21. Wahlperiode

Drucksache **21/3261**

HESSISCHER LANDTAG

14. 04. 2026

Vierundfünfzigster Tätigkeitsbericht zum Datenschutz und Achter Tätigkeitsbericht zur Informationsfreiheit

Hessischer Beauftragter für Datenschutz und Informationsfreiheit

vorgelegt zum 31. Dezember 2025
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 14. April 2026 · Ausgegeben am 14. April 2026
Gestaltung: Satzbüro Peters, Taunusstein · Herstellung: AC medienhaus, Wiesbaden · Landtagsinformationssystem: www.Hessischer-Landtag.de

Vierundfünfzigster Tätigkeitsbericht zum Datenschutz
und
Achter Tätigkeitsbericht zur Informationsfreiheit

des

Hessischen Beauftragten für Datenschutz
und Informationsfreiheit

Professor Dr. Alexander Roßnagel

vorgelegt zum 31. Dezember 2025
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
Wilhelmstraße 7, 65185 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 21/3261

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

Inhaltsverzeichnis

Anhang zu Teil I

Kernpunkte

1. Die Datenschutzaufsicht in Hessen war im Jahr 2025 von einer sehr hohen Zunahme von Eingaben, insbesondere Beschwerden geprägt. Diese sind in diesem Jahr insgesamt von 3.839 auf 6.070, also um 58 % angestiegen. In bestimmten Bereichen nahmen die Fallzahlen noch stärker zu: Die Beschwerden stiegen in den Sachgebieten Auskunfteien von 503 auf 1613 (um 221 %), Videobeobachtung von 295 auf 539 (um 83 %) und Beschäftigtendatenschutz von 287 auf 525 (um 83 %) (Teil 1 Kap. 18). Die gestiegenen Fallzahlen zeigen, dass der Datenschutz in einer zunehmend digitalisierten Welt in der Wahrnehmung von Bürgerinnen und Bürgern immer mehr an Bedeutung gewinnt: Betroffene legen mehr Wert auf ihre Persönlichkeitsrechte und fordern die Unterstützung und den Schutz durch die Datenschutzaufsicht. Zugleich suchen öffentliche und nicht-öffentliche Stellen nach Rechtssicherheit und wenden sich mit Beratungsanfragen an mich.
2. Wir befassen uns mit allen Beschwerden. Soweit wir Verstöße feststellen, sorgen wir für Abhilfe. Die meisten Verantwortlichen beseitigen nach einem Hinweis auf datenschutzwidrige Zustände diese umgehend. Eine formelle Maßnahme ist dann entbehrlich. Soweit dies nicht der Fall ist, helfen förmliche Anordnungen, Durchsetzungsmaßnahmen und Sanktionen. Die Zahl der Anordnungen stieg von 115 im Vorjahr auf 124 im Berichtsjahr, davon – wie im Vorjahr– 47 Geldbußen. Die Gerichtsverfahren nahmen von 37 im Jahr 2024 auf 50 im Jahr 2025 zu (Teil I Kap. 3). Grundsätzlich ist festzuhalten: Datenschutz wird in Hessen akzeptiert und nicht in Frage gestellt. Schwerwiegende Verstöße waren im Berichtszeitraum nicht festzustellen.
3. Die zunehmende Inanspruchnahme der Datenschutzaufsicht ist nicht nur ein Indikator für die Bedeutung, die Bürgerinnen und Bürger ihren Persönlichkeitsrechten zumessen. Sie führt auch zu einer steigenden Überlastung. Nicht nur ist die Zahl der schriftlichen Eingaben (Beschwerden, Beratungen und Hinweise) im Jahr 2025 um 48 % auf 8.488 angestiegen, nachdem diese bereits im Vorjahr um 10 % zugenommen hatte. Auch die Zahl der gemeldeten Datenpannen, die hinzuzurechnen ist, stieg um 28 % auf 2.730. Zudem werden durch die zunehmende Digitalisierung aller Lebensbereiche die Aufklärungen, Beratungen und Hilfestellungen qualitativ anspruchsvoller. Dadurch stieg die Arbeitsbelastung noch stärker als die Zahl der Vorgänge. Dennoch ist die Zahl der Mitarbeitenden in der Aufsichtsbehörde in den letzten Jahren gleich geblieben. Vor diesem Hintergrund haben wir vielfältige Maßnahmen zur Steigerung der Effizienz in der Fallbearbeitung eingeleitet oder bereits umgesetzt. Trotzdem wird

es immer schwieriger, den gesetzlichen Aufgaben und Anforderungen der Datenschutz-Grundverordnung (DS-GVO) – etwa hinsichtlich einer angemessenen Frist zur Bearbeitung von Beschwerden – sowie den berechtigten Erwartungen von Bürgerinnen und Bürgern gerecht zu werden. Für die künftige Bearbeitung der Beschwerden, Hinweise, Beratungen und Datenpannenmeldungen werden Priorisierungen bei der Vorgangsbearbeitung nach dem jeweiligen konkreten Schutzbedarf der betroffenen Grundrechte und längere Bearbeitungszeiten unvermeidbar sein.

4. Datenverarbeitung in hessischen Unternehmen und Behörden ist stark abhängig von den IT-Systemen und -Dienstleistungen internationaler Digitalkonzerne – hauptsächlich aus den USA und China. Dies wird sich durch die zunehmende Nutzung von Systemen Künstlicher Intelligenz noch verstärken. Diese Abhängigkeit hat aus Sicht des Datenschutzes zwei Nachteile: Zum einen entsprechen diese Systeme und Dienstleistungen meist nicht den Anforderungen der DS-GVO. Dies hat die 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.
5. Soweit und solange diese Abhängigkeit besteht, kommt es darauf an, eine Anpassung von Angeboten und Vertragsregelungen an die europäischen Datenschutzanforderungen zu erreichen. Daher ist es ein wichtiger Schritt zu mehr Rechtssicherheit, dass es mir in intensiven und schwierigen Gesprächen mit Microsoft gelungen ist, Wege zu finden, wie die Nutzer von Microsoft 365 in Hessen ihre Datenverarbeitung datenschutzgerecht durchführen können. Hierfür hat Microsoft sein Data Protection Addendum und seine Datenverarbeitung verändert und den Nutzern zusätzliche Informationen und Handlungsmöglichkeiten zur Verfügung gestellt. Dies ermöglicht den Nutzern, ihren notwendigen Beitrag zur datenschutzgerechten Nutzung zu leisten (Teil 1 Kap. 1.5 und 16.2).
6. 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 und wie die Erfüllung dieser Vorgaben praktisch möglich ist. Im Berichtsjahr hat der Europäische Datenschutzausschuss (EDSA) mit vielen Leitlinien, Empfehlungen und Stellungnahmen zu einer weiteren Konsolidierung

des Datenschutzrechts und zu einem unionsweit einheitlichen Vollzug beigetragen. Um auf diese Entwicklung Einfluss zu nehmen, bringen sich Mitarbeitende meiner Behörde – vor allem durch engagierte Mitarbeit in Arbeitskreisen des EDSA – in die europäischen Diskussionen ein. Die Anzahl der europaweiten Verfahren, an denen ich beteiligt war, ist von 848 im Jahr 2024 auf 1.589 im Jahr 2025 gestiegen. (Teil I Kap. 2.1).

7. Die Meldungen von Datenschutzverstößen gemäß Art. 33 DS-GVO nahmen im Berichtszeitraum um 28 % zu: von 2.141 im Jahr 2024 auf 2.730 im Jahr 2025. 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 um 30 % von 482 im Jahr 2024 auf 625 im Jahr 2025 zu und werden qualitativ immer raffinierter und professioneller. Sie richten sich zunehmend gegen Auftragsverarbeiter, die für viele Unternehmen und Behörden arbeiten, und verstärken damit das Schadenspotenzial (Teil 1 Kap. 16.8).
8. Nach der neuen Rechtsprechung des EuGH unterfällt die gesamte Datenverarbeitung des Hessischen Landtages, seiner Fraktionen, seiner Ausschüsse und seiner Abgeordneten der DS-GVO und ich übe die Datenschutzaufsicht über diese öffentlichen Stellen aus. Daher habe ich Handlungsempfehlungen für sie erarbeitet, die ihnen für typische Situationen zeigen sollen, wie Datenschutz im Hessischen Landtag umgesetzt werden kann (Teil I Kap. 5.1). Die Ergänzungen des Abgeordneten- und des Fraktionsgesetzes, um den Landtag gegen Mitarbeitende zu schützen, die parlamentarische Schutzgüter gefährden, sind mit Datenschutzrecht vereinbar (Teil I Kap. 5.2).
9. Polizei, Verfassungsschutz und Staatsanwaltschaften haben weitreichende Befugnisse zur Verarbeitung personenbezogener Daten, die zu tiefen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen führen können. Diese Befugnisse sind jedoch immer an einschränkende gesetzliche Voraussetzungen gebunden. Datenschutzprüfungen bei der Polizei, dem Landesamt für Verfassungsschutz und einer Staatsanwaltschaft stellten fest, dass die datenschutzrechtlichen Vorgaben weitgehend eingehalten wurden. Ihre gesetzliche Festlegung war Gegenstand meiner kritischen Stellungnahme im Gesetzgebungsverfahren zur Änderung des Hessischen Verfassungsschutzgesetzes (Teil I Kap. 4).
10. In den Verwaltungsbehörden des Landes sowie der Landkreise, Städte und Gemeinden werden überwiegend personenbezogene Daten verarbeitet. Sowohl die Datenverarbeitung als auch der datenschutzrechtli-

che Rahmen werden weiterentwickelt. Die Verwaltung setzt auch neue Techniken ein, wie etwa Luftbilder durch Drohnen für die Ermittlung von Abwassergebühren. Daneben ergaben sich immer wieder grundlegende Fragen zum Datenschutz in der Verwaltung (Teil I Kap. 6).

11. Das Hessische Landesarchiv bewahrt Dokumente auf, die für das Verständnis der gesellschaftlichen und politischen Entwicklung Hessens von Bedeutung sein können. Für das dadurch entstehende Spannungsverhältnis zum Datenschutz wurde mit dem Landesarchiv eine Lösung gefunden (Teil I Kap. 7.1). Zur Unterstützung langfristig kranker Kinder werden in manchen hessischen Schulen Avatare eingesetzt, die diese Kinder im Klassenzimmer vertreten sollen. Unter bestimmten Voraussetzungen ist dies mit dem Datenschutzrecht vereinbar (Teil I Kap. 7.2).
12. Im Bereich des Beschäftigtendatenschutzes erhalte ich viele Beschwerden, die es oft erfordern, korrigierend einzugreifen. Dies gilt insbesondere für Fälle, in denen das Verhalten und die Leistung von Beschäftigten überwacht werden. Zu berücksichtigen ist aber auch, dass Arbeitgeber ihre berechtigten und überwiegenden Interessen wahrnehmen können, etwa um Daten über Straftaten eines Beschäftigten zu verarbeiten (Teil I Kap. 8).
13. Die Rechtsentwicklungen in der EU und in anderen Bundesländern zeigen an, dass ein spezifischer Rechtsrahmen erforderlich ist, um Hindernisse und Rechtsunsicherheiten für den Einsatz Künstlicher Intelligenz (KI) in der öffentlichen Verwaltung zu beseitigen. Für diese zeigt sich, dass die Anwendung von Retrieval Augmented Generation (RAG) bei der Nutzung von intelligenten Sprachmodellen besondere Vorteile für lokale Problemlösungen, digitale Souveränität und Datenschutz ermöglicht. Ich biete für die Verwaltung in Hessen vielfach Fortbildungen für den datenschutzgerechten KI-Einsatz in der öffentlichen Verwaltung an (Teil I Kap. 9).
14. Viele Privatpersonen nutzen Onlinedienste, um Daten, Bilder und Filme einer großen Anzahl von Empfängern zugänglich zu machen. Sie überschreiten damit die Grenze der rein privaten Datenverarbeitung und unterfallen dadurch der DS-GVO, ohne sich dessen bewusst zu sein. Sie sind auch meist nicht in der Lage, die datenschutzrechtlichen Anforderungen für diese Form der Datenverarbeitung zu erfüllen (Teil I Kap. 10).
15. Im Bereich Werbung und Adresshandel musste ich mehrfach intervenieren, weil Unternehmen personenbezogene Daten, die sie für andere Zwecke erhalten haben, unzulässigerweise für Werbezwecke verwendet haben. Vielfach wurden auch Werbewidersprüche ignoriert, weil die Unternehmen für die automatisierte Bearbeitung ungeeignete technisch-organisatorische Maßnahmen eingesetzt haben. Daten, die sie rechtmäßig erhalten

haben, dürfen sie für Werbezwecke nicht zeitlich unbegrenzt einsetzen (Teil I Kap. 11).

16. Im Bereich der Wirtschaft waren die neuen Verhaltensregeln für die Prüf- und Speicherfristen von rechtmäßig gespeicherten personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien Gegenstand mehrerer gerichtlicher Verfahren. Eine Entscheidung des Bundesgerichtshofs hat schließlich festgestellt, dass diese Verhaltensregeln im Regelfall einen angemessenen Interessenausgleich enthalten. Erfolgen Datenverstöße im Rahmen des internationalen Wirtschaftsverkehrs, stoßen meine Möglichkeiten, den betroffenen Personen zu helfen, auf rechtliche und praktische Schwierigkeiten (Teil I Kap. 13).
17. Im Gesundheitsbereich konnte ich den Aufbau einer Treuhandstelle beratend unterstützen, die die mehrfache Nutzung von Gesundheitsdaten durch verschiedene Stellen in der Gesundheitsversorgung und der Gesundheitsforschung datenschutzgerecht ermöglicht. Auch beriet ich Ärzte, die aus einer Gemeinschaftspraxis ausscheiden wollten, wie sie dabei verfahren müssen, um die Patientenakten ausreichend zu schützen. Im Berichtszeitraum war es wieder vielfach notwendig, zum Schutz von Patientendaten in Kliniken, Arztpraxen und Apotheken zu intervenieren. Um das Patientengeheimnis zu wahren und die notwendige Vertraulichkeit sicherzustellen, sind im Anmeldebereich von Arztpraxen und Notaufnahmen geeignete bauliche und organisatorische Maßnahmen notwendig (Teil I Kap. 14).
18. Mir ist es wichtig, die datenschutzkonforme wissenschaftliche Forschung durch konstruktive Hilfen zu unterstützen. Hierzu zählen die von mir initiierten Anwendungshinweise der DSK zum Drittstaatentransfer in der medizinischen Forschung, Erleichterungen für die gemeinsame Verarbeitung von Gesundheitsdaten durch Forschungseinrichtungen und der datenschutzgerechte Zugang zu Daten sehr großer Online-Plattformen und Suchmaschinen. Zusammen mit der Deutschen Gesellschaft für Innere Medizin (DGMI) habe ich einen Leitfaden für Datenschutz in der medizinischen Forschung erarbeitet, der für medizinische Forschungsprojekte mehr Rechtssicherheit gewährleisten kann (Teil I Kap. 15).
19. Zur Auswahl, zur Gestaltung und zum Einsatz von Software und IT-Diensten bei Unternehmen und Behörden, zu angemessenen technischen und organisatorischen Schutzmaßnahmen, zur Nutzung von Microsoft 365 und zur Einführung der Bezahlkarte für Asylsuchende hat meine Behörde viele Beratungen durchgeführt. Zur Analyse von Datenveröffentlichungen im Darknet und für Webseiten-Checks für Vereine hat sie jeweils ein technisches Werkzeug entwickelt. Datenschutzverletzungen größeren Ausmaßes wie z. B. Ransomware-Angriffe auf Pflegeeinrichtungen, Da-

tenpreisgaben bei einem Luftfahrtkonzern und Datenschutzvorfälle durch Phishing erforderten besondere Prüfungen (Teil I Kap. 16).

20. Obwohl die Informationsfreiheit in Hessen immer noch nur in der Landesverwaltung und in 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. Die Informationsfreiheit muss sich dynamisch an die rasanten Entwicklungen in Technik, Wirtschaft, Verwaltung und Gesellschaft anpassen. Die Digitalisierung der Verwaltung vermehrt zum einen die verfügbaren Informationen. Sie erzeugt damit Mehrwerte für die Nutzung dieser Informationen, die der Gesellschaft, insbesondere für die Forschung und weitere Allgemeininteressen, zur Verfügung gestellt werden müssen. Zum anderen erleichtert sie die Erfüllung von Informationsbegehren, insbesondere wenn sie Prinzipien der „Informationsfreiheit by Design“ beachtet. Für beides wird Künstliche Intelligenz grundlegende Veränderungen bringen. Im Berichtszeitraum entstanden neue gesetzliche Möglichkeiten für Gemeindevertretungen, Stadtverordnetenversammlungen und Kreistage, die Protokolle der Kommunalparlamente im Internet öffentlich zugänglich zu machen. Außerdem waren u. a. die Fragen zu beantworten, welche Auswirkungen es hat, wenn in amtlichen Informationen Geschäftsgeheimnisse enthalten sind, und ob Forschende im Rahmen eines Forschungsprojekts an einer öffentlichen Hochschule als natürliche Personen anzusehen sind, die sich auf die Informationsfreiheit berufen können (Teil II).

Vorwort

Dies ist der 54. Tätigkeitsbericht zum Datenschutz und der 8. 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 und über die Maßnahmen der Aufsichtsbehörde zu berichten, auf diese zugunsten der Grundrechte und der Demokratie Einfluss zu nehmen.

Der 54. Tätigkeitsbericht zum Datenschutz, der die Entwicklungen im Jahr 2025 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 2025 an vielen Stellen und in vielen Verfahren Datenschutz durchzusetzen.

Für die Wahrnehmung der Grundrechte und die Teilnahme an der demokratischen Willensbildung ist in einer digitalen Gesellschaft neben dem Datenschutz der Zugang zu öffentlichen Informationen von besonderer Bedeutung. Diese Informationsfreiheit ist in Hessen erst seit 2018 im Gesetz vorgesehen. Ihre praktische Inanspruchnahme und Erfüllung müssen sich in Hessen noch weiterentwickeln. 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 28. Februar 2026

Prof. Dr. Alexander Roßnagel

I
Erster Teil
54. Tätigkeitsbericht zum Datenschutz

1. Neue Aufgaben und Rahmenbedingungen

Für die Datenschutzpraxis wichtige Klarstellungen hat ein Urteil des Europäischen Gerichtshofs (EuGH) gebracht, das festgestellt hat, wann Daten anonym sind und nicht mehr der DS-GVO unterfallen (Kap. 1.1). Rechtspolitisch war die Datenschutzdiskussion im Berichtsjahr stark geprägt durch die Forderungen nach Entbürokratisierung (Kap. 1.2). Zu dieser können die Möglichkeiten, Rechtssicherheit durch Verhaltensregeln einzelner Branchen (Kap. 1.3) und die Harmonisierung der Datenschutzpraxis durch Zusammenarbeit der Aufsichtsbehörden der Länder (1.4) zu erreichen, beitragen. Rechtssicherheit im Datenschutz kann auch durch Verhandlungen mit großen Datenverarbeitern wie Microsoft erreicht werden (Kap. 1.5). Diese Erfahrungen sollten für die Diskussionen um die Bündelung von Kompetenzen der Datenschutzaufsichtsbehörden (Kap. 1.6) und um die Verteilung von Aufsichtskompetenzen nach der Verordnung für Künstliche Intelligenz (KI-VO) und nach der Datenverordnung (Data Act – DA) (Kap. 1.7) berücksichtigt werden.

1.1 Rechtsprechung des Europäischen Gerichtshofs

Am 4. September 2025 hat der Europäische Gerichtshof (EuGH) eine für die Praxis des Datenschutzes in Europa sehr wichtige Entscheidung getroffen. Sie klärt eine bis dahin umstrittene Frage zum Verständnis von Anonymität. Sie ist deswegen bedeutsam, weil anonyme Daten nicht in den Anwendungsbereich der DS-GVO fallen. Die Feststellungen des EuGH erleichtern künftig die Annahme von Anonymität und die Verarbeitung von anonymen Daten erheblich.

Der Entscheidung (EuGH, Urteil vom 4. September 2025, C-413/23 – ECLI:EU:C:2025:654 – EDSB/SRB) lag ein Streit zwischen dem Europäischen Datenschutzbeauftragten (EDSB), der durch den Europäischen Datenschutzausschuss (EDSA) unterstützt wurde, und dem Einheitlichen Abwicklungsausschuss der Europäischen Union (SRB), den die Europäische Kommission unterstützte, zugrunde. Der SRB hatte Gläubiger der Banco Popular Espanol SA in dem Verfahren zur Abwicklung dieser Bank aufgefordert, ihre Forderungen zu melden und nachzuweisen. Der SRB pseudonymisierte die eingehenden Meldungen mit einer zufälligen 33-stelligen eindeutigen Identifikationsnummer und sandte die Nachweise an die Wirtschaftsprüfungsgesellschaft Deloitte, um sie von dieser bewerten zu lassen. Deloitte konnte die Nachweise nicht einzelnen Gläubigern zuordnen. Der SRB unterließ es, die Gläubiger über diese Übermittlung ihrer Unterlagen an Deloitte zu

informieren, weil er der Meinung war, die übermittelten Daten seien anonym. Dagegen hielt der EDSB diese Daten nicht für anonym und verwarnte den SRB wegen unterlassener Information. Dagegen klagte der SRB vor dem Europäischen Gericht, das ihm recht gab und die Verwarnung des EDSB für nichtig erklärte. Dagegen legte der EDSB beim EuGH Rechtsmittel ein.

