verwarnungen (Art. 58 Abs. 2 b DS-GVO)	31	**55**
(3) Anweisungen und Anordnungen (Art. 58 Abs. 2 c-g, j DS-GVO)	16	**13**
(4) Geldbußen (Art. 58 Abs. 2 i DS-GVO)	124	**47**
(5) Widerruf von Zertifizierungen (Art. 58 Abs. 2 h DS-GVO)	0	**0**
Gesamt	171	**115**

Gerichtsverfahren	Anzahl 2023	Anzahl 2024
Klagen gemäß Art. 78 Abs. 1 DS-GVO	12	**21**
Klagen gemäß Art. 78 Abs. 2 DS-GVO	4	**6**
Verfahren vor dem VGH in 2. Instanz	6	**7**
Verfahren vor dem Bundesverfassungsgericht	3	**1**
Eilverfahren	1	**1**
Sonstige	1	1
Gesamt	27	**37**

Meldungen von Datenschutzverletzungen nach Art. 33 DS-GVO und §60 HDSIG

Gesamtübersicht		
Grund	**Anzahl 2023**	**Anzahl 2024**
Fehlversand/Fehlzuordnung von Daten/Dokumenten	728	**895**
Hackerangriffe, Phishing, Schadsoftware, Sicherheitslücke	502	**482**
Verlust/ Diebstahl von Unterlagen, Geräten etc.	143	**140**
Unrechtmäßige Offenlegung/Weitergabe von Daten	209	**185**
Unzulässige Einsichtnahme (fehlerhafte Einrichtung von Zugriffsrechten u. a.)	117	**153**
Offener E-Mail-Verteiler	102	**110**
Missbrauch von Zugriffsrechten	79	**92**
Unzulässige Veröffentlichung	25	**34**
Nicht datenschutzkonforme Entsorgung	6	**14**

Unverschlüsselter E-Mail-Versand	17	**21**
Sonstige	6	**15**
Gesamt	**1.934**	**2.141**

Am stärksten betroffene Bereiche	**Fälle 2023**	**Fälle 2024**
Kreditwirtschaft, Auskunfteien, Handel und Gewerbe	718	**537**
Technischer Bereich, IT	466	**477**
Gesundheitsbereich	299	**323**
Beschäftigtendatenschutz	362	**294**

Anhang zu I

Ausgewählte Materialien der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder aus dem Jahr 2024

1. Entschließungen

1.1
Nationalen Zuständigkeiten für die Verordnung zur Künstlichen Intelligenz (KI-VO) vom 3.5 2024

https://www.datenschutzkonferenz-online.de/media/dskb/20240503_DSK_Positionspapier_Zustaendigkeiten_KI_VO.pdf

1.2
Besserer Schutz von Patientendaten bei Schließung von Krankenhäusern vom 15.5.2024

https://www.datenschutzkonferenz-online.de/media/en/2024-05-15_DSK-Entschliessung_Krankenhausschliessung.pdf

1.3
Recht auf kostenlose Erstkopie der Patientenakte kann durch eine nationale Regelung nicht eingeschränkt werden! Datenschutzaufsichtsbehörden sehen konkreten Handlungsbedarf auf Seiten der Heilberufskammern vom 11.9.2024

https://www.datenschutzkonferenz-online.de/media/en/2024-09-11_Entschliessung_DSK_Patientenakte.pdf

1.4

Vorsicht bei dem Einsatz von Gesichtserkennungssystemen durch Sicherheitsbehörden vom 20.9.2024

https://www.datenschutzkonferenz-online.de/media/en/2024-09-20_Entschliessung_DSK_Gesichtserkennung.pdf

1.5
Menschenzentrierte Digitalisierung in der Daseinsvorsorge sicherstellen! vom 19.12.2024

https://www.datenschutzkonferenz-online.de/media/en/2024-12-19_DSK-Entschliessung_Menschenzentrierte-Digitalisierung.pdf

2. Beschlüsse

2.1
Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken vom 15.5.2024

https://www.datenschutzkonferenz-online.de/media/dskb/2024-05-15_DSK-Beschluss_Genetische-Daten.pdf

2.2
Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG) vom 19.8.2024

https://www.datenschutzkonferenz-online.de/media/dskb/2024_08_19_DSK_Beschluss_Bezahlkarte.pdf

2.3
DS-GVO privilegiert wissenschaftliche Forschung – Positionspapier zum Begriff „wissenschaftliche Forschungszwecke“ vom 11.9.2024

https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf

2.4
Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals vom 11.9.2024

https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_Beschluss%20DSK_%20Asset_Deals.pdf

3. Orientierungshilfen und Anwendungshinweise

3.1
Orientierungshilfe zur Einholung von Selbstauskünften bei Mietinteressent:innen Version 1.0 vom 24.1.2024

https://www.datenschutzkonferenz-online.de/media/oh/2024-01-24_DSK-OH_Mietinteresse_V1.0.pdf

3.2
Orientierungshilfe der DSK zu Künstlicher Intelligenz und Datenschutz Version 1.0 vom 6.5.2024

https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

3.3
Datenverarbeitung im Zusammenhang mit funkbasierten Zählern Version 1.0 vom 16.8.2024

https://www.datenschutzkonferenz-online.de/media/oh/240816_DSK_OH_Datenverarbeitung_funkbasierte_Zaehler.pdf

3.4
Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes – Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen, Version 1.0, 11/2024

https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG.pdf

3.5

Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste) Version 1.2, 11/2024

https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf

3.6
Standard-Datenschutzmodell (SDM) Version 3.1 vom 14.5.2024

https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf

II
Zweiter Teil
7. Tätigkeitsbericht zur Informationsfreiheit

1. Entwicklung der Informationsfreiheit

Der vorliegende siebte Tätigkeitsbericht zur Informationsfreiheit beschreibt und analysiert die Informationsfreiheit in Hessen im Jahr 7 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 zu Wahl anstehenden Leiter der öffentlichen Verwaltung nachzuvollziehen und zu bewerten. Sie sollen sich zum anderen, informiert über die Wissensgrundlagen und Handlungsmöglichkeiten der Verwaltung, daran beteiligen können, wie das Gemeinwohl durch Verwaltungshandeln konkretisiert wird. Sie sollen ihre Erfahrungen und ihre Vorstellungen in die aktuelle öffentliche Diskussion einbringen können. Durch das Recht auf Informationszugang gegenüber den öffentlichen Stellen erhalten Bürgerinnen und Bürger die Möglichkeit, unmittelbar Einblick in Vorgänge der öffentlichen Verwaltung zu nehmen. Sie können dadurch Entscheidungen der Verwaltung nachvollziehen, verstehen und leichter akzeptieren. Informationsfreiheit hat somit eine wichtige

demokratische und rechtsstaatliche Funktion, stärkt die bürgerschaftliche Partizipation und die Kontrolle staatlichen Handelns.