Der EuGH wies die Ansicht zurück, pseudonymisierte Daten seien immer personenbezogen, weil der Inhaber der Zuordnungsinformation die pseudonymen Daten zuordnen könnte. Im Gegensatz dazu stellte er fest, dass die Pseudonymisierung gerade darauf abziele, dass andere Verantwortliche die Daten nicht der betroffenen Person zuordnen können. Für diese anderen Verantwortlichen – wie z. B. Delloite – sind die pseudonymen Daten anonym (Rn. 75, 76, 86). Daher bedeutet „die Existenz von zusätzlichen, die Identifizierung der betroffenen Person ermöglichenden Information für sich genommen nicht (…), dass pseudonymisierte Daten (…) in jedem Fall und für jede Person als personenbezogene Daten zu betrachten sind“ (Rn. 82). Entscheidend ist allein, ob der jeweils Verantwortliche mit den ihm zur Verfügung stehenden Mitteln die Daten einer bestimmten Person zuordnen kann.

Der EuGH geht damit nicht auf den dogmatischen Streit zwischen relativem und absolutem Verständnis des Begriffs der Anonymität ein, sondern entwickelt konsequent sein eigenes Verständnis von Personenbezug und Anonymität, indem er die vier Präjudizien des EuGH zu diesen Fragestellungen einbezieht (Rn. 81-84). Entscheidend sind die Umstände des konkreten Falls und die konkreten Mittel des jeweils Verantwortlichen, nicht eine bestimmte Theorie (s. Roßnagel, Datenschutz und Datensicherheit (DuD) 2024, 513, 515 f.).

Der EUGH wies auch die Ansicht zurück, durch die Übermittlung pseudonymisierter Daten an einen Verantwortlichen würden diese Daten zu Unrecht dem Schutzbereich der DS-GVO entzogen. Wenn nämlich die Daten an andere Verantwortliche weitergegeben werden, die durch ihr Wissen und ihre Mittel die Daten einer betroffenen Person zuordnen können, unterfallen die Daten (wieder) dem Anwendungsbereich der DS-GVO (Rn. 85).

Hinsichtlich der fehlenden Information der betroffenen Personen über die Empfänger der erhobenen Daten, die zum Zeitpunkt der Erhebung zu erfolgen hat, ist auf den erhebenden Verantwortlichen abzustellen. Für den SRB waren die Daten personenbezogen. Er hätte also über potenzielle Empfänger informieren müssen, auch wenn für diese die später übermittelten Daten anonym sind. Nur dadurch erhält die betroffene Person einen vollständigen Überblick, was mit ihren Daten geschieht, und kann informiert darüber entscheiden, ob sie ihre Daten preisgibt oder ob sie Rechte gegenüber dem Empfänger geltend macht.

Das Urteil des EuGH kommt somit zu folgenden wesentlichen Erkenntnissen, dass

– Anonymität oder Personenbeziehbarkeit allein aus der Sicht des jeweils Verantwortlichen bestimmt werden muss. Die gleichen Daten können daher für unterschiedliche Verantwortliche anonym oder personenbeziehbar sein.
– die Daten ihren Charakter als anonym oder personenbezogen wechseln können, wenn sie einem anderen Verantwortlichen übermittelt werden.
– auch pseudonyme Daten dann anonym sein können, wenn der Verantwortliche die pseudonymen Daten nicht einer bestimmten Person zuordnen kann.
– anonyme Daten (wieder) personenbeziehbar werden können und dann die DS-GVO auf ihre Verarbeitung anwendbar ist.
– Verantwortliche, die einen Personenbezug herstellen können, müssen die betroffenen Personen nach Art. 13 Abs. 1 Buchst. e DS-GVO über eine Datenübermittlung informieren, auch wenn die Daten für den Empfänger anonym sind.

Mit diesem Urteil bekräftigt der EuGH seine bisherige Rechtsprechung zur Anonymität von Daten (s. hierzu 53. Tätigkeitsbericht zum Datenschutz, Kap. 1.4). Es widerlegt eindeutig das bisher vielfach vertretene absolute Verständnis von Anonymität, nach dem die Möglichkeit von irgendjemandem, Daten einer Person zuzuordnen, Anonymität ausschließt. Dadurch wurde der Begriff der Anonymität sehr eingeengt und auf sehr seltene Fälle beschränkt. Indem der EuGH allein auf den Verantwortlichen abstellt und dessen Möglichkeiten, die Daten – auch mit Hilfe Dritter – einer betroffenen Person zuzuordnen, wird die Anwendbarkeit der DS-GVO auf die praktisch relevanten Fälle beschränkt und Datenverarbeitung – insbesondere für die Entwicklung von Künstlicher Intelligenz oder die Durchführung von Forschungsprojekten – erheblich erleichtert.

1.2
Bürokratieabbau im Datenschutz

Der Abbau von Bürokratie ist eine politische Zielsetzung, die sehr breit geteilt wird. Diese Zielsetzung gilt auch für den Datenschutz, auch wenn bürokratische Belastungen durch Datenschutz nicht als das größte Problem angesehen werden. Bürokratie ist jedoch nicht grundsätzlich schlecht. Nach Max Weber (Wirtschaft und Gesellschaft. Grundriss der verstehenden Soziologie, 1921/1922, 5. Aufl. 1972, 125 ff., 551 ff., 565 ff.) ist Bürokratie eine Art der Verwaltung, die durch Trennung von Amt und Person, Neutralität, Regelgebundenheit, Schriftlichkeit und Fachkunde gekennzeichnet ist. Insofern

ist Bürokratie eine wichtige Grundlage für Demokratie, Grundrechtsschutz und Rechtsstaat. Datenschutzrechtliche Vorgaben sind nicht aus Schikane entstanden, sondern zum Schutz von Grundrechten und öffentlichen Interessen. Schutz der Persönlichkeit, Bildung von Vertrauen, Gewährleistung von demokratischer Willensbildung sind Werte, die auch im Rahmen der Digitalisierung der Gesellschaft gelten sollen. Sie zu verwirklichen, ist auch das Ziel der DS-GVO. Soweit Regelungen diesem Ziel dienen, müssen sie auch regelhaft, effektiv und effizient umgesetzt werden.

Notwendig ist also, gute und schlechte, notwendige und unnötige Bürokratie zu unterscheiden. Um herauszufinden, wo die Ursachen für kritikwürdige Bürokratie liegen und wo die Ansatzpunkte für Maßnahmen zum Abbau von Bürokratie möglich und erforderlich sind, habe ich am 5. Mai 2025 zusammen mit der Landtagspräsidentin Astrid Wallmann eine wissenschaftliche Tagung zum Thema „Bürokratieabbau im Datenschutz“ durchgeführt und die Vorträge und Diskussionen veröffentlicht (Roßnagel/Wallmann (Hrsg.), Bürokratieabbau im Datenschutz, 2025).

Der Abbau bürokratischer Anforderungen soll vor allem den Verantwortlichen als Regelungsadressaten, also den Unternehmen und öffentlichen Stellen, die personenbezogene Daten verarbeiten, gelten. Für die Verantwortlichen sind vor allem zwei Gründe relevant, um auf einen Abbau von Bürokratie zu dringen.

Ineffektive und ineffiziente Belastungen

Zum einen können bürokratische Vorgaben schädlich sein, die von dem Ziel der Regulierung nicht gefordert werden oder unverhältnismäßig sind. Sie sind dann bezogen auf das Ziel auch nicht effektiv oder nicht effizient oder verfehlen beides. Dies kann der Fall sein, wenn Schutzmaßnahmen gefordert werden, wo kein Risiko besteht oder wenn für Amateurvereine oder Handwerker die gleichen Dokumentations- oder Schutzpflichten bestehen wie für Weltkonzerne. Ansatzpunkte für Bürokratieabbau bestehen darin, die Kosten der Rechtsbefolgung ins rechte Verhältnis zu den Risiken zu setzen, die es zu vermeiden gilt.

Bürokratische Vorgaben sind ebenfalls schädlich, wenn sie die Kosten für die Zielerreichung den Falschen anlasten. Sie sollten denen angelastet werden, die Probleme oder Risiken verursachen, die Gestaltungsmacht haben, sie zu vermeiden, und bei denen dies die geringsten Kosten hervorruft. Die Aufgabe der datenschutzgerechten Systemgestaltung nach Art. 25 Abs. 1 DS-GVO können der Hersteller von IT-Systemen oder der Anbieter von Systemdiensten meist erheblich einfacher und kostengünstiger erfüllen als die von der Vorschrift verpflichteten Millionen Verantwortlichen. Auch kennt der Hersteller

oder Anbieter die Verarbeitungsvorgänge in seinem System besser als der verantwortliche Nutzer und könnte durch Muster für Verarbeitungsverzeichnisse Millionen Nutzer entlasten (s. hierzu auch den gemeinsamen Beschluss des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder zur Staatsmodernisierung vom 4. Dezember 2025, Rn. 166 Nr. 4).

Belastung durch Rechtsunsicherheit

Zum anderen können bürokratische Vorgaben schädlich sein, die Rechtsunsicherheit erzeugen. Dies ist der Fall, wenn Vorgaben zu abstrakt, zu allgemein oder zu kompliziert sind, um klare Handlungsanweisungen zu geben. Diese Rechtsunsicherheit wird vor allem durch technikneutrale Regelungen der DS-GVO verursacht, die für alle Technikausprägungen gleichermaßen gelten – von Adresslisten, E-Mail, Bürosoftware, Gerätesteuerung über Datenbanken, Videokonferenzsystemen, Plattformen, Social Media, Big Data-Anwendungen bis hin zu Systemen der Künstlichen Intelligenz – und in allen Wirtschafts-, Verwaltungs- und Gesellschaftsbereichen gleichermaßen Anwendung finden.

Rechtsunsicherheiten hemmen die Handlungsbereitschaft und Handlungsfähigkeit, weil unsicher ist, ob und wann man Grenzen des Zulässigen überschreitet und dadurch Nachteile erleidet. Sie führen leicht zu Übersteigerungen der eigenen Anforderungen, um auf der „sicheren Seite“ zu sein. Wer keine Verantwortung übernehmen möchte, rät zu oder entscheidet sich für die „obere Kante“ des Entscheidungsspielraums. Klare und überzeugende Anforderungen stärken dagegen Investitionsbereitschaft, Wettbewerb und wirtschaftliche Entwicklung.

Wirksame Entlastungen

Bei der Beseitigung schlechter Bürokratie muss es vor allem darum gehen, Verantwortliche zu entlasten. Für sie soll der Bürokratieabbau Freiräume für Entfaltung bringen, ohne neue bürokratische Hürden aufzurichten oder bürokratische Belastungen zu verschieben. Umgekehrt heißt das, dass rechtliche Regelungen, die unvermeidliche oder sinnvolle bürokratische Vorgaben enthalten, risikoorientiert, verhältnismäßig und rechtssicher sein müssen.

Wenn es gute und schlechte Bürokratie gibt, dann müssen Maßnahmen zur Entlastung von Bürokratie hinsichtlich ihrer vorhersehbaren positiven und negativen Auswirkungen auf Rechtssicherheit und Risikogerechtigkeit mit ihren Nebenwirkungen auf andere Interessen gegeneinander abgewogen werden. Zu vermeiden sind Scheinentlastungen, Belastungsverschiebungen und Aufbau neuer Bürokratien.

Eine scheinbare Entlastung entsteht, wenn eine Verpflichtung wegfällt, dadurch aber die Effektivität und Rechtssicherheit des Handelns ebenfalls gemindert werden. Dies ist etwa der Fall, wenn Unternehmen auf den betrieblichen Datenschutzbeauftragten verzichten können. Wenn aber die materiellen Vorgaben für Verantwortliche und die Rechte der Betroffenen ebenso wie die Nachweispflicht ihrer Erfüllung und Notwendigkeit ihrer Dokumentation bestehen bleiben, erhöht sich durch den Wegfall des Datenschutzbeauftragten die Belastung durch Rechtsunsicherheit und ineffektive Bearbeitung der Aufgaben. Denn dann fehlt ausgerechnet der interne Ansprechpartner, der die Pflichten kennen und bei der Erfüllung beistehen könnte.

Eine Verschiebung von Belastungen erfolgt, wenn eine Entlastung bei einem Akteur eine Belastung bei einem anderen Akteur bewirkt. Dies wäre etwa der Fall, wenn die Zuständigkeit für die nicht-öffentlichen Verantwortlichen von den Landesaufsichtsbehörden zur Bundesdatenschutzbeauftragten verschoben würden. Dadurch hätten die großen Unternehmen, die länderübergreifend tätig sind – d. h. 0,7 % aller Unternehmen in Deutschland –, den Vorteil, sich nur noch mit einer Aufsichtsbehörde auseinandersetzen zu müssen. Zugleich müssten aber 99,3 % der Unternehmen, also kleine und mittlere Unternehmen, sowie Bürgerinnen und Bürger auf die Nähe zu ihrer Aufsichtsbehörde und deren lokale Expertise verzichten (s. Kap. 1.5).

Aufbau neuer Bürokratie oder Verdopplungen von Zuständigkeiten führen ebenfalls nicht zu einer positiven Bilanz der Entbürokratisierung. So können Veränderungen in der Aufsichtsstruktur, die zum Aufbau Hunderter neuer Beamtenstellen führen, nicht als Bürokratieabbau gesehen werden (s. Kap. 1.6). Ebenso wird Bürokratie vermehrt, wenn für den gleichen Lebenssachverhalt – wie bei der Aufsicht über den Einsatz von KI oder der Aufsicht über Datenverarbeitungen nach dem Data Act – die Aufsichtsstrukturen verdoppelt werden (s. Kap. 1.7).

Berücksichtigung von Praxiserfahrung

Der Abbau von Bürokratie, die sich als unnötig oder gar schädlich erweist, ist notwendig. Bei der Bewertung gesetzlicher Vorgaben oder Verwaltungspraktiken, die bürokratischen Aufwand erfordern, ist vorsichtig vorzugehen und es sind die politischen Kosten des vermeintlichen Bürokratieabbaus zu beachten. Die Datenschutzaufsichtsbehörden bieten den Gesetzgebern an, sie mit ihrer Praxiserfahrung zu beraten. Sie werden im Rahmen ihrer Entscheidungsspielräume im Vollzug des Datenschutzrechts selbst nach Möglichkeiten der Entlastung suchen. Hinsichtlich der notwendigen Rechtssicherheit haben sie in den letzten Jahren durch zahlreiche Maßnahmen

erreicht, ihre Rechtsauffassung und Datenschutzpraxis zu vereinheitlichen, und hoffen auf weitere Unterstützung durch die Politik.

1.3
Bedeutung von Verhaltensregeln

Eine hervorragende Möglichkeit zum Abbau bürokratischer Belastungen bieten Verhaltensregeln der Regelungsadressaten. Branchenverbände können durch Verhaltensregeln abstrakte Datenschutzvorgaben bereichsspezifisch konkretisieren und dadurch für ihre Datenschutzpraxis mehr Rechtssicherheit erzeugen. Hierzu müssen aber vor allem Aufsichtsbehörden und Gerichte die Erstellung und Anwendung von genehmigten Verhaltensregeln unterstützen.

Die DS-GVO regelt für das gesamte Gebiet der EU und des EWR die Querschnittsmaterie des Datenschutzrechts für alle Formen der Verarbeitung personenbezogener Daten – von einfachen Adresslisten bis hin zu Systemen Künstlicher Intelligenz in allen Gesellschaftsbereichen – in nur 50 Artikeln mit materiellen Vorgaben. Der Unionsgesetzgeber hat hierfür den Weg anwendungsunabhängiger und technikneutraler Regulierung gewählt. Das war vielfach nur um den Preis höchster Allgemeinheit und Abstraktheit möglich.

Die allgemeinen und abstrakten Regelungen verursachen hohe Rechtsunsicherheit und in deren Folge Handlungshindernisse. Um Entscheidungen im konkreten Fall treffen zu können, müssen die Vorgaben der DS-GVO für unterschiedliche Handlungsfelder präzisiert und in den einzelnen Anwendungen konkretisiert werden. Hierfür sieht die DS-GVO in Art. 40 und 41 selbst vor, dass die Verbände und Vereinigungen der Regelungsadressaten bereichs-, branchen- oder technikspezifische Konkretisierungen der abstrakten Vorgaben vornehmen können.

Dieses von der DS-GVO verfolgte Konzept der Ko-Regulierung durch Staat und Verbände (s. EDSA, Leitlinien 1/2019 Rn. 13) soll dazu beitragen, die abstrakten Regelungen der DS-GVO den Besonderheiten der einzelnen Verarbeitungsbereiche anzupassen (s. EuGH vom 7. Dezember 2023, C 26/22 und C-64/22, Rn. 101 ff. – SCHUFA I). Diese Form der regulierten Selbstregulierung kann dazu beitragen, die Verantwortung der betroffenen Verantwortlichen zu aktivieren, ihre Kenntnisse über Möglichkeiten zur wirtschaftlichen Erfüllung der Datenschutzanforderungen zu nutzen, ihr Interesse an einem Datenschutz durch Technikgestaltung zu stärken und die abstrakten Vorgaben der DS-GVO in vollzugstauglicher Weise zu präzisieren (s. EuGH vom 7. Dezember 2023, C 26/22 und C-64/22, Rn. 101, 104 – SCHUFA I). Damit die Selbstregulierung aber im Rahmen der DS-GVO bleibt und nicht zu einer einseitigen Reduzierung von Datenschutzvorgaben führt, müssen

die Verhaltensregeln nach Art. 40 Abs. 5 DS-GVO zu ihrer Wirksamkeit von der zuständigen Aufsichtsbehörde genehmigt werden.

Für die Nutzung des Instruments der Verhaltensregeln und für die durch sie erreichbare Verbesserung der Rechtssicherheit ist entscheidend, welche Rechtswirkungen mit Verhaltensregeln verbunden sind. Diese Frage wird von der DS-GVO zwar nicht generell beantwortet. Sie enthält zu dieser Frage aber einige Regelungen, die auf Art. 40 DS-GVO verweisen (s. hierzu EDSA, Leitlinien 1/2019, Rn. 18.; näher Roßnagel, Zeitschrift für Datenschutz 2025, 669, 672 f.).

Nach Art. 24 Abs. 3 DS-GVO kann „die Einhaltung der genehmigten Verhaltensregeln gemäß Art. 40 DS-GVO (…) als Gesichtspunkt herangezogen werden, um die Erfüllung der Pflichten des Verantwortlichen nachzuweisen“ (s. auch ErwG 77 Satz 1 DS-GVO).

Verhaltensregeln sind nach Art. 28 Abs. 5 DS-GVO auch für die Pflichten des Auftragsverarbeiters von Bedeutung. Danach kann „die Einhaltung genehmigter Verhaltensregeln (…) durch einen Auftragsverarbeiter (…) als Faktor herangezogen werden, um hinreichende Garantien“ im Sinne des Art. 28 Abs. 1 und 4 DS-GVO „nachzuweisen“.

Nach Art. 32 Abs. 3 DS-GVO kann „die Einhaltung genehmigter Verhaltensregeln (…) als Faktor herangezogen werden, um die Erfüllung der in Art. 32 Abs. 1 DS-GVO genannten Anforderungen nachzuweisen“.

Genehmigte Verhaltensregeln sind nach Art. 35 Abs. 8 DS-GVO außerdem für die Beurteilung der Auswirkungen der Datenverarbeitungsvorgänge im Rahmen der Datenschutz-Folgenabschätzung „gebührend zu berücksichtigen“.

Nach Art. 46 Abs. 2 Buchst. e DS-GVO können genehmigte Verhaltensregeln als „geeignete Garantien“ angesehen werden, um ohne besondere Genehmigung einer Aufsichtsbehörde personenbezogene Daten an ein Drittland oder eine internationale Organisation zu übermitteln.

Schließlich ist bei der Verhängung von Geldbußen nach Art. 83 Abs. 2 Satz 2 Buchst. j DS-GVO die Einhaltung von genehmigten Verhaltensregeln „gebührend“ zu berücksichtigen. Die Einhaltung von Verhaltensregeln soll geldbußenmindernd wirken.

Nach all diesen Regelungen ist die Einhaltung der Verhaltensregeln bei der Konkretisierung der Datenschutzvorgaben „zu berücksichtigen“ (Martini in Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, DS-GVO Art. 24 Rn. 45; Petri/Stief in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, DS-GVO, Art. 24 Rn. 27). Bei einem gelungenen Nachweis kommt diesem eine „Indizwirkung“ zu (Martini in Paal/Pauly, DS-GVO/BDSG, 3. Aufl. 2021, DS-GVO Art. 24 Rn. 45). Manche sehen darin sogar eine „widerlegli-

che Vermutung“ (Sydow/Marsch/Raschauer, DS-GVO/BDSG, 3. Aufl. 2022, DS-GVO Art. 24 Rn. 49; Art. 40 Rn. 6).

Der EDSA fasst die Regelungen der DS-GVO zu Verhaltensregeln dahingehend zusammen, dass Verhaltensregeln ein Instrument sind, um die Einhaltung der DS-GVO nachzuweisen (EDSA, Leitlinien 1/2019, Rn. 1). „Genehmigte Verhaltensregeln haben das Potenzial, sowohl für Auftragsverarbeiter als auch für Verantwortliche wirksame Instrumente zur Gewährleistung der Rechenschaftspflicht zu sein. ErwG 77 DS-GVO und Art. 24 Abs. 3 DS-GVO sehen vor, dass die Einhaltung genehmigter Verhaltensregeln unter anderem eine geeignete Methode bietet, mit der ein Verantwortlicher oder Auftragsverarbeiter die Einhaltung bestimmter Teile oder Grundsätze der Verordnung oder der gesamten Verordnung nachweisen kann“ (EDSA, Leitlinien 1/2019, Rn. 18). Dies gilt sowohl für Aufsichtsbehörden als auch für Gerichte.