Die Bundesrepublik Deutschland und dreizehn Bundesländer haben seit vielen Jahren Informationsfreiheitsgesetze, die den Informationszugang zu allen öffentlichen Stellen eröffnen. In einigen Bundesländern wurden diese Gesetze inzwischen zu Transparenzgesetzen weiterentwickelt, die die öffentliche Verwaltung verpflichten, von sich aus möglichst viele Informationen öffentlich zu stellen.

Hessen war in dieser Entwicklung ein Nachzügler und hat erst vor sieben 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 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 der Landtag sich diesen Entwicklungen angeschlossen und ein Open-Data-Gesetz beschlossen, das am 24. März 2023 in Kraft getreten ist (s. 6. Tätigkeitsbericht zur Informationsfreiheit, 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 siebte Tätigkeitsbericht eine kleine Auswahl. Er greift die Praxis einiger Gemeinden auf, die Informationsfreiheit durch Satzung grundsätzlich einzuführen, aber zugleich für privatrechtlich organisierte kommunale Stellen auszuschließen (Kap. 2). Er untersucht, ob das Informationsfreiheitsrecht auch für öffentliche Stellen, ihre Untergliederungen oder ihre Mitglieder gilt, um Informationen von anderen öffentlichen Stellen oder innerhalb der öffentlichen Stellen zu erlangen (Kap. 3). Gegenüber manchen öffentlichen Stellen, wie gegenüber dem Landtag, den Gerichten oder dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit, gilt das Recht auf Aktenzugang nur, soweit diese Verwaltungsaufgaben wahrnehmen. Daher ist es von hohem praktischen Interesse zu klären, was öffentlich-rechtliche Verwaltungsaufgaben sind (Kap. 4).

2. (Kein) Informationszugang zu privatrechtlich organisierten kommunalen Stellen

Im Gesetzgebungsverfahren zum hessischen Informationsfreiheitsrecht ist man mit Blick auf den kommunalen Satzungsvorbehalt davon ausgegangen, dass im Fall einer solchen Satzung seitens einer Kommune das hessische Informationsfreiheitsrecht für kommunal anwendbar beschlossen ist. Die kommunale Praxis hat jedoch Satzungsvarianten kreiert, die in erster Linie den Informationszugangsausschluss mit Blick auf privatrechtlich organisierte kommunale Stellen im Fokus haben.

Zunächst: Der Kasseler Fall

Ein Bürger beschwerte sich bei mir vor einigen Jahren darüber, dass sein Informationsfreiheitsantrag von der Stadt Kassel zurückgewiesen worden sei. Da die Stadt Kassel jedoch eine Informationsfreiheits-Satzung im Sinne von § 81 Abs. Nr. 7 HDSIG erlassen hatte, forderte ich sie seinerzeit zur Stellungnahme in der Angelegenheit auf. Daraufhin machte mich die Stadt Kassel darauf aufmerksam, dass sie ihre Satzung auf den „eigenen Wirkungskreis" im Sinne von § 2 HGO (Selbstverwaltungsbereich) beschränkt habe und deshalb Weisungsaufgaben und Auftragsangelegenheiten (§ 4 HGO) vom diesem Informationszugang nicht betroffen seien. In dem vorliegenden Fall ging es aber gerade um eine solche Angelegenheit, also eine außerhalb des Selbstverwaltungsbereichs.

Kommunale Satzungen im Übrigen

Viele Städte und Landkreise haben bislang keine Informationsfreiheits-Satzungen erlassen, die meisten größeren Städte allerdings mittlerweile schon (insb. auch Wiesbaden, Frankfurt am Main, Darmstadt, Offenbach). Außer Wiesbaden beschränken diese Städte und auch Landkreise den Informationszugang explizit auf den „eigenen Wirkungskreis" (§§ 2 HGO, 2 HKO) und das bedeutet auch hier – kommunal-rechtssystematisch betrachtet – die Verneinung des Informationszugangs im Kontext von Weisungsaufgaben und Auftragsangelegenheiten (§§ 4 HGO, 4 HKO). Vor diesem Hintergrund ist allerdings folgende Entwicklung für mich „überraschend" gewesen:

Der Landkreis Darmstadt-Dieburg hat seine Informationsfreiheits-Satzung wieder aufgehoben. Ich habe diesen Landkreis dazu um Stellungnahme gebeten. Aus seiner Antwort ging hervor, und das war für mich unerwartet, dass er auch Informationsfreiheits-Anträge beauskunftet hatte, die den Weisungs- und Auftragsbereich betrafen, obwohl in seiner Satzung die

Informationsfreiheit auf den „eigenen Wirkungskreis“ begrenzt worden war. Dies war ein Indiz für mich, dass mit dieser Begrenzung auf den „eigenen Wirkungskreis“ offenbar ein anderes Ziel verfolgt wird.

Der „Bedeutungs-Wechsel“

Auch die Stadt Darmstadt beschränkt die Informationsfreiheit auf den eigenen Wirkungskreis. Eine Rückfrage ergab jedoch auch, dass Weisungs- und Auftragsangelegenheiten beauskunftet würden und die Einschränkung „eigener Wirkungskreis“ als Satzungsformulierung nur dazu diene, privatrechtlich organisierte Stellen der Kommune auszunehmen.

Auch die Stadt Frankfurt am Main ist dementsprechend verfahren. Offenbar besteht die Befürchtung, ohne die explizite Nennung (nur) des „eigenen Wirkungskreises“ in die Situation zu geraten, dass auch privatrechtlich organisierte Stellen der Kommune auskunftspflichtig werden. Dass genau dies nicht eintritt, soll durch die exklusive Hervorhebung (nur) des eigenen Wirkungskreises sichergestellt werden.