Diese Bedeutung von Verhaltensregeln hat das OLG Köln in seinem Urteil vom 10. April 2025 (Az. 15 U 249/24) verkannt. Es hielt die genehmigten Verhaltensregeln des Verbands der Wirtschaftsauskunfteien „für die Prüf- und Löschfristen von personenbezogenen Daten“ „für unerheblich“ (Rn. 24) und hat sich nicht mit ihnen auseinandergesetzt. Hätte sich dieses Urteil durchgesetzt, wären die Wirkungen von Verhaltensregeln praktisch bedeutungslos. Die Zielsetzung von Art. 40 DS-GVO und die Pflicht seines Abs. 1, die Entstehung und Anwendung von Verhaltensregeln zu fördern, wäre „leer gelaufen“.

In der Revisionsinstanz hat jedoch der BGH mit Urteil 18. Dezember 2025 (Az. I ZR 97/25) das Urteil des OLG Köln aufgehoben (s. näher Kap. 13.1). Er führt in seiner Entscheidung aus, dass die in den Verhaltensregeln geregelten Prüf- und Speicherfristen sachgerecht sind und grundsätzlich einen angemessenen Interessenausgleich vornehmen. Im Interesse der Rechtssicherheit und auch mit Blick auf das von Wirtschaftsauskunfteien betriebene Massengeschäft stellen die Verhaltensregeln eine „Orientierung“ für die nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO vorzunehmende Interessenabwägung dar (BGH, Az. I ZR 97/25, Rn. 49 ff.).

1.4
Harmonisierung der Aufsichtstätigkeit durch „Einer für Alle“

Ein gelungenes Beispiel für die Harmonisierung der Aufsichtstätigkeit durch Zusammenarbeit der Aufsichtsbehörden der Länder ist die Datenschutzberatung im Projekt zur Einführung der Bezahlkarte für Asylsuchende. Es zeigt, dass das Konzept „Einer für Alle“ (EfA) auch im Datenschutz umgesetzt werden kann und zu konstruktiven Ergebnissen führt (s. näher Kap. 16.3).

Nachdem politisch der Beschluss gefasst worden war, für Asylsuchende bundesländerübergreifend eine Bezahlkarte einzuführen, beschlossen die Länder (mit Ausnahme von Bayern und Mecklenburg-Vorpommern) im Januar 2024, ein gemeinsames Vergabeverfahren durchzuführen. Da ich im Jahr 2024 Vorsitzender der DSK war und das Land Hessen den Vorsitz in der Ministerpräsidentenkonferenz innehatte, bat mich die Hessische Staatskanzlei, eine frühzeitige Berücksichtigung von datenschutzrechtlichen Belangen bei der konkreten Einführung der Bezahlkarte zu ermöglichen und eine übergreifende Datenschutzbegleitung des Projekts durchzuführen. Der Aufwand für die 14 von dieser gemeinsamen Ausschreibung berührten Aufsichtsbehörden sollte begrenzt und eine einheitliche Bewertung sichergestellt werden. Daher bildeten die betroffenen Aufsichtsbehörden eine kleine Arbeitsgruppe unter meiner Leitung. Sie sollte für alle Aufsichtsbehörden eine gemeinsame Bewertung und Beratung durchführen. Sie bestand aus Vertretern und Vertreterinnen der Aufsichtsbehörden von Hamburg, Baden-Württemberg, Nordrhein-Westfalen und Hessen.

Die Arbeitsgruppe hatte die Aufgabe, zum einen beratend Stellung zu nehmen zu den rechtlichen und technischen Datenschutzanforderungen der Leistungsbeschreibung im Vergabeverfahren und bei Bedarf beispielhafte Ergänzungsvorschläge anzubringen und zum anderen die Entwicklung einer Muster-Datenschutzfolgenabschätzung beratend zu unterstützen. Das Projekt endete im Juni 2025.

Die Vorschläge und Empfehlungen der Arbeitsgruppe wurden von den Ländern nahezu vollständig übernommen und führten dazu, dass Datenschutzaspekte bei der Ausschreibung und der Einführung berücksichtigt wurden. Die Arbeit der Arbeitsgruppe war aber nicht nur inhaltlich erfolgreich, sondern entlastete alle anderen Aufsichtsbehörden, die zwar weiterhin für den Datenschutz der Bezahlkarte in ihrem Bundesland verantwortlich waren, aber die Bewertung der Arbeitsgruppe übernehmen konnten. Sie zeigte außerdem, dass auch in komplexen Verfahren eine bundesweit einheitliche Bewertung der Aufsichtsbehörden der Länder sichergestellt werden kann.

1.5
Mehr Rechtssicherheit durch Gutachten zum Datenschutznachtrag von Microsoft

Eine Stärkung der Rechtssicherheit konnte durch Verhandlungen mit Microsoft (MS) über deren Datenschutznachtrag (Data Protection Addendum – DPA) für die Online-Dienste erzielt werden. In einem umfangreichen Gutachten konnte ich feststellen, dass Microsoft 365 (M365) in Hessen datenschutz-

konform genutzt werden kann, wenn meine Empfehlungen an die nutzenden Verantwortlichen umgesetzt werden.

MS bietet M365 als Cloud-Dienst an. Datenschutzrechtlich gesehen ist daher MS Auftragsverarbeiter und der nutzende Kunde Verantwortlicher. Der Kunde muss mit MS als seinem Auftragsverarbeiter einen in Art. 28 Abs. 3 DS-GVO beschriebenen Vertrag abschließen. MS nutzt dafür seinen DPA. Im November 2022 stellte die DSK fest, dass Verantwortliche den von Art. 5 Abs. 2 DS-GVO geforderten Nachweis, M365 datenschutzrechtskonform zu betreiben, auf der Grundlage des DPA vom 15. September 2022 nicht führen können. Als Grund nannte die DSK, dass das DPA in sieben Kritikpunkten den Vorgaben des Art. 28 DS-GVO für Auftragsverarbeiter nicht entspreche (s. DSK, Festlegung vom 24.11.2022, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf; DSK, Bewertung der aktuellen Vereinbarung zur Auftragsverarbeitung, https://www.datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf).

Über diesen Beschluss der DSK habe ich in Hessen öffentliche und nicht-öffentliche Stellen ausführlich informiert und sie gedrängt, von MS Änderungen des DPA zu verlangen, damit sie M365 datenschutzkonform betreiben können (52. Tätigkeitsbericht zum Datenschutz, Kap. 1.2, S. 11 f.). Mit dieser Zielsetzung habe ich auch mehrere Aufsichtsverfahren durchgeführt. Der Beschluss der DSK und die Umsetzungsmaßnahmen in Hessen haben zu einer großen Verunsicherung geführt. Um mit MS zu klären, unter welchen Voraussetzungen das DPA mit der DS-GVO in Einklang gebracht werden kann, habe ich von Juli 2024 bis November 2025 in vielen intensiven Diskussionsrunden mit MS verhandelt, unter welchen Bedingungen eine praxistaugliche und datenschutzkonforme Nutzung von M365 möglich ist (s. auch 53. Tätigkeitsbericht zum Datenschutz, Kap. 1.7). Maßstab waren die sieben Kritikpunkte der DSK. Ich habe keine technische Untersuchung einzelner M365-Dienste durchgeführt.

In den Verhandlungen konnte ich feststellen, dass sich nach drei Jahren entscheidende Bedingungen geändert haben. Zum einen haben sich rechtliche Vorgaben verändert wie z. B. die Zulässigkeit der Übertragung personenbezogener Daten in die USA auf der Grundlage des EU-US Data Privacy Frameworks. Zum anderen hat MS seine Datenverarbeitung an europäische Anforderungen angepasst wie z. B. durch die EU-Datengrenze, durch die MS fast alle personenbezogenen Daten im Europäischen Wirtschaftsraum verarbeitet. Drittens hat MS Veränderungen in seinem Datenschutzkonzept durchgeführt und ausführlich erläutert. Viertens konnte ich erreichen, dass MS das DPA (für öffentliche Stellen) fortentwickelt hat. Schließlich stellt MS

zusätzliche Informationen bereit wie z. B. das M365-Kit, das den Verantwortlichen bei seiner datenschutzrechtlichen Dokumentation unterstützt (s. ausführlich Kap. 16.2). Die Ergebnisse der Untersuchung sind in dem „Abschlussbericht des HBDI zum Einsatz von M365“ vom 15. November 2025 (137 Seiten) (https://datenschutz.hessen.de/hbdi_m365_bericht) nachzulesen.

Das positive Ergebnis beruht auch auf der Erwartung, dass MS und die Verantwortlichen zusammenwirken, damit Verantwortliche M365 datenschutzrechtskonform nutzen können. Daher endet der Bericht mit Handlungsempfehlungen für die verantwortlichen öffentlichen und nicht-öffentlichen Stellen in Hessen. Auf ihrer Grundlage können verantwortliche Stellen einzelne Bestandteile von M365 einer vertiefenden datenschutzrechtlichen Betrachtung für den konkreten Einsatz unterziehen und im Erfolgsfall datenschutzkonform einsetzen. Das positive Ergebnis bietet nun den Unternehmen und Behörden in Hessen grundlegende Rechts- und Handlungssicherheit für den datenschutzkonformen Einsatz von M365-Produkten. Auch andere Aufsichtsbehörden können sich an diesem Ergebnis und seiner Begründung orientieren, wenn sie eine eigene Bewertung zu dem neuen DPA für öffentliche Stellen durchführen müssen.

1.6
Bündelung von Kompetenzen

Diese Beispiele für den Bürokratieabbau im Datenschutz und die Harmonisierung der Aufsichtstätigkeit sind auch bei einer möglichen Bündelung von Aspekten der Datenschutzaufsicht zu berücksichtigen. Statt neue Bürokratie durch die Zentralisierung der Datenschutzaufsicht über den nicht-öffentlichen Bereich aufzubauen, sollte die Zusammenarbeit zwischen den Aufsichtsbehörden gestärkt werden.

Im Koalitionsvertrag der Fraktionen von CDU, CSU und SPD vom April 2025 findet sich zur Datenschutzaufsicht die nicht weiter ausgeführte Zielsetzung: „Im Interesse der Wirtschaft streben wir eine Bündelung der Zuständigkeiten und Kompetenzen bei der Bundesdatenschutzbeauftragten an“ (Koalitionsvertrag Zeilen 2106–2108). In einem gemeinsamen Beschluss des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder zur Staatsmodernisierung vom 4. Dezember 2025 wird diese Zielsetzung wieder aufgegriffen: „Der Bund wird in Abstimmung mit den Ländern die Datenschutzaufsicht für den nicht-öffentlichen Bereich bis spätestens 31.12.2027 reformieren und dabei gegebenenfalls auch die Aufgabenverteilung im Föderalstaat neu justieren. Ziel ist die Sicherstellung der **einheitlichen** Rechtsauslegung und -anwendung sowie Erhöhung der Effizienz im Zusammenspiel

der Aufsichtsbehörden. Hierzu können insbesondere die **Bündelung von Kompetenzen bei der BfDI oder Aufsichtsbehörden der Länder** (bspw. durch Zuständigkeitskonzentration und/oder One-Stop-Shop-Regelungen), eine bessere Einbindung der DSK und/oder die Einführung eines Kohärenzverfahrens unter Nutzung der Möglichkeiten des Art. 87 Abs. 3 GG auf Bundesebene oder im Wege von Staatsverträgen zwischen den Ländern gehören“ (Rn. 158 – Hervorhebungen im Original).

Bei der Umsetzung dieser Vorhaben ist zu berücksichtigen, welche Interessen bei einer Reform der Datenschutzaufsicht „die Wirtschaft“ hat und welche Anforderungen an eine effektive Aufsicht zu stellen sind. Hinsichtlich der Aufsichtsstruktur gibt es kein einheitliches Interesse „der“ Wirtschaft (s. Tagesspiegel vom 23. Januar 2026 zu den Stellungnahmen von Wirtschaftsverbänden gegenüber den Bundesministerien für Wirtschaft und Energie sowie des Innern). Vielmehr gibt es vielfältige, sogar gegenläufige Interessen von Wirtschaftsakteuren. Zu bedenken ist, dass 99,3 % der Wirtschaftsakteure kleine oder mittlere Unternehmen sind. Diese bevorzugen mehrheitlich eine Aufsicht in ihrer Nähe, die mit den lokalen Besonderheiten vertraut und jederzeit unmittelbar ansprechbar ist. Diesem Interesse würde eine Bündelung von Zuständigkeiten bei einer Bundesbehörde in Bonn widersprechen.

Die Datenaufsichtsbehörden unterstützen die Zielsetzung, bürokratische Aufwände zu reduzieren (s. Kap. 1.2). Nur: Dies geht nicht über die Aufsichtsstruktur, sondern nur durch Änderungen der Rechtsgrundlagen, also der DS-GVO, des BDSG und der Landesdatenschutzgesetze –, etwa durch einen viel stärker am Risiko – nicht an der Größe – orientierten Pflichtenkatalog für Unternehmen oder durch eine Verlagerung von Pflichten auf Hersteller eines IT-Systems oder Anbieter eines IT-Dienstes, die über die notwendigen Informationen verfügen, um z. B. Musterdokumentationen zu erstellen, die Millionen Nutzende, denen diese Informationen fehlen, entlasten würden (s. Kap. 1.2).

Eine Reform der Datenschutzaufsichtsstruktur sollte darauf zielen, möglichst nur einen behördlichen Ansprechpartner sowie klare rechtliche Rahmenbedingungen zu haben. Dafür braucht es eine Konzentration von Zuständigkeiten im föderalen Gefüge, die von zentraler Koordinierung begleitet werden.

Die Aufsichtsbehörden der Länder schlagen daher folgende konkrete Maßnahmen vor, die in das BDSG übernommen werden sollten (s. Fuchs/Kamp/Roßnagel, Frankfurter Allgemeine Zeitung vom 9. Juli 2025, S. 18):

1. Nationaler One-Stop-Shop: Bei länderübergreifenden Datenverarbeitungen durch verbundene Unternehmen oder Forschungsvorhaben sollte nur

noch eine Aufsichtsbehörde zuständig sein, wie dies im Entwurf eines Forschungsdatengesetzes vorgesehen ist.

2. Einer-für-Alle-Prinzip: Eine Aufsichtsbehörde sollte für alle anderen Aufsichtsbehörden verbindlich Datenverarbeitungsverfahren prüfen, die in identischer Form in verschiedenen Bundesländern oder länderübergreifend zum Einsatz kommen (s. das Beispiel Kap. 1.4).
3. Institutionalisierung der DSK mit verbindlichen Beschlüssen: Die DSK sollte gesetzlich verankert werden und die Befugnis erhalten, mit Mehrheitsentscheidungen für alle Mitglieder bindende Beschlüsse zu treffen.
4. Zentrale Zuständigkeit bei „Marktortfällen“: Die Bundesdatenschutzbeauftragte (BfDI) sollte in Fällen allein zuständig sein, in denen Verantwortliche keine Niederlassung in der Europäischen Union oder im Europäischen Wirtschaftsraum unterhalten, aber gleichwohl der DS-GVO unterfallen.
5. Zentrale Technologieberatung: Die BfDI sollte allein zuständig sein, Anbieter von Datenverarbeitungsdiensten mit Infrastrukturcharakter für viele Nutzer im Bundesgebiet zu beraten, wie sie technisch das Prinzip des „Data Protection by Design“ umsetzen können.
6. Zentrale Koordinierung: Bei der BfDI sollte eine Geschäftsstelle der DSK eingerichtet werden, um eine effiziente Koordinierung der Aufsichtsbehörden zu unterstützen.
7. Zentrale Koordinierung von Verhaltensregeln und Akkreditierung von Zertifizierungsstellen: Verhaltensregeln von Verbänden und die Zertifizierung von Verarbeitungsvorgängen sind Mechanismen zum Bürokratieabbau, die die DS-GVO selbst vorsieht, um Rechtsunsicherheit zu verringern (s. Kap. 1.3). Verhaltensregeln sind von der zuständigen Aufsichtsbehörde zu genehmigen und Zertifizierungsstellen zu akkreditieren. Die BfDI sollte diese Prüfungen zentral koordinieren.
8. Zentrale Vertretung in Normierungsverfahren: Werden in technischen Standards Datenschutzanforderungen berücksichtigt, entlastet dies die Anwender von Informationstechnik sehr. Daher sollte die BfDI in solchen Normierungsverfahren zur Erarbeitung technischer Standards stellvertretend für alle übrigen Aufsichtsbehörden mitwirken.

Dieser Reformvorschlag wahrt die Vorteile einer föderalen Aufsichtsstruktur. Die Datenschutzaufsichtsbehörden der Länder garantieren einen einheitlichen Datenschutz im öffentlichen und nicht-öffentlichen Bereich. Sie verfügen über spezifische Branchenexpertise, gewährleisten kurze Wege für Betroffene und Unternehmen und ermöglichen eine effiziente Lastenverteilung. Durch ihre föderale Struktur geben sie auch die Garantie dafür, dass durch die Einflussnahme auf eine einzige Behörde der Datenschutz nicht flächendeckend ausgehebelt werden kann.

Der Reformvorschlag erreicht aber auch die Zielsetzung des Koalitionsvertrags und des Beschlusses von Bund und Ländern zur Staatsmodernisierung. Er ermöglicht eine Vereinheitlichung der Rechtsanwendung und eine effizientere Organisation der Datenschutzaufsicht. Bereits bisher hat die DSK in ihrer Geschäftsordnung bindende Mehrheitsentscheidungen vorgesehen. Nun gilt es diesen Kooperationsmechanismus zu stärken und auf gesetzliche Ebene zu heben, mit einer Institutionalisierung der DSK und einer Regelung zu verbindlichen Mehrheitsbeschlüssen.

Durch zentrale Ansprechpartner und verbindliche Prüfergebnisse auf der Basis gemeinsamer Prüfstandards im Sinne eines „Eine-prüft-für-alle“ können Zuständigkeitsabgrenzungen und Doppelprüfungen vermieden werden. Davon profitieren sowohl die Wirtschaft als auch die Forschung, die auch in verschiedenen Ländern mit einheitlichen Entscheidungen rechnen können. Die Bündelung von Koordinierungsfunktionen bei der BfDI unterstützt kohärente Aufsichtsstrukturen.

Eine vollständige Aufgabenübertragung an eine zentrale Bundesbehörde wird hingegen nicht funktionieren. Dieser Idee liegt ein falsches Bild der tatsächlichen, bürgernahen Aufgabenwahrnehmung durch Datenschutzbehörden zugrunde. Denn diese ist dadurch geprägt, individuellen Beschwerden, Hinweisen und Beratungsanfragen nachzugehen. Im nicht öffentlichen Bereich bearbeiten die Aufsichtsbehörden zusammen jedes Jahr ca. 70.000 Fälle. Alle diese Fälle auf die BfDI zu übertragen, würde einen Ressourcenzuwachs von jetzt 430 auf etwa 900 Stellen erfordern. Das kostet Zeit und Geld. Außerdem zeigt die Erfahrung, dass sehr große Behörden nicht weniger bürokratisch arbeiten (Roßnagel, Zeitschrift für Datenschutz 2025, 181 f).

1.7
Bürokratiezuwachs durch Zuständigkeitsverteilung

Bürokratie wird auch abgebaut, wenn Doppelzuständigkeiten vermieden oder beseitigt werden. Solche Doppelzuständigkeiten werden jedoch nach den Entwürfen der Bundesregierung für ein Gesetz zur Durchführung der KI-VO und für ein Gesetz zur Durchführung des Data Act neu geschaffen.

Datenverarbeitung durch KI

Der Gesetzentwurf regelt die behördliche Aufsichtsstruktur zur Durchführung und Überwachung der KI-VO. Damit kommt er dem Auftrag der KI-VO nach, wonach innerhalb von 12 Monaten nach Inkrafttreten der KI-VO am 1. August 2024 national zuständige Behörden einzurichten oder zu benennen sind.

Art. 74 Abs. 8 KI-VO und ErwG 159 KI-VO sehen für die Marktaufsicht über die Hochrisiko-KI-Systeme im Kontext von Strafverfolgung, Wahlen, Grenzkontrolle und Justizverwaltung gemäß Anhang III Nr. 1, 6, 7, 8 KI-VO die nach der JI-Richtlinie zuständigen Behörden vor. Dies sind in Deutschland die Datenschutzaufsichtsbehörden. Damit wollte der EU-Gesetzgeber die bei den Datenschutzaufsichtsbehörden bestehenden Befugnisse und vorhandenen Erfahrungen in der Aufsicht über die entsprechenden sensiblen Bereiche nutzen und Doppelzuständigkeiten für ein und denselben Lebenssachverhalt vermeiden.

Der Gesetzentwurf überträgt die Marktaufsicht über diese Hochrisiko-KI-Systeme vollständig auf die Bundesnetzagentur – mit der Folge, dass dadurch Doppelzuständigkeiten entstehen. Denn die Datenschutzaufsichtsbehörden behalten ihre Aufgaben nach der DS-GVO und der JI-RL, da bei dem Einsatz von KI in der Strafverfolgung und in der Justizverwaltung sowie bei Wahlen und Grenzkontrollen immer personenbezogene Daten verarbeitet werden. Für die gleiche Datenverarbeitung würde nach dem Gesetzentwurf die Bundesnetzagentur für die Einhaltung der KI-VO und die zuständige Datenschutzaufsichtsbehörde für die Einhaltung der Datenschutzvorschriften zuständig sein (s. auch DSK, Stellungnahme zum Entwurf eines Gesetzes zur Durchführung der KI-VO vom 10. Oktober 2025, https://www.datenschutzkonferenz-online.de/media/st/Stellungnahme_Durchfuehrungsgesetz_KI-VO.pdf). Dieser Gesetzentwurf führt zum Gegenteil von Bürokratieabbau.

Datenverarbeitung nach dem Data Act

Ziel des Data Act (DA) ist es, die Verwendung von Daten, die bei der Nutzung von vernetzten Produkten und verbundenen Diensten (z. B. Geräte in der Industrie, in der Verwaltung und in privaten Haushalten mit Verbindungen zum Internet) entstehen, zu verbessern und die sie betreffenden Regelungen unionsweit zu vereinheitlichen. Nutzerinnen und Nutzer sollen darüber entscheiden können, ob sie diese Daten erhalten oder ob sie an Dritte (z. B. Reparaturbetriebe) weitergegeben werden. Auch öffentliche Stellen haben einen Anspruch, dass ihnen in Notfällen die Daten aus der Gerätenutzung übermittelt werden.

Sind in den nutzungsgenerierten Daten auch personenbezogene Daten enthalten (also zum Beispiel bei Geräten, die klar einer Person zugeordnet werden können, wie zum Beispiel Haushaltsgeräte oder Autos), richtet sich deren Verarbeitung nach der DS-GVO. Im Fall eines Widerspruchs zwischen DA und DS-GVO geht nach Art. 1 Abs. 5 Satz 3 DA die DS-GVO vor.

Nach Art. 37 Abs. 1 DA benennen die Mitgliedstaaten eine oder mehrere zuständige Behörden, die für die Anwendung und Durchsetzung des DA verantwortlich sind. Nach § 2 des Entwurfs der Bundesregierung zur Umsetzung des DA soll diese Zuständigkeit bei der Bundesnetzagentur liegen.

In Art. 37 Abs. 3 Satz 1 DA ist ferner geregelt, dass die für die Überwachung der Anwendung der DS-GVO zuständigen Aufsichtsbehörden bezüglich des Schutzes personenbezogener Daten auch für die Überwachung der Anwendung des DA zuständig sind. Diese Aufsicht über die Verarbeitung personenbezogener Daten durch Verantwortliche aus dem öffentlichen und nicht-öffentlichen Bereich in Hessen haben § 40 Abs. 1 BDSG und § 13 Abs. 1 HDSIG mir, als dem Hessischen Beauftragten für Datenschutz, übertragen.

Im Gegensatz dazu soll nach § 3 des Entwurfs die Zuständigkeit für die Überwachung der Anwendung der DS-GVO im Rahmen des DA auf die BfDI übertragen werden. Dies führt zu Doppelzuständigkeiten für den gleichen Lebenssachverhalt und zu Rechtsunsicherheiten für alle Beteiligten (s. hierzu auch DSK, Stellungnahme zum Entwurf eines Data Act-Durchführungsgesetzes vom 13. März 2025, https://datenschutzkonferenz-online.de/media/st/Data_Act_Umsetzung_Laenderstellungnahme.pdf).

Denn nach § 3 des Entwurfs sind für die Bereitstellung von Daten die BfDI und für alle anderen Formen der Datenverarbeitung die Landesaufsichtsbehörden zuständig. Für die der Bereitstellung vorangehende Erhebung und weitere Verarbeitung von Nutzungsdaten gilt die DS-GVO und sind nach wie vor die Landesaufsichtsbehörden zuständig. Soweit es im Anwendungsbereich des DA um Nutzungsanliegen mit personenbezogenen Daten geht, sind damit zwangsläufig auf Seiten der Datenempfänger stets (Weiter-)Verarbeitungen verbunden, die ebenfalls in vollem Umfang der DS-GVO unterliegen. Damit ergibt sich für Unternehmen und Behörden das Gegenteil der beabsichtigten Zuständigkeitsvereinfachung, nämlich eine Doppelaufsicht durch eine Bundes- und eine Landesbehörde zum gleichen Lebenssachverhalt. Für die primäre Bewertung ihres Datennutzungsanliegens nach dem DA sind BNetzA und BfDI zuständig und für vorausgehende und nachfolgende Datenverarbeitungen die Landesaufsichtsbehörden.

Um dies an einem Beispiel zu illustrieren: Ob der Hersteller eines vernetzten Gerätes bestimmte Daten, die durch die Gerätenutzung entstehen, erheben, speichern und auswerten darf, wäre eine Frage, die ich zu entscheiden hätte. Ob der Nutzer einen Anspruch hat, dass der Hersteller ihm oder einem Dritten diese bereitstellt, hätte die BfDI zu prüfen und ihr Ergebnis mit der BNetzA abzustimmen. Ob der Nutzer die Daten abfragen und für eigene Zwecke weiterverarbeiten darf oder ob der Dritte die Daten für irgendwelche Zwecke verarbeiten darf, hätte wiederum ich zu prüfen. Hätte der Hersteller

die Nutzungsdaten z. B. mit anderen Daten zusammen zu einem Nutzungsprofil verarbeitet, wäre für diese Datenverarbeitung und die Verwendung des Ergebnisses ebenfalls ich zuständig. Für diese Daten gilt der DA nicht.

Da die Datenschutzfragen im Rahmen des DA beinahe immer auch mit Datenschutzfragen zu den Datenverarbeitungen vor der Bereitstellung und zu Weiterverarbeitungen nach der Bereitstellung verbunden sind, bewirkt der Entwurf, dass immer mindestens zwei Datenschutzaufsichtsbehörden für den gleichen Lebenssachverhalt zuständig sind. Mindestens zwei unterschiedliche Aufsichtsbehörden führen parallele Aufsichtsverfahren durch und sind für die Interpretation von Grundfragen des Datenschutzrechts sowie zur Bewertung eines verwobenen Sachverhalts zuständig. Dies ist immer mit dem Risiko divergierender Beurteilungen verbunden. Die dadurch entstehende Rechtsunsicherheit wird durch die Möglichkeit divergierender Entscheidungen unterschiedlicher Gerichte erheblich verstärkt.

Eine einheitliche Vollzugspraxis kann nicht dadurch erreicht werden, dass allein die BfDI im Rahmen des DA zuständig wäre. Denn es geht um Regeln und Begriffe der DS-GVO, die für alle Anwendungsbereiche gleich ausgelegt und praktiziert werden müssen. Die BfDI käme daher auch in diesem Fall nicht darum herum, sich mit den Aufsichtsbehörden der Länder in diesen Fragen abzustimmen.

Um Bürokratieaufbau und Rechtsunsicherheit zu vermeiden, sollte § 3 des Entwurfs ersatzlos gestrichen werden. (s. hierzu auch die Stellungnahme des Bundesrats vom 19. Dezember 2025, BR-Drs. 636/25, S. 2).

2. Europäische und internationale Zusammenarbeit

Als hessische Aufsichtsbehörde für den Datenschutz bin ich zwar nur für Verantwortliche in Hessen zuständig, aber zugleich in ein europäisches Netzwerk von Aufsichtsbehörden eingebunden, um dazu beizutragen, dass die DS-GVO in Europa möglichst einheitlich angewendet wird. Die europaweite und weltweite Nutzung von Datenverarbeitungssystemen erfordert eine grenzüberschreitende Zusammenarbeit mit Aufsichtsbehörden in anderen Ländern. Diese grenzüberschreitenden Verfahren haben sich im Berichtsjahr weiterentwickelt (Kap. 2.1). Die grenzüberschreitende Zusammenarbeit mit Verantwortlichen in den USA wird durch das EU-US-Datentransferabkommen geprägt. Dieses wurde durch ein Urteil des Europäischen Gerichts bestätigt (Kap. 2.2). Die Zusammenarbeit mit anderen Aufsichtsbehörden in der EU wird durch ein Austausch-Programm des Europäischen Datenschutzausschusses gefördert, an dem auch meine Behörde teilgenommen hat (Kap. 2.3). Internationale Begegnungen in meiner Dienststelle in Wiesbaden fanden mit Japan und der Türkei statt (Kap. 2.4).

2.1 Entwicklung der grenzüberschreitenden Verfahren

Im Jahr 2025 sind die Verfahren zur Feststellung der federführenden Behörde nach Art. 56 DS-GVO deutlich angestiegen. Diese Entwicklung entspricht einem europaweit beobachteten Trend zu mehr grenzüberschreitender Zusammenarbeit der Datenschutzaufsichtsbehörden. Auch andere Datenschutzaufsichtsbehörden in Deutschland berichten von ähnlichen Zuwächsen.

Für Hessen zeigt sich der Anstieg vor allem in der Gesamtzahl der Beschwerden, die zu einem Art. 56-Verfahren führen. Bei den Verfahren, in denen ich als federführende Aufsichtsbehörde eingebunden bin, zeigt sich hingegen ein leichter Rückgang.

Europäisches Verfahren	Anzahl 2021	Anzahl 2022	Anzahl 2023	Anzahl 2024	Anzahl 2025
Art. 56-Verfahren gesamt	1.419	645	562	883	1.072
Art. 56-Verfahren mit Betroffenheit	47	11	13	289	308
Art. 56-Verfahren mit Federführung	16	2	4	12	10
Art. 61-Verfahren (Amtshilfe)	92	155	144	192	204

Eine eindeutige Ursache lässt sich nicht benennen. Allerdings ist zu erwähnen, dass einzelne eindeutig zuzuordnende Fälle über Art. 61-Verfahren an uns übermittelt wurden und daher nicht als federführende Art. 56-Verfahren erfasst werden. Darüber hinaus werden zunehmend weniger komplexe Sachverhalte im Binnenmarktinformationssystem (Internal Market Information System, IMI) eingestellt, was ebenfalls zu einer Verschiebung zwischen den Verfahrenskategorien führt.

Zudem tragen international ausgerichtete Unternehmen mit hohem Beschwerdeaufkommen – etwa aus den Bereichen Luftverkehr oder Vermittlungsplattformen – zu dem beobachteten Anstieg der grenzüberschreitenden Verfahren bei.

Die steigende Zahl der Verfahren nach Art. 56 DS-GVO unterstreicht die wachsende Bedeutung der europäischen Kooperation. Für meine Behörde bringt diese Entwicklung vor allem eine steigende Arbeitsbelastung in grenzüberschreitenden Verfahren mit sich. Gleichzeitig gewinnt die Rolle als federführende Behörde an Bedeutung, da häufiger Verfahren koordiniert und zwischen mehreren Aufsichtsbehörden abgestimmt werden müssen.

2.2
EuG-Urteil zum EU-US-Datentransferabkommen

Am 3. September 2025 hat das Europäische Gericht (EuG) in erster Instanz eine Nichtigkeitsklage des französischen Abgeordneten und Mitglieds der französischen Datenschutzaufsichtsbehörde „Commission Nationale de l'Informatique et des Libertés“ (CNIL) Philippe Latombe gegen den Angemessenheitsbeschluss der Europäischen Kommission zum EU-US Data Privacy Framework vom 10. Juli 2023 abgewiesen (Rechtssache T-553/23) und bestätigt, dass die USA zum Zeitpunkt der Entscheidung ein angemessenes Datenschutzniveau gewährleistet haben. Das Datentransferabkommen zwischen der EU und den USA bleibt damit – zumindest vorerst – als Grundlage für transatlantische Datenübermittlungen in Kraft. Das EuG-Urteil hat daher – jedenfalls kurzfristig – für Aufatmen in der Wirtschaft und bei den Aufsichtsbehörden gesorgt.

Der mit der Klage angegriffene Angemessenheitsbeschluss der Europäischen Kommission nach Art. 45 DS-GVO bescheinigt den USA ein adäquates Datenschutzniveau und ausreichende Rechtsdurchsetzungsmöglichkeiten für EU-Bürgerinnen und -Bürger. Der Beschluss kam zustande, weil die frühere US-Regierung von Präsident Joe Biden im Oktober 2022 mit dem „Trans Atlantic Data Privacy Framework“ (TADPF) neue Schutzmechanismen für Daten europäischer Bürgerinnen und Bürger in den USA installiert

hatte. Allerdings hatte Biden diese Mechanismen nicht mit einem Gesetz abgesichert, sondern lediglich per präsidialem Dekret erlassen (S. 52 Tätigkeitsbericht, Kap. 2.2).

Das Bestehen eines angemessenen Datenschutzniveaus und ausreichender Rechtsdurchsetzungsmöglichkeiten zweifelte der französische Abgeordnete Latombe an und wollte den Angemessenheitsbeschluss mit einer am 6. September 2023 eingereichten Nichtigkeitsklage zu Fall bringen. Er berief sich in seiner Klage ausdrücklich auf seine Rechte als Privatbürger und monierte seitens der USA Verstöße gegen die Grundrechtecharta der EU. Die Europäische Kommission könne einen wirksamen Rechtsbehelf in den USA und ein unparteiisches Gericht nicht garantieren, weil beide im TADPF nicht vorgesehen seien. Die in den USA errichtete Rechtsbehelfsbehörde (Data Protection Review Court, DPRC) sei durch einen Akt der amerikanischen Exekutive und nicht durch Gesetz geschaffen und deshalb kein unabhängiges Gericht, wie es die DS-GVO fordere.

Das EuG sah dies in seinem Urteil im September 2025 anders. Die Ernennung der Richter des DPRC und seine Arbeitsweise seien „ausweislich der Akten mit mehreren Garantien und Bedingungen verbunden, die die Unabhängigkeit seiner Mitglieder gewährleisten sollen“. Ohnehin habe die Europäische Kommission sich selbst im Angemessenheitsbeschluss auferlegt, „die Anwendung des Rechtsrahmens, der Gegenstand des Beschlusses ist, fortlaufend zu überwachen“. Wenn sich der Rechtsrahmen ändere, also etwa das von Joe Biden installierte TADPF-Dekret von seinem Nachfolger US-Präsident Donald Trump für nichtig erklärt würde, könne die Europäische Kommission „soweit erforderlich beschließen, den angefochtenen Beschluss auszusetzen, zu ändern oder aufzuheben oder seinen Anwendungsbereich einzuschränken“.

Das Urteil war von der Wirtschaft und den Aufsichtsbehörden mit Spannung erwartet worden. Denn die Auswirkungen einer Nichtigerklärung des Angemessenheitsbeschlusses wären immens. Von dem Bestehen des Angemessenheitsbeschlusses ist etwa abhängig, ob in der EU ansässige Unternehmen rechtssicher personenbezogene Daten in US-Clouds speichern und verarbeiten können. Ich musste im Vorfeld des Urteils daher einen starken Anstieg an Beratungsanfragen bewältigen und mich auf alle im Rahmen der Urteilsverkündung möglichen Szenarien vorbereiten.

Letztlich ist der französische Abgeordnete Latombe mit seinem Anliegen, den Angemessenheitsbeschluss zu kippen, zwar in erster Instanz gescheitert, hat jedoch bereits Rechtsmittel gegen die Entscheidung des EuG eingelegt. Auch das EuG hatte in seinem Urteil dessen Vorläufigkeit bereits deutlich gemacht, indem es in Randnummer 22 ausführte, dass es die Rechtmäßigkeit des Unionsakts anhand der zum Zeitpunkt des Erlasses vorliegenden

tatsächlichen und rechtlichen Umstände zu beurteilen habe und zugleich in Randnummer 58 feststellte, dass die Europäische Kommission verpflichtet sei, kontinuierlich zu überwachen, ob die USA weiterhin ein angemessenes Schutzniveau gewährleisten. Dies ist unter der Trump-Administration zweifelhaft.

Die Entscheidung des EuG wird aufgrund des eingelegten Rechtsmittels in zweiter Instanz vom Europäischen Gerichtshof (EuGH) überprüft werden. Der Ausgang und die Auswirkungen für meine aufsichtsbehördliche Praxis sind offen.

2.3
Austausch-Programm des Europäischen Datenschutzausschusses

Im Berichtsjahr hat meine Behörde erneut am Secondment Programm des Europäischen Datenschutzausschusses (EDSA) teilgenommen. Im Rahmen dieses Austauschprogramms finden alle zwei Jahre Kurzzeit-Abordnungen des Personals der europäischen Datenschutzaufsichtsbehörden, des EDSA und des Europäischen Datenschutzbeauftragten (EDSB) statt. Mitarbeitende können für einen Zeitraum von mindestens zwei Wochen bis zu sechs Monaten zu einer anderen Datenschutzaufsichtsbehörde wechseln. Vor der Abordnung findet ein zweitägiges Secondment Training in Brüssel statt.

Mit dem Angebot des Secondment Programms kommt der EDSA seiner in Art. 70 Abs. 1 Buchst. v DS-GVO festgeschriebenen Aufgabe nach, Schulungsprogramme zu fördern und den Personalaustausch zwischen den Aufsichtsbehörden zu erleichtern. Das übergeordnete Ziel des Secondment Programms ist es, durch den Personalaustausch ein gemeinsames Verständnis der DS-GVO und deren einheitliche Anwendung zu fördern. In der täglichen Arbeit meiner Behörde zeigt sich immer wieder, wie wichtig es ist, dass die Datenschutzaufsichtsbehörden in Deutschland sowie in Europa mit möglichst einer Stimme sprechen. Jedoch treffen in der Praxis teils sehr unterschiedliche (Verwaltungs-)Kulturen, Rechtstraditionen und nationale Verfahrensvorschriften aufeinander, was die Zusammenarbeit vor Hürden stellen kann. Vor diesem Hintergrund leistet das Secondment Programm einen wertvollen und wichtigen Beitrag dazu, Brücken zu bauen und die DS-GVO einheitlich anzuwenden.

Bereits vor zwei Jahren hatte eine Mitarbeiterin am Pilotprojekt des Secondment Programms teilgenommen und für zwei Wochen bei der schwedischen Datenschutzaufsichtsbehörde „Integritetsskyddsmyndigheten“ gearbeitet. Diese Erfahrung zeigte ganz ausdrücklich, dass der Austausch die Auf-

sichtsbehörden zusammenrücken lässt und helfen kann, unterschiedliche Rechtsauffassungen in Einklang zu bringen.

Bei der diesjährigen zweiten Auflage des Secondment Programms war nun auch meine Behörde Gastgeber für Kolleginnen anderer europäischer Datenschutzaufsichtsbehörden. So war im März und April dieses Jahres eine Kollegin der ungarischen Datenschutzaufsichtsbehörde „Nemzeti Adatvédelmi és Információszabadság Hatóság“ für zwei Wochen zu uns nach Wiesbaden abgeordnet und hat insbesondere die Stabsstelle Europa und Internationales sowie das Justiziariat tatkräftig unterstützt. Im Juni durften wir dann für einen Monat eine Kollegin der finnischen Datenschutzaufsichtsbehörde „Tietosuojavaltuutetun toimisto“ als Gast empfangen. Auch die finnische Kollegin war vorwiegend in der Stabsstelle Europa und Internationales tätig und hat an grenzüberschreitenden One Stop Shop-Fällen und Prüfungen von Binding Corporate Rules mitgewirkt. Zudem war im Berichtsjahr eine meiner Mitarbeiterinnen für zwei Wochen an die litauische Datenschutzbehörde „Valstybinė duomenų apsaugos inspekcija“ und eine andere Mitarbeiterin für zwei Wochen an die italienische Datenschutzaufsichtsbehörde „Garante per la protezione dei dati personali“ abgeordnet.

Auch in den kommenden Jahren beabsichtige ich, Gäste von anderen Aufsichtsbehörden zu empfangen und Mitarbeitende meiner Behörde zu anderen Aufsichtsbehörden zu entsenden, um den wichtigen Austausch und Dialog fortzuführen.

2.4
Besuch internationaler Delegationen

Da sie sich für unsere Aufsichtspraxis interessierten, besuchten uns mehrere Delegationen von außerhalb der EU und des EWR.

Am 3. März 2025 begrüßten wir aus Japan den Staatsrechtler Prof. Dr. Takashi Jitsuhara von der Universität Nanzan in Nagoya, Prof. Dr. Yuta Numoto von der Universität Doshisha in Kyoto sowie Yuta Ishihara, einen Promotionsstudent der Universität Keio. Prof. Jitsuhara leitet eine Forschungsgruppe der Stiftung des Japanischen Rechtsanwaltsverbands. Die Forschungsgruppe besteht aus etwa zehn Rechtsanwälten und akademischen Mitgliedern. Sie untersucht die notwendigen materiellen Bedingungen für die Unabhängigkeit der „Personal Information Protection Commission“, der japanischen Datenschutzaufsichtsbehörde. Themen der Besprechung waren insbesondere die Situation der deutschen Datenschutzaufsichtsbehörden, die Unabhängigkeit und die Anforderungen an unabhängige Datenschutzbeauftragte, der Vergleich zwischen Datenschutzbeauftragten und Koordinatoren im Rahmen des Data

Services Act sowie das Verhältnis zwischen dem Bund, den Ländern und der EU in Fragen der Datenschutzaufsicht.

Am 16. Dezember 2025 besuchten uns der Präsident der Türkischen Datenschutzaufsichtsbehörde (KVKK), Prof. Dr. Faruk Bilir, und der Vizepräsident der Datenschutzaufsichtsbehörde und Mitglied des Datenschutzausschusses Tamer Aksoy sowie die Datenschutzexpertin Hazal Deniz Atasoy in Wiesbaden. Gegenstände des Erfahrungs- und Meinungsaustausches waren die unterschiedlichen und überschneidenden Aufgaben der beiden Aufsichtsbehörden, besondere aktuelle Herausforderungen für den Datenschutz, Erfahrungen aus der Sanktionspraxis und weitere Themen der praktischen Aufsichtstätigkeit.