Die Stadt Wiesbaden geht stattdessen davon aus, dass das hessische Informationsfreiheitsrecht ohnehin nur für ihre unmittelbare, öffentlich-rechtlich organisierte Kommunalverwaltung gilt, also eben nicht für ihre aus der originären Stadtverwaltung ausgelagerten, privatrechtlich verfassten Stellen.

Diese Auffassung der Stadt Wiesbaden ist aus meiner Sicht jedenfalls vertretbar. Das Auskunftsverfahren nach § 87 HDSIG ist als öffentlich-rechtliches Verwaltungsverfahren im Sinne der §§ 9 ff. HVwVfG ausgestaltet und verpflichtet und befugt zum Erlass eines Verwaltungsakts (bei Drittbetroffenheit also auch eines belastenden Verwaltungsakts). Außerdem ist nach § 88 HDSIG eine öffentlich-rechtliche Kostenbescheidung vorgesehen. Es bestehen daher zumindest Zweifel, ob durch die §§ 80 und 81 (Abs. 1 Nr. 7) HDSIG angesichts der §§ 87 und 88 HDSIG im Ergebnis auch privatrechtlich organisierte Stellen der Kommunen gesetzlich hinreichend erfasst werden. Freilich ist diese Fragestellung eher von theoretischer Natur. Denn die Kommunen sind ja in jedem Fall berechtigt, auf der Grundlage von § 81 Abs. 1 Nr. 7 HDSIG den Informationszugang für privatrechtlich organisierte kommunale Stellen per Satzung auszuschließen. Im Gesetzgebungsverfahren ging man von speziell formulierten Satzungen zwar nicht aus, aber der Wortlaut des § 81 Abs. 1 Nr. 7 HDSIG lautet ja schließlich „soweit“ und das gewährleistet somit kommunale Gestaltungsfreiheit für solche Satzungen.

3. Informationsfreiheitsrecht: Jeder ist nicht „Jeder“

Das Informationsfreiheitsrecht hat den Zweck, die demokratische Meinungs- und Willensbildung der Zivilgesellschaft zu unterstützen, indem es die Transparenz der öffentlichen Hand gegenüber der Zivilgesellschaft mittels der gesetzlichen Verankerung von Informationszugangsansprüchen erhöht. Das Informationsfreiheitsrecht ist kein Mittel, das der öffentlichen Verwaltung und ihren Untergliederungen oder Mitgliedern selbst zur Informationsbeschaffung zur Verfügung steht.

Der Anlass

In den ersten Jahren seit Geltung des hessischen Informationsfreiheitsrechts (2018) gab es mehrere kommunale Anfragen, ob Mitglieder von Gemeindevertretungen gegenüber dem jeweiligen Gemeindevorstand im Wege eines gestellten Informationsfreiheitsantrages amtliche Informationen beanspruchen können.

Ein weiteres Beispiel aus dem Wirkungskreis der öffentlichen Verwaltung ist die in Hessen in letzter Zeit aufgetretene Frage, ob bspw. ein Personalrat oder ein Mitglied des Personalrats etwa von seinem Dienstherrn oder der sonstigen öffentlichen Verwaltung unter Berufung auf das Informationsfreiheitsrecht amtliche Informationen für seine Aufgaben als Personalrat verlangen kann.

Rechtliche Bewertung

Gemeindevertreter und Gemeindevertreterinnen oder auch etwa ein Personalratsmitglied machen regelmäßig geltend, das Informationsfreiheitsrecht spreche mit Blick auf die Innehabung von Informationszugangsansprüchen von „jeder“ und als natürliche Person sei man ein solcher „Jeder“.

In der Tat ist es so, dass der Normtext des Informationsfreiheitsrechts, auch der des hessischen Informationsfreiheitsrechts, so ausgestaltet ist. Das hessische Informationsfreiheitsrecht ist der Vierte Teil des Hessischen Datenschutz- und Informationsfreiheitsgesetzes (§§ 80 ff. HDSIG).

§ 80 Abs. 1 S. 1 HDSIG

(1) Jeder hat nach Maßgabe des Vierten Teils gegenüber öffentlichen Stellen Anspruch auf Zugang zu amtlichen Informationen (Informationszugang).

Die alleinige Orientierung am Wortlaut „Jeder“ ist jedoch verfehlt. Geboten ist vielmehr, bei der Auslegung dieses Rechtsbegriffs „Jeder“ den Sinn und Zweck des Informationsfreiheitsrechts zu berücksichtigen.

Dieser besteht ja nicht darin, Informationszugangsansprüche der öffentlichen Verwaltung oder der ihr angehörigen natürlichen Personen im Kontext von deren amtlichen Funktionen zu schaffen. Maßgebend für die Anspruchsberechtigung ist vielmehr das Kriterium, dass ein zivilgesellschaftlicher Anspruchskontext gegenüber der öffentlichen Verwaltung mit Blick auf den Informationszugangsantrag besteht.

Dass (nur) dieses rechtliche Interpretationskonzept (also eine teleologische Auslegung) mit Blick auf den Rechtsbegriff „Jeder“ sinnvoll ist, ergeben zusätzlich auch Folgeüberlegungen.

Würde man es nämlich schon für hinreichend, es also für allein entscheidungserheblich halten, dass eine natürliche Person den Antrag stellt, hätte das recht skurrile rechtliche Konsequenzen:

Beispielsweise könnte dann jedes Mitglied einer hessischen Gemeindevertretung leicht das von § 50 Abs. 2 Satz 2 HGO geforderte Quorum im Kontext der Überwachung der Gemeindeverwaltung neutralisieren oder konterkarieren.

§ 50 Abs. 2 Satz 2 HGO

Sie kann zu diesem Zweck in bestimmten Angelegenheiten vom Gemeindevorstand in dessen Amtsräumen Einsicht in die Akten durch einen von ihr gebildeten oder bestimmten Ausschuss fordern; der Ausschuss ist zu bilden oder zu bestimmen, wenn es ein Viertel der Gemeindevertreter oder eine Fraktion verlangt.

Diese Vorschrift würde nunmehr in die Leere laufen, wenn Gemeindevertreter, die dieses Ein-Viertel-Quorum nicht erreichen, berechtigt wären, die begehrten Informationen im Wege eines Informationszugangsantrages zu beanspruchen, unter Hinweis, sie seien ja natürliche Personen.