3. Verfahren vor Gerichten und zur Verhängung von Geldbußen

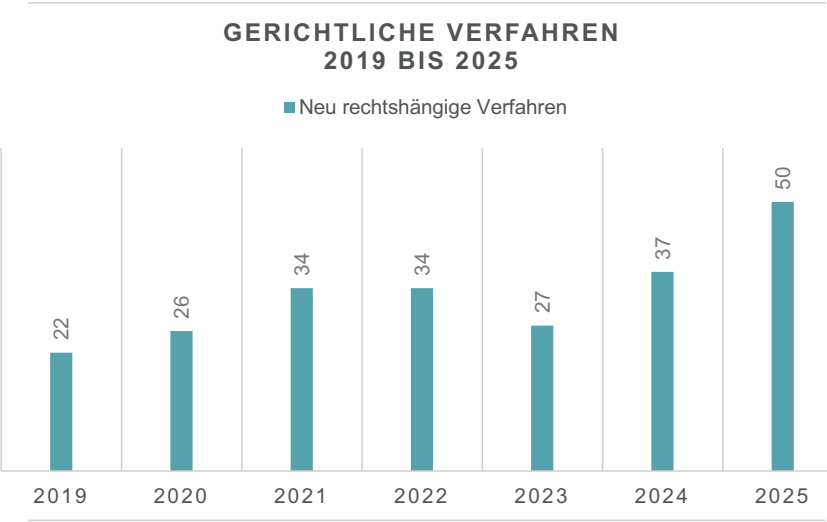
Die DS-GVO hat dazu geführt, dass Gerichts- und Sanktionsverfahren für die Tätigkeit der Datenschutzaufsichtsbehörden an Bedeutung zunehmen (s. 51. Tätigkeitsbericht Kap. 1). Auch im Berichtszeitraum ist die Zahl der Gerichtsverfahren (Kap. 3.1) und der Verfahren zur Verhängung von Geldbußen (Kap. 3.2) jeweils weiter angestiegen. Dies ist vor allem für die Bearbeitung von Beschwerden für meine Behörde herausfordernd. Durch die Rechtsprechung des EuGH, aber auch des örtlich zuständigen Verwaltungsgerichts Wiesbaden nimmt die Rechtssicherheit in der Datenschutzaufsicht immer mehr zu.

3.1
Gerichtsverfahren

Im Jahr 2025 nahm die Zahl gerichtlicher Auseinandersetzungen deutlich zu. Diese Entwicklung zur immer stärkeren Juridifizierung des Datenschutzes unterstreicht die wachsende Bedeutung verbindlicher rechtlicher Einordnungen. Der folgende Überblick stellt die maßgeblichen Entwicklungen und Entscheidungen vor.

Im Berichtsjahr war ich im Bereich der Gerichtsverfahren stärker gefordert als je zuvor. Zusätzlich zu einigen älteren Verfahren erforderten insgesamt 50 neue Verfahren meine Mitwirkung. Diese Entwicklung zeigt, dass datenschutzrechtliche Fragestellungen vermehrt vor die Gerichte getragen werden und meine Behörde in ihrer prozessualen Rolle zunehmend beansprucht wird.

Den Schwerpunkt bildeten wie in den Vorjahren Klagen vor dem Verwaltungsgericht Wiesbaden. Hinzu kamen unter anderem Verfahren vor dem Hessischen Verwaltungsgerichtshof Kassel sowie ein Verfahren vor dem Landgericht Marburg. Zudem erhielt ich in einer Grundrechtsklage vor dem Staatsgerichtshof des Landes Hessen sowie in zwei Unterlassungsklageverfahren vor dem Oberlandesgericht Frankfurt am Main Gelegenheit, meine datenschutzrechtliche Auffassung darzustellen. Einen detaillierten Einblick geben die folgenden Übersichten:



Die hohe Zahl und die Vielfalt der einzelnen Verfahren zeigen nicht nur die breite Themenpalette, mit der ich mich im Berichtsjahr befassen musste, sondern auch die zunehmende Bedeutung gerichtlicher Klärung für die Anwendung des Datenschutzrechts. Ein klarer Schwerpunkt trat dabei nicht hervor. Die thematische Bandbreite reichte von grundsätzlichen Fragen bis hin zu wiederkehrenden formalen Streitigkeiten ohne datenschutzrechtlichen Bezug, wie sie im Alltag meiner Behörde häufiger auftreten. Im Folgenden beleuchte ich die wichtigsten Entwicklungen sowie ausgewählte Entscheidungen, die im Berichtsjahr für meine Tätigkeit besonders relevant waren.

Unterlassungsklageverfahren gegen die Deutsche Bahn Fernverkehr AG

Das Urteil des Oberlandesgerichts Frankfurt am Main vom 10. Juli 2025 (6 UKl 14/24) im Unterlassungsklageverfahren gegen die Deutsche Bahn Fernverkehr AG (Deutsche Bahn) fand breite mediale Aufmerksamkeit. Mit seiner Entscheidung verurteilte das Gericht die Deutsche Bahn, es zu unterlassen, den Erwerb von „Spar-“ und „Super-Sparpreistickets“ von der Angabe einer E-Mail-Adresse oder einer Mobilfunknummer abhängig zu machen. Ich habe in diesem Verfahren gemäß § 12a Unterlassungsklagengesetz (UKlaG) Gelegenheit erhalten, meine datenschutzrechtliche Bewertung abzugeben.

Im Zusammenhang mit den sogenannten Sparpreistickets der Deutschen Bahn lagen mir bereits mehrere Eingaben gegen die Deutsche Bahn vor. Ursprüng-

lich bestand beim Kauf von Sparpreistickets ein ausnahmsloser Zwang zur Angabe von Namen sowie einer E-Mail-Adresse oder Mobilfunknummer zur anschließenden Verarbeitung dieser Daten in den IT-Systemen der Verantwortlichen. Vor dem Hintergrund der damit verbundenen digitalen Zugangshürden war dieses Vorgehen aus datenschutzrechtlicher Sicht unzulässig und mit den Grundsätzen der DS-GVO nicht vereinbar. Infolge meines Tätigwerdens änderte die Deutsche Bahn zum Fahrplanwechsel am 15. Dezember 2024 ihre Bedingungen für den Erwerb von Sparpreistickets. Seitdem ist der Ticketerwerb nicht mehr zwingend an die Angabe einer E-Mail-Adresse oder einer Mobilfunknummer gebunden. Kundinnen und Kunden haben seither die Möglichkeit, Sparpreistickets am Schalter in ausgedruckter Form zu erhalten, ohne entsprechende Kontaktdaten angeben zu müssen.

Auch im Rahmen des Unterlassungsklageverfahrens erläuterte ich, dass das bis zum 15. Dezember 2024 praktizierte Verfahren zur Ausgabe von Sparpreistickets mehrere Grundsätze der Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DS-GVO verletzt. Die Verarbeitung von Namen sowie E-Mail-Adressen oder Mobilfunknummern war aus meiner Sicht nicht durch einen Erlaubnistatbestand des Art. 6 Abs. 1 DS-GVO gedeckt und damit rechtswidrig. Darüber hinaus entsprach eine solche Ausgestaltung des Ticketvertriebs nicht den Anforderungen an eine datenschutzgerechte Systemgestaltung nach Art. 25 Abs. 1 DS-GVO.

Im Ergebnis habe ich erläutert, dass digitale Zugangsvoraussetzungen nur dann mit den datenschutzrechtlichen Vorgaben der DS-GVO vereinbar sind, wenn sie keinen faktischen Zwang zur Preisgabe personenbezogener Daten begründen. Ein solcher Zwang liegt insbesondere dann vor, wenn betroffene Personen vor die Wahl gestellt werden, entweder personenbezogene Daten offenzulegen oder auf eine Leistung zu verzichten, die für die wirtschaftliche, soziale oder kulturelle Teilhabe von Bedeutung ist. Gerade im Bereich der Daseinsvorsorge ist sicherzustellen, dass eine zumutbare und gleichwertige Alternative zum digitalen Zugang besteht, die den Bezug der jeweiligen Leistung ohne die erzwungene Preisgabe personenbezogener Daten ermöglicht.

In dem Unterlassungsklageverfahren entschied das Oberlandesgericht Frankfurt am Main, dass die zwingende Forderung nach einer E-Mail-Adresse oder Handynummer bei dem Erwerb von „Spar-“ und „Super-Sparpreistickets“ rechtswidrig ist. Nach Auffassung des Gerichts besteht für eine solche Datenverarbeitung keine Rechtsgrundlage. Die Entscheidung ist unanfechtbar.

Güterichterverfahren

Erstmals nahm ich an einem Güterichterverfahren teil. Gesetzlich besteht die Möglichkeit, ein Verwaltungsstreitverfahren mit Einverständnis der Beteiligten für einen Güteversuch an speziell geschulte Güterichterinnen oder Güterichter zu verweisen. Diese unterstützen durch mediationsorientierte Methoden eine einvernehmliche Lösung. Das vertrauliche und strukturierte Verfahren bietet Raum, in festgefahrenen Konflikten Lösungen innerhalb des rechtlichen Rahmens zu entwickeln.

Dem hiesigen Verfahren lag eine Klage eines Unternehmens gegen meinen Bescheid zugrunde, mit dem ich die Verantwortliche angewiesen hatte, ihrer Benachrichtigungspflicht nach Art. 34 DS-GVO auf eine bestimmte Art und Weise nachzukommen. In dem Güteverfahren konnten zentrale Streitpunkte offen erörtert und Unklarheiten weitgehend ausgeräumt werden, ohne an die formalen Vorgaben eines Gerichtsverfahrens gebunden zu sein. Dabei hat sich gezeigt, dass eine Mediation nur dann erfolgreich sein kann, wenn alle Beteiligten zu einem konstruktiven Austausch bereit sind. Fehlt diese Bereitschaft, stößt das Verfahren schnell an Grenzen.

Auch wenn der Spielraum für Kompromisse durch das datenschutzrechtliche Regelwerk begrenzt ist, sehe ich in Güterichterverfahren auch künftig ein wertvolles ergänzendes Instrument. In geeigneten Konstellationen können sie dazu beitragen, Unklarheiten zu beseitigen und eine konsensuale Lösung zu erreichen, ohne die eigene Rechtsauffassung aufgeben zu müssen. Dies kann nicht nur zu einer Verfahrensbeschleunigung führen, sondern auch dazu beitragen, die Rechte betroffener Personen schneller durchzusetzen. Gleichwohl ist dieses Format nicht für alle Verwaltungsstreitverfahren geeignet, da eine Mediation eine gerichtliche Klärung grundlegender Rechtsfragen nicht ersetzen kann.

Verwaltungsstreitverfahren zum Thema Auskunft und Bonitätsscore

Das Urteil des Verwaltungsgerichts Wiesbaden vom 19. November 2025 (6 K 788/20.WI) zu den Voraussetzungen des Auskunftsanspruchs nach Art. 15 Abs. 1 Buchst. h DS-GVO markiert einen weiteren, wenn auch nicht abschließenden Schritt in einem seit mehreren Jahren anhängigen Gerichtsverfahren. Dieses Verfahren hatte zwischenzeitlich auch den EuGH in der Rechtssache C-634/21 beschäftigt (s. 52. Tätigkeitsbericht 2023, Kap. 1.1, S. 5 f. und Kap. 3.1, 30 f.). Im Mittelpunkt des Rechtsstreits stand unter anderem die Frage, ob und in welchem Umfang die Klägerin einen Anspruch nach Art. 15 Abs. 1 Buchst. h DS-GVO gegen die SCHUFA Holding AG (SCHUFA) auf Informationen über die Erstellung eines Bonitätsscores geltend machen kann.

Das Verwaltungsgericht Wiesbaden machte die Reichweite des Auskunftsanspruchs aus Art. 15 Abs. 1 Buchst. h DS-GVO maßgeblich davon abhängig, ob die Erstellung des Bonitätsscores als automatisierte Entscheidung im Einzelfall im Sinne von Art. 22 Abs. 1 DS-GVO zu qualifizieren sei, und legte diese Frage seinerzeit dem EuGH zur Vorabentscheidung vor. Der EuGH entschied mit Urteil vom 7. Dezember 2023, „dass eine ‚automatisierte Entscheidung im Einzelfall' im Sinne dieser Bestimmung vorliegt, wenn ein auf personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei automatisiert erstellt wird, sofern von diesem Wahrscheinlichkeitswert maßgeblich abhängt, ob ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet" (Rechtssache C-634/21, Rn. 73).

Mit Urteil vom 19. November 2025 verpflichtete das Verwaltungsgericht Wiesbaden mich nun, gegenüber der SCHUFA aufsichtsrechtlich einzuschreiten, um im konkreten Fall die Erfüllung der datenschutzrechtlichen Auskunftspflichten durchzusetzen. Das Gericht stellte fest, dass die Erstellung des streitgegenständlichen Scorewerts eine ausschließlich automatisierte Verarbeitung darstellt, so dass die Klägerin auf Grundlage von Art. 15 Abs. 1 Buchst. h DS-GVO aussagekräftige Informationen über die involvierte Logik sowie über die Tragweite und die angestrebten Auswirkungen der Verarbeitung verlangen kann. Unter Bezugnahme auf das Urteil des EuGH vom 27. Februar 2025 (Rechtssache C-203/22) betonte das Gericht, dass diese Informationen präzise, transparent, verständlich und in leicht zugänglicher Form sowie in klarer und einfacher Sprache bereitzustellen sind. Zugleich stellte das Verwaltungsgericht klar, dass die SCHUFA nicht verpflichtet ist, den zugrundeliegenden Algorithmus offenzulegen. Die Auskunftei müsse die bei der konkreten Scoreermittlung angewandten Verfahren und Grundsätze so erläutern, dass für die betroffene Person nachvollziehbar wird, welche personenbezogenen Daten in welcher Weise in die Bewertung eingeflossen sind.

Nach Auffassung des Gerichts genügte die von der SCHUFA erteilte Auskunft diesen Vorgaben nicht. Die Kammer verpflichtete mich daher, gegenüber der SCHUFA aufsichtsrechtlich tätig zu werden, wobei die Auswahl des konkreten aufsichtsrechtlichen Mittels in mein Ermessen gestellt wurde.

Das Urteil ist nicht rechtskräftig.

Untersuchungsumfang der Datenschutzaufsichtsbehörden

Das Verwaltungsgericht Wiesbaden befasste sich in mehreren Verfahren mit dem mir bei der Bearbeitung von Beschwerden nach Art. 77 DS-GVO eingeräumten Ermessen. In seinen Urteilen schärfte das Gericht unter

Verweis auf die europäische Rechtsprechung die Anforderungen an das aufsichtsbehördliche Ermessen und konkretisierte die dabei zu berücksichtigenden Gesichtspunkte.

Nach Art. 57 Abs. 1 Buchst. a DS-GVO obliegt es jeder Aufsichtsbehörde, die Anwendung der DS-GVO zu überwachen und durchzusetzen. Zudem ist sie nach Art. 57 Abs. 1 Buchst. f DS-GVO verpflichtet, sich mit Beschwerden betroffener Personen zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführenden innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten.

Dabei sind die Beschwerden mit der gebotenen Sorgfalt zu bearbeiten (EuGH Urteil vom 7. Dezember 2023, Rechtssache C-26/22, Rn. 56; EuGH Urteil vom 16. Juli 2020, Rechtssache C-311/18, Rn. 109). Zwar verleiht Art. 58 Abs. 1 DS-GVO den Aufsichtsbehörden umfassende Untersuchungsbefugnisse, die Verordnung legt jedoch nicht fest, wie weit diese Ermittlungen im Einzelnen reichen müssen. Über den Umfang der Untersuchung entscheidet die Aufsichtsbehörde nach pflichtgemäßem Ermessen unter Berücksichtigung der konkreten Umstände des Einzelfalls. Hierbei sind vor allem die Bedeutung des Vorgangs und die Schwere eines etwaigen Rechtsverstoßes maßgeblich. Kommt die Aufsichtsbehörde nach Abschluss ihrer Ermittlungen zu dem Ergebnis, dass ein Datenschutzverstoß gegeben ist, hat sie grundsätzlich Abhilfemaßnahmen zu treffen. Sie ist dann verpflichtet, in geeigneter Weise zu reagieren, um der festgestellten Unzulänglichkeit abzuhelfen (EuGH Urteil vom 26. September 2024, Rechtssache C-768/21 Rn. 33; EuGH Urteil vom 7. Dezember 2023, Rechtssache C-26/22 und C-64/22, Rn. 57 m. w. N.).

Art. 58 Abs. 2 DS-GVO stellt hierfür einen Katalog möglicher Maßnahmen zur Verfügung. Innerhalb dieses Rahmens entscheidet die Behörde ebenfalls nach pflichtgemäßem Ermessen, ob ein milderes Mittel genügt oder ob eine intensivere Maßnahme erforderlich ist. Eine feste Reihenfolge der vorgesehenen Befugnisse besteht dabei nicht. Hinsichtlich der Auswahl und Anwendung der Abhilfebefugnisse steht der Behörde somit ein Ermessen zu, das nach § 114 Abs. 1 VwGO gerichtlich dahingehend überprüft wird, ob die gesetzlichen Ermessensgrenzen eingehalten wurden.

In diesem Zusammenhang ist zudem zu berücksichtigen, dass sowohl Art. 57 Abs. 1 Buchst. a und f DS-GVO als auch Art. 58 Abs. 1 und 2 DS-GVO betroffenen Personen kein subjektives Recht auf ein bestimmtes Einschreiten der Aufsichtsbehörde vermitteln. Klägerinnen und Klägern steht daher in der Regel nur ein Anspruch auf ermessensfehlerfreie Behandlung der Beschwerde zu, nicht auf den Erlass einer bestimmten Maßnahme.

Die dargestellte Rechtsprechung verdeutlicht, dass der Umfang der Untersuchungs- und Abhilfetätigkeit der Datenschutzaufsichtsbehörden maßgeblich durch ein pflichtgemäß auszuübendes Ermessen bestimmt wird. Maßgeblich sind dabei insbesondere die Bedeutung des konkreten Vorgangs und die Schwere eines möglichen Datenschutzverstoßes. Die Aufsichtsbehörde ist verpflichtet, Beschwerden sorgfältig zu prüfen, den Sachverhalt angemessen aufzuklären und das Ergebnis mitzuteilen. Zugleich vermittelt die DS-GVO den betroffenen Personen regelmäßig keinen Anspruch auf ein bestimmtes aufsichtsbehördliches Einschreiten, sondern lediglich auf eine ermessensfehlerfreie Behandlung ihrer Beschwerde. Die gerichtliche Kontrolle beschränkt sich entsprechend auf die Einhaltung der gesetzlichen Ermessensgrenzen.

Missbräuchliche Inanspruchnahme

Eine wiederkehrende Herausforderung ist der Umgang mit betroffenen Personen, die eine außergewöhnlich hohe Zahl von Beschwerden einreichen. Teilweise treten diese Personen infolge der Vielzahl vorausgegangener Aufsichtsverfahren auch gehäuft als Klägerinnen oder Kläger vor dem Verwaltungsgericht Wiesbaden auf (s. bereits 53. Tätigkeitsbericht, Kap. 3.1, S. 25 ff.). Beispielsweise war ich im Berichtszeitraum als Beklagter in insgesamt sieben Gerichtsverfahren ein und desselben Klägers involviert.

Besonders der Vortrag von Vielklägern oder Beschwerdeführenden mit hoher Eingabefrequenz enthält regelmäßig Anhaltspunkte dafür, dass nicht primär der Schutz der eigenen personenbezogenen Daten verfolgt wird. Vor diesem Hintergrund stellt sich sowohl in Gerichts- als auch in Aufsichtsverfahren regelmäßig die Frage, ob ein rechtsmissbräuchliches Vorgehen gegeben ist.

Nach der Rechtsprechung des EuGH zu Art. 57 Abs. 4 DS-GVO in der Rechtssache C-416/23 kann die bloße Anzahl eingeleiteter Verfahren für sich genommen noch kein exzessives oder rechtsmissbräuchliches Verhalten begründen. Gleichwohl sieht der EuGH eine Missbrauchsabsicht, „wenn eine Person Beschwerden einreicht, ohne dass dies objektiv erforderlich ist, um ihre Rechte aus der Verordnung zu schützen“ (Rn. 50). Über diese Entscheidung wurde bereits im letzten Tätigkeitsbericht ausführlich berichtet (vgl. 53. Tätigkeitsbericht, Kap. 1.3, S. 7 f.). Das Urteil fügt sich in die gefestigte Rechtsprechung des EuGH ein, wonach sich niemand betrügerisch oder missbräuchlich auf das Unionsrecht berufen kann (vgl. Rechtssache C-116/16, Rn. 70).

Nach dieser Maßgabe werde ich auch weiterhin Eingaben danach untersuchen, ob konkrete Anhaltspunkte dafür bestehen, dass das jeweilige Vorgehen dem Schutz personenbezogener Daten dient und zur Wahrnehmung der Rechte aus der DS-GVO objektiv erforderlich ist. Wird ein rechtsmissbräuchliches

Verhalten festgestellt, werde ich die Bearbeitung des Anliegens zurückstellen. Auf diese Weise wird sichergestellt, dass die vorhandenen Arbeitskapazitäten meiner Behörde zielgerichtet eingesetzt und nicht durch missbräuchliche Inanspruchnahmen gebunden werden.

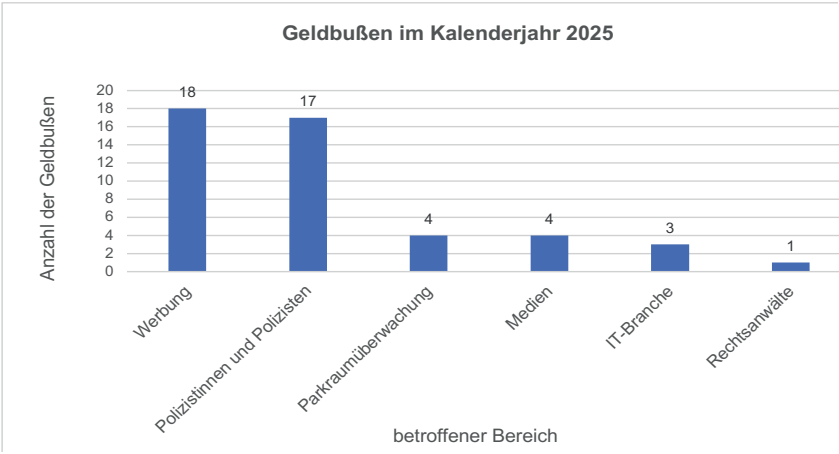
3.2
Verfahren über die Verhängung von Geldbußen

Die Bandbreite der im Jahr 2025 geprüften Geldbußenverfahren zeigt deutlich, dass Datenschutzverstöße, die die Verhängung einer Geldbuße im Einzelfall erforderlich machen, alle Akteure der Datenverarbeitung unabhängig von Branche und Tätigkeit treffen können. Schwerpunkte der Tätigkeit meiner Sanktionsstelle bildeten im Berichtsjahr insbesondere Verstöße im Zusammenhang mit unrechtmäßiger Werbung, der Verletzung der Kooperationspflicht sowie Mitarbeiterexzesse durch Angehörige der hessischen Polizei. Darüber hinaus verhängte ich zum ersten Mal Geldbußen gegen Auftragsverarbeiter, Parkraumüberwachungsunternehmen sowie einen Rechtsanwalt.