Ganz generell soll aber vor allem auf ein jüngeres Urteil des BVerwG hingewiesen werden, das die Frage behandelt, wer berechtigter Antragsteller zur Ausübung des Informationsfreiheitsrechts sein kann. Es betont, dass dieses nur der Zivilgesellschaft, nämlich natürliche Personen und juristische Personen des Privatrechts, zusteht, und stellt ausdrücklich klar, dass juristische Personen des öffentlichen Rechts nicht antragsberechtigt sind (BVerwG, Urt. v. 20.3.236, C 8.22, Rn. 58).

Das bedeutet also, dass beispielsweise der Freistaat Bayern, vertreten durch den Ministerpräsidenten Markus Söder, nicht berechtigt wäre, bei der

hessischen Staatskanzlei einen Informationszugangsantrag zu stellen. Die Staatskanzlei könnte und müsste diesen Antrag also zu Recht zurückweisen. Es sollte auf der Hand liegen, dass diese Rechtslage nicht dadurch ausgehebelt werden kann, dass nunmehr Markus Söder persönlich diesen Antrag stellt unter Hinweis, er stelle diesen jetzt als natürliche Person und er sei deshalb ein „Jeder“ im Sinne des Informationsfreiheitsrechts.

Bislang und auch in Zukunft werde ich daher als Informationsfreiheitsbeauftragter (§ 89 HDSIG) natürliche Personen nicht unterstützen, die im Kontext eines öffentlichen Amtes Informationsfreiheitsanträge stellen, sei es als Gemeindevertreter oder sei es als Personalrat.

4. Was sind öffentlich-rechtliche Verwaltungsaufgaben?

Der Anspruch auf Informationszugang besteht nach § 81 Abs. 1 HDSIG gegenüber manchen öffentlichen Stellen nur, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen. Dies gilt nach Nr. 1 für den Hessischen Landtag, nach Nr. 3 für den Hessischen Datenschutzbeauftragten, nach Nr. 4 für die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden und sonstige in § 40 Abs. 2 HDSIG genannten Stellen sowie Disziplinarbehörden und nach Nr. 8 für den Hessischen Rundfunk. Da der Umstand, Verwaltungsaufgaben wahrzunehmen, darüber entscheidet, ob ein Anspruch auf Informationszugang besteht, ist es von hohem praktischen Interesse zu klären, was öffentlich-rechtliche Verwaltungsaufgaben sind.

Informationszugang gegenüber der Justiz

Im Berichtszeitraum erreichte mich eine Beschwerde gegen ein Landgericht in Hessen. Ein Rechtsanwalt hatte dort Auskunft über alle unter Beteiligung einer bestimmten Krankenkasse geführten Gerichtsverfahren verlangt, um eine sich aus der Zwangsvollstreckung ergebende Auskunft der Krankenkasse auf deren Richtigkeit überprüfen zu können. Das Gericht hatte den Informationszugang nach dem Vierten Teil des HDSIG verweigert und damit argumentiert, dass nach § 80 Abs. 2 HDSIG die Vorschrift des § 299 ZPO den Anspruch auf Einsicht in Gerichtsakten abschließend regelt.

§ 299 Abs. 1 und 2 ZPO

(1) Die Parteien können die Prozessakten einsehen und sich aus ihnen durch die Geschäftsstelle Ausfertigungen, Auszüge und Abschriften erteilen lassen.

(2) Dritten kann der Vorstand des Gerichts ohne Einwilligung der Parteien die Einsicht der Akten nur gestatten, wenn ein rechtliches Interesse glaubhaft gemacht wird.

§ 80 Abs. 2 HDSIG

(2) Soweit besondere Rechtsvorschriften die Auskunftserteilung regeln, gehen sie den Vorschriften des Vierten Teils vor.

Der Rechtsanwalt legte daraufhin bei mir Beschwerde ein und argumentierte, er habe keine Einsicht in Gerichtsakten verlangt, sondern lediglich eine Übersicht über die unter die Beteiligung der genannten Krankenkasse geführten Verfahren. Diese Beschwerde habe ich jedoch zurückgewiesen.

Der Argumentation des Gerichts, nach der ein allgemeiner Informationszugangsanspruch durch eine speziellere Vorschrift verdrängt wird, ist Folge zu leisten (so auch VG Weimar vom 8. Mai 2023, bislang nicht veröffentlicht). Diese speziellere Vorschrift ist hier § 299 ZPO. Selbst wenn man jedoch annehmen würde, dass die Information, in welchen Verfahren eine bestimmte Krankenkasse beteiligt war, nicht zu den Gerichtsakten gehört, scheidet ein Informationszugangsanspruch aus.

Es handelt sich bei der angefragten Information nicht um eine solche, die öffentlich-rechtliche Verwaltungsaufgaben des Gerichts betrifft. Nach § 81 Abs. 1 Nr. 4 HDSIG besteht gegenüber der Justiz ein Anspruch auf Informationszugang nur, soweit diese öffentlich-rechtliche Verwaltungsaufgaben wahrnimmt.

§ 81 HDSIG

(1) Nach Maßgabe des § 2 Abs. 1 bis 3 gelten die Vorschriften über den Informationszugang auch für (…)

4. die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden und sonstige in § 40 Abs.2 genannten Stellen, jedoch nur soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen und nicht, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln.

Eine einheitliche Definition für den Begriff der öffentlich-rechtlichen Verwaltung gibt es nicht (Bogumil, Öffentliche Verwaltung, Bundeszentrale politische Bildung, https://www.bpb.de/kurz-knapp/lexika/handwoerterbuch-politisches-system/511486/oeffentliche-verwaltung/). Eine Definition für den Begriff des Verwaltungsverfahrens findet sich in § 9 HVwVfG.

§ 9 HVwVfG

Das Verwaltungsverfahren im Sinne dieses Gesetzes ist die nach außen wirkende Tätigkeit der Behörden, die auf die Prüfung der Voraussetzungen, die Vorbereitung und den Erlass eines Verwaltungsaktes oder auf den Abschluss eines öffentlich-rechtlichen Vertrages gerichtet ist; es schließt den Erlass des Verwaltungsaktes oder den Abschluss des öffentlich-rechtlichen Vertrages ein.