Geldbußenverfahren in Zahlen

Im Berichtsjahr leitete ich 48 Geldbußenverfahren ein. Damit stieg die Zahl der neuen Fälle im Vergleich zum vergangenen Jahr leicht an. Mit insgesamt 47 verhängten einzelnen Geldbußen entspricht die Anzahl derjenigen aus dem Vorjahr. Das Gesamtvolumen der festgesetzten Geldbußen belief sich im Berichtsjahr auf einen Betrag von 190.100 €. Der Großteil der erlassenen Geldbußenbescheide ist bereits rechtskräftig.

Das nachfolgend abgebildete Diagramm veranschaulicht, auf welche Bereiche sich die verhängten Geldbußen verteilen.



Verstöße im Zusammenhang mit Werbung

Bereits in meinem 53. Tätigkeitsbericht 2024 informierte ich über Verstöße im Zusammenhang mit unrechtmäßiger Werbung (s. 53. Tätigkeitsbericht 2024, Kap. 3.2, S. 29 f.). Auch im Berichtszeitraum 2025 war dies Gegenstand mehrerer Geldbußenverfahren. So standen insbesondere Verstöße wegen Verarbeitung personenbezogener Daten zu Zwecken der Direktwerbung ohne Rechtsgrundlage und die Nichtberücksichtigung von Werbewidersprüchen betroffener Personen erneut im Fokus.

In einem Verfahren gegen ein Unternehmen aus der Kreuzfahrt- und Tourismusbranche machte ein Beschwerdeführer Gebrauch von seinem Widerspruchsrecht aus Art. 21 Abs. 2 DS-GVO und forderte das Unternehmen auf, künftig keine Werbeansprachen mehr an ihn zu versenden. Über die auf den Antrag des Beschwerdeführers ergriffenen Maßnahmen hätte das Unternehmen den Beschwerdeführer nach Art. 12 Abs. 3 Satz 1 DS-GVO unverzüglich, in jedem Falle aber innerhalb eines Monats nach dem Widerspruch informieren müssen. Eine solche Rückmeldung unterblieb jedoch, weshalb ich diesen Verstoß mit einer Geldbuße in Höhe von 5.000 € sanktionierte.

In demselben Verfahren kam hinzu, dass das Unternehmen über 5.000 weitere Personen kontaktiert hatte, obwohl diese zuvor der Zusendung von Werbung widersprochen hatten. Darin war die Nichteinhaltung des durch Art. 21 Abs. 3 DS-GVO angeordneten Verarbeitungsverbots zu Zwecken der Direktwerbung zu sehen. Die Ursache lag in einem technischen Fehler bei

der Pflege der Kundendaten. Im Rahmen eines internen Prozesses wurden zusätzliche Datensätze angelegt, in denen bestehende Werbewidersprüche nicht übernommen wurden. Wegen dieses Verstoßes verhängte ich eine Geldbuße in Höhe von 70.000 € gegen das Unternehmen.

Bei der Zumessung der Geldbußen berücksichtigte ich die Leitlinien des EDSA für die Berechnung von Geldbußen sowie die Rechtsprechung des EuGH zum Begriff des Unternehmens im Sinne des Art. 83 DS-GVO (vgl. EuGH Urteil vom 5. Dezember 2023, C807/21; EuGH Urteil vom 13. Februar 2025, C-383/23). Zugunsten des Unternehmens fiel insbesondere ins Gewicht, dass das Unternehmen bislang keine einschlägigen Verstöße begangen hatte, die Sachverhaltsaufklärung durchgehend kooperativ unterstützte und die Verstöße offen einräumte. Der erlassene Geldbußenbescheid ist rechtskräftig.

Verstöße aus dem Polizeibereich

Datenschutzverstöße im Polizeibereich betreffen häufig unberechtigte Abfragen in polizeilichen oder der Polizei zur Verfügung stehenden Informationssystemen zu außerdienstlichen Zwecken. Im Berichtszeitraum verhängte ich insgesamt 17 Geldbußen gegen Beamtinnen und Beamte der hessischen Polizei.

Hervorheben möchte ich einen Fall, an dem mehrere Polizistinnen und Polizisten beteiligt waren. In diesem hatte die Polizei einen Mann vorübergehend festgenommen und in einer Gewahrsamszelle untergebracht. Während seines Aufenthalts in der Gewahrsamszelle nahm eine fest installierte Überwachungskamera eine Situation auf, in der der Mann sexuelle Handlungen an sich selbst vornahm. Die Aufnahmen wurden live auf einen Kontrollmonitor übertragen. Drei Polizeibeamtinnen und -beamte fertigten mit ihren Smartphones Fotos von diesem Bildschirm. Die Aufnahmen dienten ausschließlich privaten Zwecken. Eine Beamtin leitete das Bild zudem an eine Kollegin weiter, die es anschließend in einer WhatsApp-Gruppe teilte. Auf diese Weise war das Foto für mindestens neun Personen einsehbar.

Durch das Anfertigen der Bilder wurden besonders schützenswerte personenbezogene Daten im Sinne des Art. 9 Abs. 1 DS-GVO verarbeitet. Diese Verarbeitungen verletzten den Grundsatz der Zweckbindung (Art. 5 Abs. 1 Buchst. b DS-GVO) sowie den Grundsatz der Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 Buchst. a DS-GVO). Die Übermittlung und Weiterleitung des Fotos über WhatsApp stellten für sich gesehen jeweils weitere Verstöße gegen den Grundsatz der Rechtmäßigkeit dar.

Für die Verstöße verhängte ich Geldbußen zwischen 800 € und 1.500 €. Bei der Bemessung berücksichtigte ich erschwerend, dass ein Datum zum

Sexualleben des betroffenen Mannes rechtswidrig verarbeitet wurde. Demgegenüber wirkte sich teilweise mildernd aus, dass die Tat eingeräumt wurde.

Verstöße gegen die Kooperationspflicht

Der bereits in den letzten beiden Berichtsjahren (s. 52. Tätigkeitsbericht 2023, Kap. 3.2, S. 37 ff; 53. Tätigkeitsbericht 2024, Kap. 3.2, S. 30 f.) beobachtete Trend zunehmender Verstöße gegen die Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde aus Art. 31 DS-GVO setzte sich auch in diesem Jahr fort.

Ein besonders aussagekräftiger Fall betraf ein Unternehmen aus der Immobilienbranche, gegen das zahlreiche Vorwürfe in mehreren Beschwerden eingegangen waren. Das Unternehmen versendete an mehrere Personen werbliche E-Mails, ohne dies auf einen Erlaubnistatbestand aus Art. 6 Abs. 1 UAbs. 1 DS-GVO stützen zu können. Zudem kam das Unternehmen seinen Pflichten im Zusammenhang mit Betroffenenrechten, insbesondere dem Auskunftsrecht, nicht nach. Auf meine Anfragen reagierte das Unternehmen auch nach Androhung und anschließender Festsetzung von Zwangsgeldern über einen Zeitraum von mehr als einem Jahr nicht. In drei von insgesamt acht Beschwerdeverfahren, die in ein Geldbußenverfahren mündeten, sanktionierte ich deshalb Verstöße gegen Art. 31 DS-GVO und setzte Geldbußen in Höhe von jeweils 2.000 € fest.

Ein weiteres Geldbußenverfahren betraf ein Unternehmen aus der Modebranche. Das Unternehmen hatte ich aufgefordert, zu möglichen Verstößen gegen Art. 21 Abs. 3 DS-GVO sowie Art. 15 Abs. 1 in Verbindung mit Art. 12 Abs. 3 DS-GVO Stellung zu nehmen. Wegen der weiteren Verwendung personenbezogener Daten eines Beschwerdeführers untersagte ich dem Unternehmen die weitere Verarbeitung derselben zu werblichen Zwecken. Ferner wies ich die verantwortliche Stelle an, eine zuvor von der betroffenen Person beantragte Auskunft zu erteilen. Für den Fall, dass dem nicht nachgekommen werden sollte, drohte ich jeweils die Verhängung eines Zwangsgeldes an. Auch hier blieb eine Reaktion zunächst aus, so dass ich die Zwangsgelder festsetzte. Erst danach nahm das Unternehmen Kontakt zu mir auf. So verstrichen zwischen meiner ersten Anfrage und der tatsächlichen Zusammenarbeit mehr als fünf Monate. Das unkooperative Verhalten führte zu einer Geldbuße in Höhe von 10.000 €.

In einem weiteren Verfahren befasste ich mich mit einem Unternehmen, das unter anderem eine Plattform zum Vergleich von ärztlichen und zahnärztlichen Dienstleistungen im Internet anbietet. Anlass war eine Beschwerde im Zusammenhang mit einer Auskunft nach Art. 15 DS-GVO. Im Rahmen der Sachverhaltsermittlung ergab sich weiterer Klärungsbedarf, etwa zur Erfor-

derlichkeit der Verarbeitung bestimmter Daten zur ärztlichen Einschätzung von Behandlungsgesuchen bzw. zur Erstellung von Therapieplanungen.

Die anschließenden Ermittlungen wurden durch verspätete, unklare und unvollständige Antworten erheblich erschwert. Obwohl dem Unternehmen ausnahmsweise eine dreimonatige Fristverlängerung eingeräumt worden war, blieb auch diese ungenutzt. Erst nach erneuter Intervention und dem Hinweis auf einen möglichen Verstoß gegen die Kooperationspflicht wurden die erforderlichen Informationen übermittelt. Nach wenigen Anpassungen der Datenerhebungsformulare durch den Verantwortlichen schloss ich das Aufsichtsverfahren ab. Wegen des Verstoßes gegen die Mitwirkungspflicht setzte ich eine Geldbuße in Höhe von 5.000 € fest.

Der Fall verdeutlicht, dass eine Verletzung der Kooperationspflicht des Art. 31 DS-GVO auch dann vorliegen kann, wenn die Beschwerde (größtenteils) erfolglos bleibt und kein ahndungswürdiger Verstoß im Zusammenhang mit Verarbeitungsvorgängen besteht. Unzureichende oder ausbleibende Zusammenarbeit führt regelmäßig zu einer Verzögerung der Verfahren und erschwert die Arbeit der Aufsichtsbehörden erheblich, so dass die Verhängung einer Geldbuße geboten sein kann.

Zusammenfassend möchte ich an dieser Stelle betonen, dass ich Verstöße gegen die allgemeine Kooperationspflicht auch in Zukunft entschieden verfolgen und in angezeigten Fällen durch entsprechende Sanktionen ahnden werde. Ich empfehle und erwarte daher von verantwortlichen Stellen eine zeitnahe, konstruktive Zusammenarbeit mit meiner Behörde, insbesondere durch die vollständige Bereitstellung der relevanten Informationen.

Verstöße im Rahmen der Parkraumüberwachung

Im 53. Tätigkeitsbericht 2024 (Kap. 10.1, S. 145 ff.) hatte ich über zahlreiche Beschwerden und Eingaben gegen ein Unternehmen aus dem Bereich der digitalen Parkraumüberwachung informiert. Damals stand vor allem die Funktionsweise des eingesetzten Systems einschließlich des Einsatzes von Videoüberwachungssystemen im Mittelpunkt. Nach einem sehr arbeits- und zeitintensiven Aufsichtsverfahren konnte ich erreichen, dass das Unternehmen die konkrete Ausgestaltung des Systems nachvollziehbar darlegte und wesentlich anpasste. Wegen der zuvor unzureichenden Zusammenarbeit des Unternehmens mit meiner Behörde leitete ich jedoch ein Geldbußenverfahren ein.

Über einen Zeitraum von ca. 1,5 Jahren hatte das Unternehmen seine Datenverarbeitungen nicht ausreichend erläutert, erforderliche Unterlagen nicht vorgelegt und Anfragen meiner Behörde nur unvollständig beantwortet. Die

Zusammenarbeit war insgesamt von Intransparenz, fehlender Struktur und einer schleppenden, teils widersprüchlichen Kommunikation geprägt. Dieses Verhalten ging mit einer Zäsur der Ermittlungen und erheblichen Verzögerungen des Prüfverfahrens einher. Den Verstoß sanktionierte ich mit einer Geldbuße in Höhe von 10.000 €.

Darüber hinaus prüfte ich gegen denselben Verantwortlichen sowie ein weiteres Unternehmen aus dem Bereich der digitalen Parkraumüberwachung mehrere Verfahren im Zusammenhang mit der Einhaltung von Rechenschafts- und Dokumentationspflichten. In beiden Fällen wurden vermeintliche Falschparker zur Zahlung von Vertragsstrafen aufgefordert, während die Unternehmen bereits wenige Tage später keine Unterlagen mehr zu den jeweiligen Vorgängen vorlegen konnten. Betroffene Personen, die den Parkverstoß überprüfen wollten und eine Auskunft nach Art. 15 DS-GVO beim Verantwortlichen beantragten, erhielten regelmäßig lediglich eine Negativauskunft. Im Rahmen des Aufsichtsverfahrens stellte sich heraus, dass die Unternehmen, „um guten Datenschutz zu forcieren“, grundsätzlich alle personenbezogenen Daten einschließlich Rechnungen, Zahlungserinnerungen, Korrespondenz zu Datenschutzauskünften und andere Datenspuren gelöscht hatten, sobald die Forderung beglichen oder der Fall aus anderen Gründen nicht weiterverfolgt wurde.

Abgesehen von den zu berücksichtigenden Aufbewahrungspflichten nach Handels- und Steuerrecht verstößt diese Praxis gegen die Rechenschaftspflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO sowie den Grundsatz der Rechtmäßigkeit der Verarbeitung nach Art. 5 Abs. 1 Buchst. a i. V. m. Art. 6 Abs. 1 DS-GVO. Im Ergebnis konnten die Unternehmen weder den Nachweis nach Art. 5 Abs. 2 DS-GVO erbringen noch eine tragfähige Rechtsgrundlage für die vorzeitige Löschung der Daten darlegen. Dieses Vorgehen führte zu intransparenten Datenverarbeitungen und der Vereitelung geltend gemachter Betroffenenrechte. Durch mein Einschreiten wurde eine datenschutzkonforme Lösung eingeführt. Bezüglich der geschilderten Verstöße setzte ich gegen die Unternehmen Geldbußen in Höhe von 7.000 € und 5.000 € fest.

Erste Geldbußen gegen Auftragsverarbeiter

Im Berichtsjahr bearbeitete ich mehrere Geldbußenverfahren wegen Verstößen gegen die Sicherheit der Verarbeitung personenbezogener Daten (Art. 32 Abs. 1 DS-GVO). Zwei Verfahren schloss ich jeweils mit Erlass eines Bescheids über die Verhängung von Geldbußen ab. Hervorzuheben ist, dass es sich hierbei um erste Geldbußen handelt, die ich gegen Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DS-GVO verhängt habe.

Ein Verfahren betraf ein Unternehmen, das Apps und Online-Dienstleistungen für den Gastronomiebereich anbietet. Es stellt unter anderem einen Online-Dienst zur Verfügung, über den Gastronomiebetriebe Bestellungen abwickeln können. Nutzerinnen und Nutzer des Dienstes haben dort die Möglichkeit, ihre Bestellhistorie über einen Webbrowser einzusehen.

Durch eine einfache Veränderung der in der URL enthaltenen Kennung konnten mit gängigen Entwickler-Tools eines beliebigen Browsers personenbezogene Daten von Kundinnen und Kunden eingesehen werden (s. hierzu Kap. 13.7). Diese Daten hätten ausschließlich für die jeweils bestellende Person zugänglich sein dürfen. Erforderliche technische Schutzmaßnahmen waren nicht implementiert.

Der Vorfall führte zu einer unbefugten Offenlegung von und zu unbefugtem Zugang zu personenbezogenen Daten und stellte zugleich eine nach Art. 33 Abs. 2 DS-GVO meldepflichtige Verletzung des Schutzes personenbezogener Daten dar. Der Meldepflicht kam das Unternehmen nicht vollumfänglich nach. Wegen der Verstöße verhängte ich zwei Geldbußen in Höhe von jeweils 10.000 €. Der Geldbußenbescheid ist inzwischen rechtskräftig.

Darüber hinaus konnte ich ein älteres Verfahren gegen ein Unternehmen aus der IT-Branche abschließen, das als Unterauftragsverarbeiter für einen Laborbetreiber tätig war. Dieser bot eine Online-Lösung zum Abruf von Testergebnissen für Corona-Testzentren an. Aufgrund einer Sicherheitslücke war der Zugriff auf einzelne Testergebnisse teilweise ohne Passwortschutz möglich. Potenzielle Angreifer konnten die Daten mit marginalem Aufwand einsehen, kopieren oder missbrauchen. Einzelne unautorisierte Zugriffe wurden festgestellt. Im Aufsichtsverfahren wirkte ich erfolgreich auf die Fehlerbehebung und die Implementierung eines Schutzes beim Abruf der Tests durch die Abfrage eines geeigneten Passwortes hin.

Die unzureichenden Schutzmaßnahmen stellten einen Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 Buchst. f DS-GVO sowie gegen die Pflichten des Auftragsverarbeiters nach Art. 32 Abs. 1 Buchst. b DS-GVO dar. Diesen Verstoß ahndete ich mit einer Geldbuße weit im unteren Bereich des Geldbußenrahmens in Höhe von 3.000 €. Dies resultierte insbesondere daraus, dass es sich bei dem Unterauftragsverarbeiter um ein Kleinstunternehmen mit geringem Umsatz handelte. Entlastend berücksichtigte ich in erheblichem Maße, dass sich das Unternehmen kooperativ und lösungsorientiert verhielt. Zu Lasten des Unternehmens wog dagegen, dass unter anderem besonders schützenswerte Gesundheitsdaten betroffen waren.

Erste Geldbuße gegen einen Rechtsanwalt

In vergangenen Jahren berichtete ich regelmäßig über die Verhängung von Geldbußen gegen Ärztinnen und Ärzte (s. 52. Tätigkeitsbericht 2023, Kap. 3.3, S. 34 f.; 53. Tätigkeitsbericht 2024, Kap. 3.2, S. 27 ff.). Im Berichtsjahr stellte ich nun erstmals einen sanktionswürdigen Verstoß durch einen Berufsgeheimnisträger aus dem Bereich der Rechtspflege fest und erließ erstmalig einen Geldbußenbescheid gegen einen Rechtsanwalt.

Ein Strafverteidiger lud auf seinem öffentlich zugänglichen Instagram-Account ein knapp 30-sekündiges Video hoch, in welchem er einen Aktenordner mit strafrechtlichen Unterlagen durchblätterte und damit die Erfolge seiner Kanzlei bewarb. Die gezeigten Dokumente waren nicht geschwärzt, so dass beim Heranzoomen des Videomaterials personenbezogene Daten von mindestens 20 Personen lesbar waren. Erkennbar waren unter anderem Namen, Anschriften, Geburtsdaten und Staatsangehörigkeit der Mandanten sowie Tatvorwürfe und teilweise verhängte Strafen. In Einzelfällen bestand auch ein Bezug zum Jugendstrafrecht. Das Video wurde über 1.400-mal aufgerufen (s. hierzu auch Kap. 4.6).

Mit der Veröffentlichung des Videos offenbarte der Rechtsanwalt die teils sensiblen personenbezogenen Daten mehrerer Personen einem großen Adressatenkreis und verletzte dadurch insbesondere den Grundsatz der Rechtmäßigkeit aus Art. 5 Abs. 1 Buchst. a DS-GVO i. V. m. Art. 6 Abs. 1 DS-GVO und Art. 10 DS-GVO. Den Verstoß ahndete ich mit einer Geldbuße in Höhe von 4.000 €.

Bei der Bemessung der Geldbuße berücksichtigte ich unter anderem die Dauer des Verstoßes von ca. 35 Tagen, die Anzahl der von der Verarbeitung betroffenen Personen und die hohe Sensitivität der offengelegten Daten. Mildernd wertete ich, dass keine einschlägigen früheren Verstöße des Rechtsanwalts bekannt waren, dieser den Verstoß eingeräumt, Reue gezeigt und mit mir kooperativ zusammengearbeitet hat. Erschwerend fiel ins Gewicht, dass besonders schützenswerte Daten mit strafrechtlichem Bezug betroffen waren und der Umgang mit solchen Informationen zur Kerntätigkeit der Kanzlei gehört. Zudem stehen die hier verletzten Datenschutzvorschriften in einem engen inhaltlichen Zusammenhang mit den Regelungen über die anwaltliche Verschwiegenheitspflicht aus § 43a Abs. 2 Satz 1 BRAO i. V. m. § 2 Abs. 1 BORA. Diese gehören zu den Grundpflichten eines jeden Rechtsanwalts und waren dem Verantwortlichen aufgrund seiner Stellung als Berufsgeheimnisträger umfassend bekannt.