Der Begriff der öffentlich-rechtlichen Verwaltungsaufgabe ist weiter gefasst und enthält nicht nur Tätigkeiten der Behörden, die auf die Vorbereitung und den Erlass eines Verwaltungsakts oder den Abschluss eines öffentlich-rechtlichen Vertrags gerichtet sind. Das Einführungsgesetz zum Gerichtsverfassungsgesetz (EGGVG) spricht von Justizverwaltungsakten. Diese sind in § 23 Abs. 1 EGGVG näher beschrieben.

§ 23 Abs. 1 EGGVG

Über die Rechtmäßigkeit der Anordnungen, Verfügungen oder sonstigen Maßnahmen, die von den Justizbehörden zur Regelung einzelner Angelegenheiten auf den Gebieten des bürgerlichen Rechts einschließlich des Handelsrechts, des Zivilprozesses, der freiwilligen Gerichtsbarkeit und der Strafrechtspflege getroffen werden, entscheiden auf Antrag die ordentlichen Gerichte. Das gleiche gilt für Anordnungen, Verfügungen oder sonstige Maßnahmen der Vollzugsbehörden im Vollzug der Untersuchungshaft sowie derjenigen Freiheitsstrafen und Maßregeln der Besserung und Sicherung, die außerhalb des Justizvollzuges vollzogen werden.

Diese Justizverwaltungsakte sind vom Bereich der justiziellen Tätigkeit der Gerichte abzugrenzen. Dieser umfasst die rechtsprechende Gewalt. Der justizielle Bereich ist vom Anspruch auf Informationszugang ausgenommen. Dies liegt vor allem daran, dass in diesem Bereich personenbezogene Daten regelmäßig der Auskunftserteilung im Weg stehen werden (Gesetzesbegründung, LT-Drs. 19/5728, S. 127). Zudem trägt der Gesetzgeber mit der Vorschrift der richterlichen Unabhängigkeit einerseits und dem notwendigen Schutz der Verfahrensbeteiligten andererseits Rechnung (Geminn in: Roßnagel, HDSIG, 2021, § 81 Rn. 12).

Die Information, ob und in welchen Fällen eine bestimmte natürliche oder juristische Person Verfahrensbeteiligte war, betrifft die Durchführung von Gerichtsverfahren und daher den justiziellen Bereich und nicht eine öffentlich-rechtliche Verwaltungsaufgabe des Gerichts. Die Bremer Landesbeauftragte für Informationsfreiheit käme hier wohl zu einem anderen Ergebnis. Denn sie vertritt die Auffassung, dass die Entscheidung über die Herausgabe einer Entscheidungsabschrift eine öffentlich-rechtliche Verwaltungsaufgabe des Gerichts sei (17. Jahresbericht der Bremer Landesbeauftragten für Informationsfreiheit, Ziffer 3.1). Bei der Information, in welchen Verfahren eine bestimmte Person Beteiligte war, fehlt es jedoch an einer nach außen gerichteten Verwaltungstätigkeit. Die Rechtsprechung hat z. B. für Geschäftsverteilungspläne bei einem Gericht keine Justizverwaltungstätigkeit angenommen, sondern justizielles Handeln (VG Gelsenkirchen vom 18. Oktober 2020, Az. 20 K 4062/18, juris; VG Gelsenkirchen vom 20. Februar 2020, Az. 20 K 4063/18, juris). Die Information über die Parteien und Beteiligten eines Gerichtsverfahrens unterfällt ebenfalls dem justiziellen Bereich. Dies bedeutet, dass der Anspruch auf Informationszugang in dem vorliegenden Fall nach § 80 Abs. 1 Nr. 4 HDSIG ausgeschlossen war.

Informationszugang gegenüber dem Hessischen Landtag

Auch gegenüber dem Landtag besteht nach § 81 Abs. 1 Nr. 1 HDSIG ein Anspruch auf Informationszugang nur, soweit dieser öffentlich-rechtliche Verwaltungsaufgaben wahrnimmt und auszuschließen ist, dass durch die Gewährung des Informationszugangs die Freiheit des Mandats, der Bereich der Abgeordneten- und Fraktionsangelegenheiten sowie die Nichtöffentlichkeit von Landtagsberatungen beeinträchtigt wird.

§ 81 HDSIG

(1) Nach Maßgabe des § 2 Abs. 1 bis 3 gelten die Vorschriften über den Informationszugang auch für

1. *den Landtag, nur soweit er öffentlich-rechtliche Verwaltungsaufgaben wahrnimmt und auszuschließen ist, dass durch die Gewährung des Informationszugangs die Freiheit des Mandats, der Bereich der Abgeordneten- und Fraktionsangelegenheiten sowie die Nichtöffentlichkeit von Landtagsberatungen beeinträchtigt wird.*

Beim Hessischen Landtag waren im Berichtszeitraum Mitschriften des „Forums Datenschutz“ angefragt worden. Die antragstellende Person berief sich auf die Vorschriften zum Informationszugang.

Das Wiesbadener Forum Datenschutz wird im Hessischen Landtag von der Präsidentin des Hessischen Landtags und dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit veranstaltet. Einer breiten Öffentlichkeit soll an aktuellen Fragestellungen vermittelt werden, welche besonderen Facetten, Antworten und Konsequenzen das Recht auf Schutz der persönlichen Daten heute haben kann (s. https://datenschutz.hessen.de/service/wiesbadener-forum-datenschutz).

Beim Forum Datenschutz handelt es sich um eine wissenschaftliche Veranstaltung und nicht um eine Landtagsanhörung oder amtliche Handlung. Mit der Veranstaltung hat der Hessische Landtag keine öffentlich-rechtlichen Verwaltungsaufgaben wahrgenommen.

Es fehlt für einen Anspruch auf Informationszugang bereits an dem Tatbestandsmerkmal der „amtlichen Informationen“, zu denen § 80 Abs. 1 Satz 1 HDSIG einen Informationszugangsanspruch gewährt. Dies sind nach § 80 Abs. 1 Satz 3 HDSIG „zu amtlichen Zwecken dienende Aufzeichnungen“.

§ 80 Abs. 1 HDSIG

Jeder hat nach Maßgabe des Vierten Teils gegenüber öffentlichen Stellen Anspruch auf Zugang zu amtlichen Informationen (Informationszugang). Abweichend von § 2 Abs. 2 Satz 1 gelten insoweit auch öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, als öffentliche Stellen. Amtliche Informationen sind alle amtlichen Zwecken dienende Aufzeichnungen, unabhängig von der Art ihrer Speicherung. Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen, gehören nicht dazu.