4. Polizei, Verfassungsschutz und Justiz

Polizei und Verfassungsschutz haben weitreichende Befugnisse zur Verarbeitung personenbezogener Daten, die zu tiefen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen führen können. Diese Befugnisse sind jedoch immer an einschränkende gesetzliche Voraussetzungen gebunden. Zum Schutz des Grundrechts auf informationelle Selbstbestimmung ist es daher wichtig, dass diese Befugnisse, ihre Voraussetzungen und ihre Grenzen verhältnismäßig sind und im Alltag eingehalten werden. Ihre gesetzliche Festlegung war Gegenstand meiner Stellungnahme im Gesetzgebungsverfahren zur Änderung des Hessischen Verfassungsschutzgesetzes (Kap. 4.1). Ihre Einhaltung war Gegenstand einer Prüfung einer Staatsanwaltschaft (Kap. 4.2) und von Datenschutzkontrollen bei Polizeibehörden und Verfassungsschutz (Kap. 4.3). Die Funktion in Polizei-Smartphones dient tatsächlich nur dem arbeitserleichternden Scannen von Ausweisdokumenten (Kap. 4.4). In die Erprobung der biometrischen Echtzeit-Fernidentifizierung in Frankfurt bin ich beratend eingebunden (Kap. 4.5). Ein Anwalt, der zur Werbung für seine Kanzlei auf einem anwaltlichen Instagram-Profil Strafakten von Mandanten zeigte, musste sanktioniert werden (Kap. 4.6).

4.1 Gesetzgebungsverfahren zur Änderung des Hessischen Verfassungsschutzgesetzes

Im Berichtsjahr hat der hessische Gesetzgeber das Hessische Verfassungsschutzgesetz (HVSG) novelliert. Mit Beschluss 1 BvR 2133/22 vom 17. Juli 2024 hatte das Bundesverfassungsgericht das bisherige HVSG für teilweise verfassungswidrig erklärt. Die Entscheidung habe ich bereits in meinem 53. Tätigkeitsbericht ausführlich dargestellt. Der diesjährige Beitrag gibt einen Überblick über das Gesetzgebungsverfahren zur aktuellen Novellierung, einschließlich der öffentlichen Anhörung und eines anschließenden Änderungsantrages im Innenausschuss des Hessischen Landtags sowie meiner Stellungnahme. Dabei stelle ich meine eingebrachten Kritikpunkte sowie die wesentlichen Änderungen im HVSG unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts kurz dar.

Die Novellierung des HVSG erfolgte aufgrund des im Koalitionsvertrag festgelegten Ziels, den Verfassungsschutz zu stärken. Die Fraktionen der CDU und SPD brachten am 10. Juni 2025 einen Entwurf für ein Gesetz zur Änderung verfassungsrechtlicher Vorschriften zur Umsetzung der Anforde-

rungen des Bundesverfassungsgerichts (LT-Drs. 21/2376) ein sowie am 28. Oktober 2025 einen Änderungsantrag (LT-Drs. 21/2914).

Die Änderungen betreffen die §§ 2, 3, 5, 5a, 7, 7a, 8, 9, 10, 11, 12, 16, 19, 20a, 20b und 28 HVSG und sind am 13.12.2025 in Kraft getreten. Bereits im Rahmen der Ressort- und Verbändebeteiligung sowie in der öffentlichen Anhörung im Innenausschuss des Hessischen Landtags konnte ich zu den Novellierungen ausführlich Stellung nehmen (Ausschussvorlage INA 21/18 öffentlich vom 18. August 2025 Teil 1). Einige meiner Kritikpunkte wurden in dem jeweils folgenden Entwurf aufgegriffen.

Die datenschutzrechtlich relevanten Novellierungen betreffen im Wesentlichen die §§ 7a, 9, 20a und 20b HVSG. Bei der Darstellung der Novellierungen sowie meiner Anmerkungen hierzu beschränke ich mich im Folgenden auf diese Änderungen.

Verdeckter Zugriff auf informationstechnische Systeme, § 7a HVSG

Der neu eingefügte § 7a HVSG regelt die Befugnis zum verdeckten Zugriff auf informationstechnische Systeme (sog. Online-Durchsuchung) auf Basis einer richterlichen Anordnung. Voraussetzung für den verdeckten Zugriff ist, dass eine „konkretisierte Gefahr“ für ein überragend wichtiges Rechtsgut nach § 7 HVSG besteht, beispielsweise für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person.

In meinen Stellungnahmen im Rahmen des Gesetzgebungsverfahrens sowie in der öffentlichen Anhörung habe ich angemerkt, dass der Begriff der „konkretisierten Gefahr“ bisher lediglich durch das Bundesverfassungsgericht in seinem Urteil zum bayerischen Verfassungsschutzgesetz definiert wurde (vgl. Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 176; BVerfGE 141, 220, 272 f., Rn. 112). Eine solche liegt nach dem Bundesverfassungsgericht unter zwei Voraussetzungen vor. Zum einen müssen bestimmte Tatsachen bereits den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen. Zum anderen muss der Schluss möglich sein, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahmen gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden können. Beim Begriff der „konkretisierten Gefahr” handelt es sich jedoch nicht um einen feststehenden Gefahrenbegriff des Gefahrenabwehrrechts. Angesichts der Eingriffstiefe eines verdeckten Zugriffs auf informationstechnische Systeme sollte die „konkretisierte Gefahr“ ähnlich wie im Hessischen Sicherheits- und Ordnungsgesetz (HSOG) direkt im Gesetz definiert werden, um der erforderlichen Normenklarheit und der Anwendungspraxis gerecht zu werden. Dieser Empfehlung ist der Gesetzgeber jedoch nicht gefolgt.

§ 7a HVSG

(1) Das Landesamt darf unter den Voraussetzungen des § 7 Abs. 1 Satz 1 und Abs. 2 Satz 1 und 2 erster Halbsatz mit der Maßgabe, dass eine konkretisierte Gefahr für ein dort genanntes Rechtsgut vorliegt, zur Abwehr dieser Gefahr mit technischen Mitteln verdeckt auf informationstechnische Systeme, welche die Zielperson in der berechtigten Erwartung von Vertraulichkeit als eigene nutzt und die ihrer selbstbestimmten Verfügung unterliegen, nur zugreifen, um

1. *Zugangsdaten und verarbeitete Daten zu erheben oder*
2. *zur Vorbereitung einer Maßnahme nach Nr. 1 spezifische Kennungen sowie den Standort eines informationstechnischen Systems zu ermitteln.*

Die erhobenen Daten dürfen über den Anlass und Zweck hinaus, zu dem sie erhoben wurden, nur zur Abwehr einer Gefahr im Sinne des Satz 1 oder zur Verfolgung einer Straftat, auf Grund derer eine entsprechende Maßnahme nach § 100b der Strafprozessordnung angeordnet werden könnte, weiterverarbeitet werden.

(2) Durch technische Maßnahmen ist sicherzustellen, dass

1. *an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und*
2. *die vorgenommenen Veränderungen bei Beendigung der Maßnahme soweit technisch möglich automatisiert rückgängig gemacht werden.*

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Erhobene Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) § 7 Abs. 1 Satz 2, Abs. 4, Abs. 5 Satz 5 bis 10 und Abs. 6 findet entsprechende Anwendung. Soweit wie informationstechnisch und ermittlungstechnisch möglich, hat die Erhebung von Erkenntnissen im Sinne des § 7 Abs. 4 Satz 1 zu unterbleiben. Der Zugriff auf informationstechnische Systeme anderer ist zulässig, wenn tatsächliche Anhaltspunkte vorliegen, dass

1. *die Zielperson deren informationstechnisches System benutzt oder benutzt hat,*
2. *sich dadurch für die Abwehr der Gefahr relevante Informationen ergeben werden und*
3. *ein Zugriff auf das informationstechnische System der Zielperson allein nicht zur Erforschung des Sachverhalts ausreicht.*

Ortung von Mobilfunkendgeräten nach § 9 HVSG

Die Neuregelung des § 9 Abs. 2 HVSG setzt die Rechtsprechung des Bundesverfassungsgerichts um. Das Gericht hatte die bisherige Norm aufgrund fehlender Eingriffsschwellen für verfassungswidrig erklärt. Insbesondere ermöglichten auch kürzere Zeiträume als die zunächst in § 9 Abs. 2 definierten bei entsprechend enger Taktung die Erstellung eines Bewegungsprofils (vgl. Bundesverfassungsgericht, Beschluss vom 17. Juli 2024, 1 BvR 2133/22, Rn. 146 f.). Auch durch wiederholtes Orten bei zwischenzeitlicher Unterbrechung könne ein zumindest lückenhaftes Bewegungsprofil erstellt werden. Es komme lediglich auf die potenzielle Eignung der erhobenen Daten zur

Profilerstellung an. Nach der Neuregelung ist der Einsatz technischer Mittel, die wiederholt über einen längeren Zeitraum oder in so enger zeitlicher Taktung eingesetzt werden, dass dadurch eine Nachverfolgung der Bewegung des Mobilfunkendgerätes im Raum ermöglicht wird und damit potenzielle Rückschlüsse gezogen werden können, nur noch dann zulässig, soweit es zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit im Einzelfall geboten ist.

Der hessische Gesetzgeber setzt die Anforderungen des Bundesverfassungsgerichts dadurch um, dass § 9 Abs. 2 HVSG abstrakt an die Eignung der erhobenen Daten zur Erstellung eines Bewegungsprofils anknüpft und die hierfür relevanten Kriterien nach dem Bundesverfassungsgericht zur Erfassung einer Persönlichkeit nun unmittelbar im Gesetz geregelt werden.

§ 9 HVSG

(1) Das Landesamt darf im Einzelfall, soweit dies aufgrund tatsächlicher Anhaltspunkte 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) Werden technische Mittel nach Abs. 1 Nr. 2 wiederholt über einen längeren Zeitraum oder in so enger zeitlicher Taktung eingesetzt, dass die dadurch ermöglichte Nachverfolgung der Bewegung des Mobilfunkendgeräts im Raum potenziell Rückschlüsse auf Verhaltensweisen, Routinen, persönliche Neigungen oder Vorlieben der betroffenen Person zulässt, so ist dies nur zulässig, soweit es zur Aufklärung einer erheblich beobachtungsbedürftigen Bestrebung oder Tätigkeit nach § 3 Abs. 2 im Einzelfall geboten ist. (…)

Informationsübermittlung an Strafverfolgungsbehörden, § 20a HVSG

Das Bundesverfassungsgericht hatte an § 20a Satz 1 HVSG kritisiert, dass § 20a Satz 2 Buchst. b und Satz 3 HVSG in der bisherigen Fassung an nicht hinreichend gewichtige Straftaten anknüpfen. Der hessische Gesetzgeber setzt diese Kritik dadurch um, dass er einen umfangreichen Straftatenkatalog einfügt. Bei den darin aufgeführten Straftatbeständen soll es sich um besonders schwere Straftaten handeln. Diese Klarstellung mittels eines Straftatenkatalogs habe ich in meinen Stellungnahmen sowie in der Anhörung mit Blick auf die Normenklarheit und Normenbestimmtheit begrüßt. Durch den Änderungsantrag wurde der Katalog der besonders schweren Straftaten reduziert. Die Streichung erfolgte zur besseren Abgrenzung besonders schwerer Straftaten im Sinne der Rechtsprechung des Bundesverfassungsgerichts. Weiterhin bleibt jedoch bei einigen Straftaten, auf die ich mich in meinen Stellungnahmen bezogen hatte, offen, warum diese Straftatbestände in den nun geltenden Katalog aufgenommen wurden. Nach

den Vorgaben des Bundesverfassungsgerichts muss sich der Umstand der Betroffenheit von Verfassungsschutzgütern bereits aus dem Tatbestand der jeweiligen Strafnorm ergeben. Dies ist nicht bei allen der Fall. Mit Blick auf einzelne Straftatbestände des Katalogs (Nr. 20 – Nichtanzeige geplanter Straftaten gem. § 138 Abs. 1 Nr. 5 und Abs. 2 StGB; Nr. 21 – Mittelbare Falschbeurkundung gem. § 271 Abs. 3 und 4 StGB; Nr. 22 – Vorbereitung der Fälschung von amtlichen Ausweisen gem. § 275 Abs. 2 1. Alt. StGB; Nr. 23 – Verschaffen von falschen amtlichen Ausweisen gem. § 276 Abs. 2 StGB; Nr. 30 – Rechtsbeugung gem. § 339 StGB; Nr. 31 – Falschbeurkundung im Amt gem. § 348 StGB) ist zudem nicht ersichtlich, warum es sich um besonders schwere Straftaten handeln soll. Dies gilt insbesondere dann, wenn es sich um Straftaten handelt, deren Begehung auch mit Geldstrafen sanktioniert werden kannn. In der öffentlichen Anhörung hatte ich erneut angemerkt, dass die Einordnung einiger Straftaten als besonders schwere Straftaten nicht nachvollziehbar ist und die Gesetzesbegründung nicht erkennen lässt, warum diese Straftatbestände in den Katalog aufgenommen wurden.

§ 20a HVSG

(1) 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) oder zu einer besonders schweren Straftat öffentlich aufgefordert (§ 111 des Strafgesetzbuchs) hat, darf das Landesamt mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an die Strafverfolgungsbehörden übermitteln, soweit dies zur Verfolgung der Tat erforderlich ist.

(2) Besonders schwere Straftaten sind solche, die mit einer Höchststrafe von mindestens zehn Jahren Freiheitsstrafe bedroht sind. Besonders schwere Straftaten sind darüber hinaus, wenn sie im Zusammenhang mit der Beteiligung an einer beobachtungsbedürftigen Bestrebung nach § 2 Abs. 2 Nr. 1, 3, 4 oder 5 oder in Ausübung einer beobachtungsbedürftigen Tätigkeit nach § 2 Abs. 2 Nr. 2 begangen werden,

20. Nichtanzeige geplanter Straftaten (§ 138 Abs. 1 Nr. 5 und Abs. 2 des Strafgesetzbuchs),

21. Mittelbare Falschbeurkundung (§ 271 Abs. 3 und 4 des Strafgesetzbuchs),

22. Vorbereitung der Fälschung von amtlichen Ausweisen (§ 275 Abs. 2 erste Alternative des Strafgesetzbuchs), auch in Verbindung mit § 276a des Strafgesetzbuchs,

23. Verschaffen von falschen amtlichen Ausweisen (§ 276 Abs. 2 des Strafgesetzbuchs), auch in Verbindung mit § 276a des Strafgesetzbuchs, (…)

30. Rechtsbeugung (§ 339 des Strafgesetzbuchs),

31. Falschbeurkundung im Amt (§ 348 des Strafgesetzbuchs), (…)

Informationsübermittlung an sonstige inländische öffentliche Stellen, § 20b HVSG

Der Gesetzgeber hat § 20b HVSG um einen Satz erweitert, um die Anforderungen des Bundesverfassungsgerichts umzusetzen: Verfügt die empfangende Stelle bei der Verwendung der mit nachrichtendienstlichen Mitteln ersterhobenen Daten über operative Anschlussbefugnisse, ist die Informationsübermittlung nur zulässig, soweit es zur Abwehr einer wenigstens „konkretisierten Gefahr" für ein Rechtsgut nach § 20 erforderlich ist. Eine operative Befugnis ist die Möglichkeit, gegenüber Einzelnen Maßnahmen erforderlichenfalls auch mit Zwang durchzusetzen. Ich habe erneut angemerkt, dass auch an dieser Stelle – wie bereits zu § 7a HVSG ausgeführt – der Begriff der „konkretisierten Gefahr" definiert werden sollte. Außerdem bleibt mit Blick auf die Gesetzesbegründung offen, welche Behörden – insbesondere in Abgrenzung zu den in den anderen Übermittlungsbefugnissen genannten Behörden – hier konkret gemeint sind. Eine beispielhafte Aufzählung hierfür hatte ich in meinen Stellungnahmen für begrüßenswert erachtet. Meine Anmerkungen hat der Gesetzgeber im Ergebnis nicht aufgegriffen.

§ 20b HVSG

(1) Das Landesamt darf mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an sonstige inländische öffentliche Stellen übermitteln, wenn eine gesetzliche Regelung, die den Schutz eines der in § 20 genannten Rechtsgüter bezweckt, eine Mitwirkung des Landesamts vorsieht und die Datenübermittlung im Einzelfall erforderlich ist

1. *zur Überprüfung der Zuverlässigkeit der betroffenen Person*

a) *im Rahmen eines Erlaubniserteilungsverfahrens auf Ersuchen der überprüfenden Stelle oder*

b) *zur Erfüllung einer gesetzlichen Nachberichtspflicht, wenn dem Landesamt im Nachhinein Informationen bekannt werden, die für die Beurteilung der Zuverlässigkeit der betreffenden Person von Bedeutung sind,*

2. *zur Prüfung der Frage, ob von der betroffenen Person oder Organisation eine Gefährdung der freiheitlichen demokratischen Grundordnung oder der Sicherheit der Bundesrepublik Deutschland ausgeht, oder ob gegen diese Person oder Organisation sonstige Sicherheitsbedenken bestehen,*

a) *auf Ersuchen der überprüfenden Stelle oder*

b) *zur Erfüllung einer gesetzlichen Unterrichtungspflicht, wenn nachträglich sicherheitserhebliche Erkenntnisse über die überprüfte Person bekannt werden.*

(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. Verfügt die empfangende Stelle bei der Verwendung der Daten über operative Anschlussbefugnisse, ist dies nur zulässig, soweit es zur Abwehr einer wenigstens kon-

kretisierten Gefahr für ein Rechtsgut nach § 20 erforderlich ist. Eine operative Anschlussbefugnis ist die Möglichkeit, gegenüber Einzelnen Maßnahmen erforderlichenfalls auch mit Zwang durchzusetzen.

(3) Das Landesamt darf mit nachrichtendienstlichen Mitteln ersterhobene personenbezogene Daten an Vereinsverbotsbehörden im Sinne des § 3 Abs. 2 des Vereinsgesetzes vom 5. August 1964 (BGBl. I S. 593), zuletzt geändert durch Gesetz vom 30. November 2020 (BGBl. I S. 2600), übermitteln, wenn Tatsachen die Annahme rechtfertigen, dass die Informationsübermittlung zur Vorbereitung oder Durchführung einer Maßnahme nach § 3 Abs. 1 Satz 1 des Vereinsgesetzes im Einzelfall erforderlich ist.

4.2
Prüfung einer Staatsanwaltschaft

Im Herbst 2025 habe ich zum vierten Mal eine Datenschutzkontrolle bei einer hessischen Staatsanwaltschaft durchgeführt. Der Schwerpunkt meiner Kontrolle lag hierbei wieder auf der Einhaltung der gesetzlichen Benachrichtigungspflicht gemäß § 101 Abs. 4 Satz 1 Nr. 3, Abs. 1 StPO nach Beendigung einer Telekommunikationsüberwachung nach Anpassung des Formblatts und der Sensibilisierung durch die Generalstaatsanwaltschaft Frankfurt am Main.

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

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 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, Abs. 1 StPO zu benachrichtigen. Eine Zurückstellung der Benachrichtigung ist unter den Voraussetzungen des § 101 Abs. 6 StPO möglich und 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 überwiegende 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.

Aufgrund des vorgefundenen Ergebnisses meiner Kontrolle einer hessischen Staatsanwaltschaft im Jahr 2023 (s. 52. Tätigkeitsbericht zum Datenschutz, Kap. 4.4) nahm die Generalstaatsanwaltschaft eine Anpassung am Vordruckformular für Anträge für verdeckte Maßnahmen vor. Das Formular wurde den hessischen Staatsanwaltschaften mit entsprechenden Hinweisen ab dem vierten Quartal desselben Jahres zur Verfügung gestellt. Dies veranlasste mich, eine weitere hessische Staatsanwaltschaft in diesem Jahr zu kontrollieren.

Für meine Datenschutzkontrolle habe ich zwölf Verfahrensakten aus dem Jahr 2024/2025 angefordert. Alle angeforderten Verfahrensakten betrafen Maßnahmen zur Telekommunikationsüberwachung nach §100a StPO von unterschiedlichen Dezernaten der geprüften Staatsanwaltschaft. Die Verfahrensakten konnten mir für meine Prüfung vollständig bereitgestellt werden.

Im Rahmen der Prüfung habe ich festgestellt, dass alle verdeckten Maßnahmen durch einen richterlichen Beschluss angeordnet waren und die Durchführung der Telekommunikationsüberwachung damit rechtmäßig war. Allerdings gab es Mängel bei der Dokumentation. So konnte beispielsweise nicht nachvollzogen werden, ob die Benachrichtigungen der Beteiligten der überwachten Telekommunikation nach § 101 Abs. 4 Satz 1 Nr. 3, Abs. 1 StPO durch die Staatsanwaltschaft 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 zwei Verfahren wurde die Zurückstellung entgegen der gesetzlichen Anforderungen bereits im Anordnungsbeschluss zur Maßnahme durch das Gericht angeordnet. Für die erstmalige Zurückstellung ist gemäß § 101 Abs. 5 Satz 2 StPO jedoch die Staatsanwaltschaft zuständig.

Durch die erneute Datenschutzkontrolle hat sich gezeigt, dass die Beteiligten der überwachten Telekommunikation nicht im Sinne des § 101 Abs. 4 Satz 1 Nr. 3, Abs. 1 StPO benachrichtigt worden sind oder zumindest eine entsprechende Dokumentierung unterblieben ist. Daraus schließe ich, dass das abgeänderte Formblatt der Generalstaatsanwaltschaft in der Praxis noch nicht ausreichend umgesetzt wird.

Das Ergebnis und die Handlungsbedarfe wurden der Leitung der geprüften Staatsanwaltschaft mitgeteilt. Auch wurde auf das Formblatt der Generalstaats-

anwaltschaft noch einmal hingewiesen. Die Generalstaatsanwaltschaft wurde anschließend über das Ergebnis der Prüfung und die erneut festgestellten Mängel unterrichtet und aufgefordert, die hessischen Staatsanwaltschaften auf das geänderte Formblatt und die Benachrichtigungspflicht nach § 101 Abs. 4 Satz 1 Nr. 3, Abs. 1 StPO noch einmal hinzuweisen.