Eine wissenschaftliche Veranstaltung mit wissenschaftlichen Vorträgen dient keinen amtlichen Zwecken. Die Vorträge von Wissenschaftlern stellen außerdem keine Aufzeichnungen für amtliche Zwecke dar. Daher habe ich auch hier einen Anspruch auf Informationszugang abgelehnt. Selbst wenn man diesen jedoch dem Grunde nach bejahen würde, ist zu berücksichtigen, dass die Autorinnen und Autoren für die Vorträge Urheberrechte haben, die nicht durch das Informationsfreiheitsrecht ausgehebelt werden können.

5. Arbeitsstatistik Informationsfreiheit

Im Vergleich zum Vorjahr nahmen sowohl die Beschwerden als auch die Beratungen zu.

IFG	2023	2024
Beschwerden	55	**65**
Beratungen	44	**51**

Anhang zu II

Ausgewählte Materialien der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) aus dem Jahr 2024

1. Entschließungen

1.1
Entschließung der 45. und 46 IFK zum Superwahljahr vom 4.6.2024

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/45_46_Konferenz_Entschlie%C3%9Fung-Superwahljahr.pdf?__blob=publicationFile&v=3

1.2
Entschließung der 46. IFK zur Pflicht zur Informationsfreiheit und Transparenz vom 5.6.2024

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/46_Konferenz_Entschlie%C3%9Fung-Pflicht-IF-Transparenz.pdf?__blob=publicationFile&v=4

1.3
Entschließung der 46. IFK zum Informationsanspruch gegenüber Rundfunkanstalten vom 5.6.2024

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/46_Konferenz_Entschlie%C3%9Fung-Rundfunkanstalten.pdf?__blob=publicationFile&v=4

1.4
Entschließung der 47. IFK zum Transparenzgesetz für Niedersachsen vom 27.11.2024

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/47_Konferenz_Entschlie%C3%9Fung-TG-Niedersachsen.pdf?__blob=publicationFile&v=3

2. Handreichungen der Informationsfreiheitsbeauftragten in Deutschland

2.1
Praxishandreichungen zur Ausgestaltung von öffentlichen Transparenzportalen vom 13.3.2025

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/Handreichungen-IFK/Praxishandreichung-Transparenzportale.pdf?__blob=publicationFile&v=1

2.2
Prinzipien der Informationsfreiheit und Umsetzungshinweise zur „Informationsfreiheit by Design“ (mit einem besonderen Fokus auf die E-Akte) vom 3.5.2024

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/Handreichungen-IFK/Prinzipien-Umsetzungshinweise-IF-by-Design.pdf?__blob=publicationFile&v=3

Verzeichnis der Abkürzungen

Abkürzung	ausgeschriebene Schreibweise
a. a. O.	am angegebenen Ort
Abs.	Absatz
Alt.	Alternative
AO	Abgabenordnung
Art.	Artikel
Art.	Artikel, mehrere
Aufl.	Auflage
ATD	Antiterrordatei
ATDG	Antiterrordateigesetz
Az	Aktenzeichen
BAR	Bundesarbeitsgemeinschaft für Rehabilitation
BCR	Binding Corporate Rules (verbindliche interne Datenschutzvorschriften)
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für Datenschutz und Informationsfreiheit
BGBl	Bundesgesetzblatt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
bspw.	beispielsweise
BT-Drucks.	Bundestags-Drucksache
BTLE	Borders, Travel & Law Enforcement (Subgroup)
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts

BvF	Registerzeichen für Normenkontrollverfahren
BvR	Aktenzeichen für eine Bundesverfassungs-beschwerde
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa
CC	Carbon Copy = Kohlepapierdurchschlag; Kopie besonders einer E-Mail
CCZ	Corporate Compliance Zeitschrift
CD	Compact Disc
DGUV	Deutsche Gesetzliche Unfallversicherung
d. h.	das heißt
DIN	Deutsches Institut für Normung
DNS	Domain Name System
DOC	Department of Commerce (US-Handelsministeri-um)
DS-GVO, DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichts-behörden des Bundes und der Länder; kurz: Datenschutzkonferenz
DVD	Digital Versatile Disc
DV-VerbundG	Datenverarbeitungsverbundgesetz
EDSA	Europäischer Datenschutzausschuss
EG	Europäische Gemeinschaft
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz
EGMR	Europäischer Gerichtshof für Menschenrechte
E-Mail	electronic mail
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
EU-US DPF	EU-US Data Privacy Framework

e. V.	eingetragener Verein
EWR	Europäischer Wirtschaftsraum
f.	folgende
ff.	folgende (Seiten) / fortfolgende
FAQ	Frequently Asked Questions
GCP	Good Clinical Practice
gem.	gemäß
GE	Gemeinsame Empfehlung
GewO	Gewerbeordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GKV	Gesetzliche Krankenversicherung
GRCh	Charta der Grundrechte der Europäischen Union
HBDI	Hessischer Beauftragter für Datenschutz und Informationsfreiheit
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz
Hessen3C	Hessen CyberCompetenceCenter
HGO	Hessische Gemeindeordnung
HKHG	Hessisches Krankenhausgesetz
HKO	Hessische Landkreisordnung
HLfGP	Hessisches Landesamt für Gesundheit und Pflege
HLKA	Hessisches Landeskriminalamt
HLStatG	Hessisches Landesstatistikgesetz
HLT	Hessischer Landtag
HMKB	Hessisches Ministerium für Kultus, Bildung und Chancen
HöMS	Hessische Hochschule für öffentliches Management und Sicherheit
HSchG	Hessisches Schulgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung

HVSG	Hessisches Verfassungsschutzgesetz
HVwVfG	Hessisches Verwaltungsverfahrensgesetz
HZD	Hessische Zentrale für Datenverarbeitung
i. d. R.	in der Regel
insb.	insbesondere
i. S. d.	Im Sinne der/des
i. V. m.	in Verbindung mit
IT	Information Technologie
IT-Dienst	Informationstechnischer Dienst
IT-Infrastruktur	Informationstechnische Infrastruktur
IT-Projekt	Informationstechnisches Projekt
IT-System	Informationstechnisches System
Kap.	Kapitel
KI	Künstliche Intelligenz
KI-VO	Verordnung über künstliche Intelligenz
KRITIS	Kritische Infrastrukturen
KritisV	KRITIS-Verordnung
KWG	Kreditwesengesetz
LKA	Landeskriminalamt
lit.	Litera, Buchstabe
LfV Hessen	Landesamt für Verfassungsschutz Hessen
LLM	Large Language Model
MStV	Medienstaatsvertrag
MVZ	Medizinisches Versorgungszentrum
m. w. N.	mit weiteren Nachweisen
Nr.	Nummer
o. Ä.	oder Ähnliche
o. g.	oben genannt/oben genannte/oben genannter etc.
OLG	Oberlandesgericht
OWASP	Open Web Application Security Projects
OWiG	Gesetz über Ordnungswidrigkeiten

PAuswG	Personalausweisgesetz
PHW	personengebundener Hinweis
RBStV	Rundfunkbeitragsstaatsvertrag
Rdnr./Rn.	Randnummer
RDG	Rechtsdienstleistungsgesetz
Rn.	Randnummer
Rs.	Rechtssache
S.	Seite *oder* Satz
s.	siehe
SaaS	Software as a Service
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
S/MIME	Secure / Multipurpose Internet Mail Extensions
sog.	sogenannte/sogenannter/sogenanntes
SPH	Schulportal Hessen
SQL	Structured Query Language (auf Deutsch: „Strukturierte Abfrage-Sprache“)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
stRspr.	ständige Rechtsprechung
StVG	Straßenverkehrsgesetz
TB	Tätigkeitsbericht
TDDDG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz)
TFG	Gesetz zur Regelung des Transfusionswesens
TLS	Transport Layer Security
TOM	technisch-organisatorische Maßnahmen
u. a.	unter anderem
UAbs.	Unterabsatz
Urt.	Urteil

USB	Universal Serial Bus
UWG	Gesetz gegen den unlauteren Wettbewerb
VE	Verdeckter Ermittler
VG	Verwaltungsgericht
VKS	Videokonferenzsystem
vgl.	vergleiche
VP	Verdeckt ermittelnde Person
WP	Working Paper
WWW	World Wide Web
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
Ziff.	Ziffer
ZPO	Zivilprozessordnung

Register der Rechtsvorschriften

Zitiert werden die jeweils zum Bearbeitungszeitpunkt geltenden Fassungen.

Gesetz/Vorschrift	Fundstelle(n)
ATDG	Antiterrordateigesetz vom 22.12.2006, zuletzt geändert durch Art. 2 Abs. 1 G v. 30.3.2021 I 402
ÄWeitBiG HE	Gesetz über das Berufsrecht und die Kammern der Heilberufe (Heilberufsgesetz) in der Fassung vom 7.2.2003 (GVBl. S. 79)
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2.1.2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Art. 14 des Gesetzes vom 23.10.2024 (BGBl. 2024 I Nr. 323)
BDSG	Bundesdatenschutzgesetz vom 30.6.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 10 G vom 23.6.2021 (BGBl. I S. 1858, 1968, ber. 2022 I S. 1045)
BDSG	Bundesdatenschutzgesetz vom 30.6.2017 (BGBl. I S. 2097), zuletzt geändert durch Art. 10 des Gesetzes vom 23.6.2021 (BGBl. I S. 1858)
BDSG	BDSG-neu (Gesetzentwurf der Bundesregierung, Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes, Stand: 31.1.2024)
BKAG	Bundeskriminalamtgesetz vom 1.6.2017 (BGBl. I S. 1354; 2019 I S. 400), zuletzt geändert durch Art. 5 des Gesetzes vom 30.7.2024 (BGBl. 2024 I Nr. 255)
BSIG	BSI-Gesetz vom 14.8.2009 (BGBl. I S. 2821), zuletzt geändert durch Art. 12 des Gesetzes vom 23.6.2021 (BGBl. I S. 1982)
DS-GVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 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 (DV-VerbundG) in der Fassung vom 4.4.2007; Stand: letzte berücksichtigte Änderung: zuletzt geändert durch Art. 2 des Gesetzes vom 11.12.2019 (GVBl. S. 416)
EGGVG	Einführungsgesetz zum Gerichtsverfassungsgesetz in der im Bundesgesetzblatt Teil III, Gliederungsnummer 300-1, veröffentlichten bereinigten Fassung, zuletzt geändert durch Art. 8 des Gesetzes vom 25.10.2024 (BGBl. 2024 I Nr. 332)
GG	Grundgesetz vom 23.5.1949, zuletzt geändert durch Art. 1 ÄndG (Art. 82) vom 19.12.2022 (BGBl. I S. 2478)
GewO	Gewerbeordnung in der Fassung der Bekanntmachung vom 22.2.1999 (BGBl. I S. 202), zuletzt geändert durch Art. 36 des Gesetzes vom 23.10.2024 (BGBl. 2024 I Nr. 323)

GRCh	Charta der Grundrechte der Europäischen Union ABl. C 326 vom 26.10.2012, S. 391
HBKG BW	Gesetz über das Berufsrecht und die Kammern der Heilberufe (Heilberufe-Kammergesetz – HBKG) in der Fassung vom 16.3.1995 (GBl. BW v. 17.5.1995 S. 314), zuletzt geändert durch das Gesetz zur Änderung des Heilberufe Kammergesetzes und weitere Gesetze vom 30.4.2024 (GBl. BW v. 6.5.2024, S. 1)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 03.5.2018 (GVBl. S. 82), in Kraft gesetzt am 25.5.2018, geändert durch Art. 9 des Gesetzes vom 15.11.2021 (GVBl. S. 718, 729)
HeilBG	Rheinland-Pfälzisches Heilberufsgesetz (HeilBG) vom 19.12.2014, zuletzt geändert durch Art. 1 des Gesetzes vom 30.4.2024 (GVBl. S. 73)
HGO	Hessische Gemeindeordnung in der Fassung der Bekanntmachung vom 7.3.2005, zuletzt geändert durch Art. 2 des Gesetzes vom 16.2.2023 (GVBl. S. 90, 93)
HKHG	Hessisches Krankenhausgesetz vom 21.12.2010, zuletzt geändert durch Art. 6 des Gesetzes vom 9.12.2022 (GVBl. S. 752, 757)
HKO	Hessische Landkreisordnung in der Fassung der Bekanntmachung vom 7.3.2005, zuletzt geändert durch Art. 2 des Gesetzes vom 11.12.2020 (GVBl. 2. 915)
HSchG	Hessisches Schulgesetz vom 17.12.2022, zuletzt geändert durch Gesetz vom 28.3.2023 (GVBl. S. 183, 216).
HSOG – alt	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung vom 14.1.2005 (GVBl. I S. 14) FFN 310-63, zuletzt geändert durch Art. 10 Hess. Ausländer-TeilhabeG Kommunalpolitik vom 7.5.2020 (GVBl. S. 318)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung vom 14.1.2005 (GVBl. I S. 14) FFN 310-63, zuletzt geändert durch Art. 1 G zur Stärkung der Inneren Sicherheit in Hessen vom 13.12.2024 (GVBl. Nr. 83)
HVSG	Hessisches Verfassungsschutzgesetz (HVSG) in der Fassung vom 20.7.2023 (GVBl. S. 614) FFN 18-7; Neubekanntmachung des HVSG vom 25.6.2018 (GVBl. S. 302) in der ab 12.7.2023 geltenden Fassung
HVwVfG	Hessisches Verwaltungsverfahrensgesetz (HVwVfG) in der Fassung vom 15.1.2010, zuletzt geändert durch Art. 3 des Gesetzes vom 16.2.2023 (GVBl. S. 78, 81)

KI-VO	Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)
KritisV	BSI-Kritisverordnung vom 22.4.2016 (BGBl. I S. 958), zuletzt geändert durch Art. 1 der Verordnung vom 29.11.2023 (BGBl. 2023 I Nr. 339)
KWG	Kreditwesengesetz in der Fassung der Bekanntmachung vom 9.9.1998 (BGBl. I S. 2776), zuletzt geändert durch Art. 12 des Gesetzes vom 22.2.2023 (BGBl. 2023 I Nr. 51)
MBO-Ä	(Muster-)Berufsordnung für die in Deutschland tätigen Ärztinnen und Ärzte in der Fassung des Beschlusses des 128. Deutschen Ärztetages vom 9.5.2024 in Mainz
MStV	Medienstaatsvertrag vom 14.–28.4.2020, zuletzt geändert durch den Vierten Medienänderungsstaatsvertrag vom 9.–16.5.2023
OWiG	Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19.2.1987 (BGBl. I S. 602), zuletzt geändert durch Art. 5 des Gesetzes vom 14.3.2023 (BGBl. I Nr. 73)
PAuswG	Personalausweisgesetz vom 18.6.2009 (BGBl. I S. 1346), zuletzt geändert durch Art. 8 des Gesetzes vom 23.10. 2024 (BGBl. 2024 I Nr. 323)
RBStV	Rundfunkbeitragsstaatsvertrag vom 15.–21.12.2010, zuletzt geändert durch den Medienstaatsvertrag vom 14.–28.4.2020, in Kraft getreten am 7.11.2020, Hess. GVBl. 2020 S. 607 ff.
RDG	Rechtsdienstleistungsgesetz
Satzung der Bundespsychotherapeutenkammer	Satzung der Bundespsychotherapeutenkammer verabschiedet auf dem 13. Deutschen Psychotherapeutentag in Leipzig am 15.11.2008
	Satzung des Hessischen Rundfunks über das Verfahren zur Leistung der Rundfunkbeiträge vom 23.12.2016
SächsHKaG	Sächsisches Heilberufekammergesetz vom 5.7.2023 (SächsGVBl. S. 559), zuletzt geändert durch Art. 3 Absatz 6 des Gesetzes vom 17.7.2024 (SächsGVBl. S. 662)
SchulGesPflV HE	Verordnung über die Zulassung und die Ausgestaltung von Untersuchungen und Maßnahmen der Schulgesundheitspflege vom 19.6.2015, zuletzt geändert durch Verordnung vom 14.10.2022 (GVBl. S. 562)
SGB X	Das Zehnte Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz (in der Fassung der Bekanntmachung vom 18.1.2001 (BGBl. I S. 130), zuletzt geändert durch Art. 8d des Gesetzes vom 19.7.2024 (BGBl. I Nr.245)

StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13.11.1998 (BGBl. I S. 3322), zuletzt geändert durch Art. 2 Abs. 2 des Gesetzes vom 7.11.2024 (BGBl. I S. 351)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 07.4.1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 2 des Gesetzes vom 26.7.2023 (BGBl. I Nr. 203)
StVG	Straßenverkehrsgesetz in der Fassung der Bekanntmachung vom 5.3.2003 (BGBl. I S. 310, 919), zuletzt geändert durch Art. 70 des Gesetzes vom 23.10.2024 (BGBl. 2024 I Nr. 323)
TDDDG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten, zuletzt geändert durch Art. 8 G vom 6.5.2024 (BGBl. 2024 I Nr. 149)
TFG	Gesetz zur Regelung des Transfusionswesens (Transfusionsgesetz) in der Fassung der Bekanntmachung vom 28. August 2007 (BGBl. I S. 2169), zuletzt geändert durch Art. 1a des Gesetzes vom 11.5.2023 (BGBl. 2023 I Nr. 123)
UWG	Gesetz gegen den unlauteren Wettbewerb vom 3.7.2004 (BGBl. I S. 1414), zuletzt geändert durch Gesetz vom 6.5.2024 (BGBl. 2024 I Nr. 149)
Verordnung (EU) 2006/114/EG	Richtlinie 2006/114EG des Europäischen Parlaments und des Rates vom 12.12.2006 über irreführende und vergleichende Werbung
Verordnung (EU) 2017/625	Verordnung (EU) 2017/625 des Europäischen Parlaments und des Rates vom 15.3.2017 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 (Verordnung über amtliche Kontrollen)
ZPO	Zivilprozessordnung in der Fassung der Bekanntmachung vom 5.12.2005 (BGBl. I S. 3202; 2006 I S. 431; 2007 I S. 1781), zuletzt geändert durch Art. 1 des Gesetzes vom 24.10.2024 (BGBl. 2024 I Nr. 328)

Stichwortverzeichnis

E

F

G

Z