§ 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.

4.3
Datenschutzkontrollen bei Polizeibehörden und Verfassungsschutz

Datenschutzkontrollen sind in verschiedenen Bereichen für meine Behörde als gesetzliche Pflichten geregelt. Turnusmäßig wurde für das Jahr 2025 die Rechtsextremismus-Datei (RED) geprüft. Begonnen wurde darüber hinaus mit der Datenschutzkontrolle der Analysesoftware hessenDATA beim Innovation Hub der Hessischen Polizei.

Gemäß § 11 Abs. 2 RED-G fand eine Datenschutzkontrolle zu Neuspeicherungen in die RED für den Zeitraum 2023–2024 beim Landesamt für Verfassungsschutz Hessen statt. Bis zur Fertigstellung dieses Tätigkeitsberichts war die Kontrolle noch nicht abgeschlossen. Über das Ergebnis wird im nächsten Jahr berichtet.

§ 2 RED-G

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

1. *Personen,*

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

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

2. *Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie rechtsextremistische Bestrebungen verfolgen und in Verbindung damit zur Gewalt aufrufen, die Anwendung von rechtsextremistisch begründeter Gewalt als Mittel zur Durchsetzung politischer Belange unterstützen, vorbereiten oder durch ihre Tätigkeiten vorsätzlich hervorrufen oder bei denen Schusswaffen ohne die erforderlichen waffenrechtlichen Berechtigungen, Kriegswaffen oder Explosivstoffe aufgefunden wurden (…).*

Die im Vorjahr begonnene Datenschutzkontrolle von verdeckten Maßnahmen – konkret Anordnungen des Einsatzes verdeckter Ermittler (VE) oder verdeckt ermittelnder Personen (VP) – gemäß § 29a HSOG wurde im Berichtsjahr abgeschlossen. Gegenstand der Prüfung waren die formellen Voraussetzungen der jeweiligen Anordnungen und das Vorliegen entsprechender richterlicher Beschlüsse gemäß § 16 Abs. 9 HSOG. Im Ergebnis wurden keine datenschutzrechtlichen Verstöße festgestellt.

§ 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.

Neben den gesetzlich vorgeschriebenen Datenschutzkontrollen wurde mit der Prüfung einzelner datenschutzrechtlicher Aspekte im Hinblick auf den Einsatz der Analysesoftware hessenDATA (§ 25a HSOG) bei der Hessischen Polizei begonnen. Diese Kontrolle konnte aufgrund ihrer Komplexität und ihres Umfangs im Berichtsjahr nicht beendet werden und wird im kommenden Jahr fortgeführt.

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

1. *wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, oder wenn gleichgewichtige Schäden für die Umwelt zu erwarten sind, erforderlich ist (Abwehr konkreter Gefahren),*

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

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

(3) Bei der Anwendung zur automatisierten Datenanalyse gilt § 20 Abs. 1 und 2. Dies wird durch eine Verwaltungsvorschrift sichergestellt, die zu veröffentlichen ist. Sie beinhaltet ein Rollen- und Rechtekonzept und ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten. Unter Berücksichtigung der in Abs. 2 Satz 1 nach Schutzgütern und Eingriffsschwellen unterschiedenen Lagebilder orientieren sich diese Konzepte an dem übergeordneten Ziel der Reduzierung des jeweils zu analysierenden Datenvolumens, der Angemessenheit der jeweils angewandten Analysemethode und des größtmöglichen Schutzes Unbeteiligter (funktionale Reduzierung der Eingriffsintensität).

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

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

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

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

(5) Die Einrichtung und wesentliche Änderung einer automatisierten Anwendung zur Datenanalyse erfolgen durch Anordnung der Behördenleitung oder einer oder eines von dieser beauftragten Bediensteten. Die oder der Hessische Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder einer wesentlichen Änderung nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung nachzuholen. Im Übrigen bleiben die Aufgaben und Befugnisse der oder des Hessischen Beauftragten für Datenschutz und Informationsfreiheit unberührt.

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

Im Nachgang zur 2023 abgeschlossenen Datenschutzkontrolle von Ausschreibungen nach § 17 HSOG und § 163e StPO in Verbindung mit Art. 36 Abs. 2 SIS II-Beschluss wurden im Frühjahr und Herbst 2025 erneut die Ausschreibungen von Kontaktpersonen im SIS durch die Hessische Polizei geprüft. Im Ergebnis wurde festgestellt, dass drei Kontaktpersonen gemäß der neuen Rechtsgrundlage Art. 36 Abs. 3 SIS 3.0 Verordnung (EU) 2018/1862 ausgeschrieben waren. Im Rahmen des Kontrollzeitraums waren zwei Ausschreibungen bereits ausgelaufen, so dass folglich neben Beanstandungen lediglich im Hinblick auf die Ausschreibung einer Kontaktperson zur Löschung aufgefordert wurde; die Löschung dieser Ausschreibung ist zeitnah erfolgt.

Bei der ergänzenden Prüfung im Herbst 2025 wurden keine Ausschreibungen von Kontaktpersonen im SIS festgestellt.

4.4
Scan-Funktion für Ausweisdokumente in Polizei-Smartphones

Im Berichtszeitraum haben sich einige Bürger darüber beschwert, dass ihr Ausweisdokument von der Polizei mit dem Handy abfotografiert wurde und dies ein datenschutzrechtlicher Verstoß sei.

In den mir vorgelegten Beschwerden haben die betroffenen Personen vorgetragen, dass das Ausweisdokument im Rahmen einer polizeilichen Kontrolle fotografiert worden sei. Ich konnte den Beschwerdeführern in allen Fällen mitteilen, dass es sich hierbei nicht um eine Fotografie, sondern um einen Scan-Vorgang im Rahmen einer polizeilichen Identitätskontrolle gehandelt hat.

Die Hessische Polizei arbeitet seit einigen Jahren mit dienstlichen Smartphones. Tatsächlich handelt es sich bei den geschilderten Vorgängen nicht um eine Ablichtung, sondern um einen Scan-Vorgang vordefinierter Bereiche des Ausweisdokuments. Der Scan-Vorgang ersetzt die manuelle Erfassung der personenbezogenen Daten im Rahmen einer Identitätsfeststellung etwa nach § 18 HSOG oder § 163b StPO.

Die Scan-Funktion, die in bestimmten dienstlichen Apps individuell im dienstlichen Smartphone installiert ist, erfasst Personalien digital statt manuell. Beim Scan-Vorgang wird – je nach zuvor ausgewähltem Ausweisdokument – ein passgenauer Rahmen vorgegeben, in dem das Dokument erfasst wird. Mithilfe einer optischen Zeichenerkennung werden Textfelder analysiert und nach enthaltener Definition der Textfeldbereiche für den individuellen Vorgang als personenbezogene Daten erfasst. Im Rahmen der Datenverarbeitung wird folglich weder ein Foto aufgenommen noch werden personenbezogene Daten auf dem Gerät gespeichert.

§ 18 HSOG

(1) Die Gefahrenabwehr- und die Polizeibehörden können die Identität einer Person feststellen, wenn dies zur Abwehr einer Gefahr, zur Erfüllung der ihnen durch andere Rechtsvorschriften zugewiesenen weiteren Aufgaben (§ 1 Abs. 2) oder zum Schutz privater Rechte (§ 1 Abs. 3) erforderlich ist. (…)

§ 163b StPO

(1) Ist jemand einer Straftat verdächtig, so können die Staatsanwaltschaft und die Beamten des Polizeidienstes die zur Feststellung seiner Identität erforderlichen Maßnahmen treffen; § 163a Abs. 4 Satz 1 gilt entsprechend. Der Verdächtige darf festgehalten werden, wenn die Identität sonst nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann. Unter den Voraussetzungen von Satz 2 sind auch die Durchsuchung der Person des

Verdächtigen und der von ihm mitgeführten Sachen sowie die Durchführung erkennungsdienstlicher Maßnahmen zulässig.

(2) Wenn und soweit dies zur Aufklärung einer Straftat geboten ist, kann auch die Identität einer Person festgestellt werden, die einer Straftat nicht verdächtig ist; § 69 Abs. 1 Satz 2 gilt entsprechend. Maßnahmen der in Absatz 1 Satz 2 bezeichneten Art dürfen nicht getroffen werden, wenn sie zur Bedeutung der Sache außer Verhältnis stehen; Maßnahmen der in Absatz 1 Satz 3 bezeichneten Art dürfen nicht gegen den Willen der betroffenen Person getroffen werden. (…)

4.5
Vorherige Konsultation zur biometrischen Echtzeit-Fernidentifizierung

Im Rahmen einer vorherigen Konsultation gemäß § 64 HDSIG wurde das Pilotprojekt zur biometrischen Echtzeit-Fernidentifizierung der Hessischen Polizei im Bahnhofsviertel in Frankfurt am Main beraten.

Das Polizeipräsidium Frankfurt am Main nutzt seit Juli 2025 die neu geschaffenen rechtlichen Möglichkeiten der Videoüberwachung gemäß § 14 Abs. 9 bis 11 HSOG mit Unterstützung künstlicher Intelligenz im Rahmen eines Pilotprojekts im Frankfurter Bahnhofsviertel.

Ich habe im Rahmen einer vorherigen Konsultation gemäß § 64 HDSIG zum zeitlich und örtlich begrenzten Pilotprojekt im Bahnhofsgebiet Frankfurt am Main gegenüber der Hessischen Polizei Stellung genommen. Die Stellungnahme hat sich ausschließlich auf die Pilotphase und nicht auf einen etwaigen Regelbetrieb bezogen.

Im Ergebnis gab es keine durchgreifenden datenschutzrechtlichen Bedenken, wobei ich davon ausgehe, dass die insbesondere im Hinblick auf technische und organisatorische Fragestellungen gemachten Anmerkungen im Pilotprojekt Berücksichtigung gefunden haben. Ich messe der Klärung offener Fragestellungen in Bezug auf den Einsatz neuer Technologien zur biometrischen Echtzeit-Fernidentifizierung eine essenzielle Bedeutung im Rahmen des Pilotprojekts bei. Dies gilt in besonderem Maße auch perspektivisch für einen späteren Regelbetrieb. Daher müssen datenschutzrechtliche Fragen systematisch ermittelt sowie als Teil des Pilotprojekts gezielt adressiert, beantwortet und die Ergebnisse evaluiert werden. Nur so kann die für einen etwaigen datenschutzrechtskonformen Regelbetrieb erforderliche Informationsbasis geschaffen werden.

Das Konsultationsverfahren diente weder einer vollumfänglichen Dokumentenprüfung noch einer umfassenden Beratung. Vielmehr soll nach § 64

Abs. 3 Satz 1 HDSIG die Datenschutzaufsichtsbehörde dem Verantwortlichen innerhalb einer kurzen Frist (schriftliche) Empfehlungen zur Ergreifung von weiteren Maßnahmen unterbreiten können. Die im Rahmen der Konsultation gemachten Anmerkungen betrafen u. a. die Inhalte der Datenschutz- und Grundrechtefolgenabschätzung, die Hinweispflichten für die Videoüberwachung, die Informationspflichten zu Betroffenenrechten, die künftig zu beachtenden Vorgaben der KI-Verordnung, Fragen zur Protokollierung, Speicherung, Löschung und Benutzerzugriffen, die verwendete Software und Technologien, die Verwaltungsvorschriften sowie die Beachtung (beschäftigten-)datenschutzrechtlicher Vorgaben.

Ich habe zudem als ergänzende Hilfestellung auf die aktuellen Orientierungshilfen der DSK im Bereich Künstliche Intelligenz hingewiesen (Orientierungshilfe vom 6. Mai 2024 Künstliche Intelligenz und Datenschutz sowie Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Stand Juni 2025).

Ich habe in Bezug auf die konkreten Maßnahmen der biometrischen Echtzeit-Fernidentifizierung lediglich begrenzte Aufsichtsmöglichkeiten, da diese Maßnahmen nur aufgrund einer richterlichen Anordnung gemäß § 14 Abs. 11 HSOG durchgeführt werden dürfen. Eine Bewertung der jeweiligen Maßnahmen obliegt damit nicht meiner Zuständigkeit, sondern der Zuständigkeit der Justiz.

§ 64 HDSIG

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten zu konsultieren, wenn

1. *aus einer Datenschutz-Folgenabschätzung nach § 62 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder*
2. *die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat. […]*

3) Falls die oder der Hessische Datenschutzbeauftragte der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu sechs Wochen nach Erhalt des Ersuchens um Konsultation schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. […]

§ 14 HSOG

(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.

4.6
Mandantendaten auf einem anwaltlichen Instagram-Profil

Durch einen Hinweis habe ich Kenntnis davon erlangt, dass ein Rechtsanwalt personenbezogene Daten aus strafrechtlichen Ermittlungs- und Gerichtsverfahren auf seinem öffentlichen Instagram-Profil veröffentlicht hat. Diese Offenlegung war mangels Rechtsgrundlage unzulässig und verstieß gegen die anwaltliche Verschwiegenheitspflicht sowie gegen datenschutzrechtliche Grundsätze. In der Folge wurde gegen den Anwalt ein Geldbußenverfahren wegen unrechtmäßiger Offenlegung der Daten eingeleitet (s. Kap. 3.2).

Zur Darlegung seiner Arbeit als Strafverteidiger hatte der Rechtsanwalt anwaltliche Handakten ungeschwärzt abgefilmt und auf seinem Instagram-Profil hochgeladen und inhaltlich erläutert. Zu sehen waren zahlreiche staatsanwaltliche Verfügungen und gerichtliche Beschlüsse, die die Einstellung von Strafverfahren zum Gegenstand hatten. Erkennbar waren hierbei die Vor- und Nachnamen der im Strafverfahren beschuldigten Mandanten des Anwalts, ihre Geburtsdaten und Adressen sowie die jeweiligen Tatvorwürfe. In einigen Fällen handelte es sich zudem um Schreiben mit jugendstrafrechtlichem Bezug. Unter dem Video fanden sich bereits Kommentare von Nutzern, die auf das Datenschutzrecht verwiesen. Zum Zeitpunkt des Hinweises war das Video nachweislich bereits mehr als 1.400 Mal aufgerufen worden.

Für die Veröffentlichung der ungeschwärzten Mandatsakten auf Instagram konnte keine Rechtsgrundlage gemäß Art. 5 Abs. 1 Buchst. a i. V. m. Art. 6 Abs. 1 DS-GVO festgestellt werden. Zudem verstößt ein solches Vorgehen gegen datenschutzrechtliche Grundsätze, beispielsweise den Grundsatz der Zweckbindung gemäß Art. 5 Abs. 1 Buchst. b DS-GVO und den Grundsatz der Integrität und Vertraulichkeit gemäß Art. 5 Abs. 1 Buchst. f DS-GVO, für deren Einhaltung der Anwalt als Verantwortlicher der Datenverarbeitung verantwortlich ist.

Art. 5 DS-GVO

(1) Personenbezogene Daten müssen (…)

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“); (…)

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").

Bei der Offenlegung von personenbezogenen Daten gegenüber Dritten handelt es sich um eine erneute Datenverarbeitung, die ihrerseits auf einer Rechtsgrundlage beruhen muss. Die Offenlegung von Namen, Adressen und strafrechtlichen Vorwürfen der Mandantschaft ohne deren Einwilligung und ohne eine andere Rechtsgrundlage ist daher nicht rechtmäßig. Eine Einwilligung zur Veröffentlichung bzw. zum Upload der Dokumente im Internet gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO lag von keinem der Mandanten vor. Auch eine andere Rechtsgrundlage für die Datenverarbeitung des Art. 6 Abs. 1 DS-GVO war in diesem Fall nicht einschlägig. Insbesondere ein berechtigtes Interesse an der Offenlegung der Daten i. S. d. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO konnte nicht festgestellt werden. Nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO ist die Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

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.

Im Rahmen des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO waren das Anonymitätsinteresse der Mandantschaft und das mögliche Informations- und Werbeinteresse für die Tätigkeiten und Erfolge der Kanzlei des Rechtsanwalts gegeneinander abzuwägen. Gerade mit Blick auf die Sensibilität von personenbezogenen Daten aus Strafverfahren, teilweise mit Bezug zum Jugendstrafrecht, und seine gesetzliche Stellung als Berufsgeheimnisträger, der zur Verschwiegenheit verpflichtet ist, überwog das Anonymitätsinteresse die Interessen des Rechtsanwalts deutlich.

Zu berücksichtigen waren insbesondere die Risiken für die Rechte und Freiheiten der betroffenen Mandantinnen und Mandanten, die sich aus der Veröffentlichung der Daten auf einem öffentlichen Instagram-Profil ergeben können. Eine Veröffentlichung im Internet ermöglicht eine schnelle und unkontrollierte Kenntnisnahme und Verbreitung der Daten durch Dritte. Die Beiträge können auf Instagram gespeichert oder erneut weiterversendet werden. Zudem können Screenshots erstellt werden. Diese Risiken wurden zudem dadurch verschärft, dass das Profil öffentlich war und alle Beiträge des Profilinhabers somit leicht zu erfassen waren.

Besonders erschwerend kam hinzu, dass der Rechtsanwalt als Berufsgeheimnisträger gemäß § 43a Abs. 2 Satz 1 Bundesrechtsanwaltsordnung (BRAO) einer gesetzlichen Verschwiegenheitspflicht unterliegt, die bereits die Information darüber, dass überhaupt ein Mandatsverhältnis besteht, umfasst. Durch die Veröffentlichung der Verfahrensakten sowie der darin enthaltenen personenbezogenen Daten und Informationen hatte der Rechtsanwalt nicht unerheblich gegen diese Regelung verstoßen. Darüber hinaus können Rückschlüsse auf Strafverfahren, in denen die Mandantinnen und Mandanten als Beschuldigte geführt werden, rufschädigende Wirkung für die Betroffenen entfalten.

§ 43a BRAO

(1) Der Rechtsanwalt darf keine Bindungen eingehen, die seine berufliche Unabhängigkeit gefährden.

(2) Der Rechtsanwalt ist zur Verschwiegenheit verpflichtet. Diese Pflicht bezieht sich auf alles, was ihm in Ausübung seines Berufes bekanntgeworden ist. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen (…).

Der Fall zeigt, dass Rechtsanwältinnen und Rechtsanwälte vorab gründlich prüfen müssen, inwiefern bei der Nutzung von Social Media oder dem Web zu Werbe- und Informationszwecken für die eigene Arbeit die Vorgaben des Datenschutzrechts und der berufsrechtlichen Verschwiegenheitspflichten eingehalten werden. Mit Blick auf die Risiken für die betroffenen Personen dürfte es sich bei Verstößen wie dem hier geschilderten regelmäßig um sanktionswürdige Datenschutzverletzungen handeln.

5. Hessischer Landtag

Da die Datenverarbeitung des Hessischen Landtages, seiner Fraktionen, seiner Ausschüsse und seiner Abgeordneten sowohl in Verwaltungs- als auch in parlamentarischen Angelegenheiten der DS-GVO unterliegt und ich die Datenschutzaufsicht über diese öffentlichen Stellen ausübe, habe ich für sie Handlungsempfehlungen erarbeitet, die ihnen für typische Situationen zeigen sollen, wie Datenschutz im Hessischen Landtag umgesetzt werden kann (Kap. 5.1). Da alle Fraktionen den Landtag gegen Mitarbeitende der Abgeordneten und der Fraktionen schützen wollen, die parlamentarische Schutzgüter gefährden, brachten sie unterschiedliche Vorschläge in das Gesetzgebungsverfahren ein, um dieses Ziel umzusetzen. Hierzu und zur Anhörung im Ältestenrat erarbeitete ich eine Stellungnahme zur Zulässigkeit der dafür vorgesehenen Datenverarbeitungen (Kap. 5.2).

5.1
Datenschutzaufsicht über den Hessischen Landtag

Spätestens seit dem EuGH-Urteil vom 16. Januar 2024 ist unstrittig, dass die DS-GVO auf alle Verarbeitungen personenbezogener Daten durch Parlamente anwendbar ist. Soweit der Hessische Landtag keine eigene Datenschutzaufsichtsbehörde im Sinne der Art. 51 ff. DS-GVO errichtet hat, übe ich die Datenschutzaufsicht über diesen aus. Zur Einhaltung der Datenschutzvorgaben nach dieser neuen Rechtslage habe ich dem Hessischen Landtag, den Landtagsfraktionen, den Ausschüssen und den Landtagsabgeordneten Handlungsempfehlungen gegeben.

Anwendbarkeit der DS-GVO und Datenschutzaufsicht

Infolge der Rechtsprechung des EuGH (s. EuGH, Urt. vom 9. Juli 2020 – C-272/19; EuGH, Urt. vom 16. Januar 2024 – C-33/22) ist die DS-GVO auf alle Verarbeitungen personenbezogener Daten – auch bei der Wahrnehmung parlamentarischer Aufgaben – durch den Hessischen Landtag, seine Mitglieder, seine Gremien, die Fraktionen sowie die Kanzlei des Landtages anwendbar. Die Datenschutzordnung des Hessischen Landtags (DSO, vom 23. Februar 2022 (s. https://www.lareda.hessenrecht.hessen.de/bshe/document/jlr-LTGOHE2024pAnlage4), welche die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben regelt, kann gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und 3 DS-GVO grundsätzlich weiterhin gelten, soweit sie nicht Vorgaben der DS-GVO widerspricht.

§ 1 DSO des Hessischen Landtags

(1) Für die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Hessischen Landtag, seine Mitglieder, seine Gremien, die Fraktionen sowie durch die Kanzlei des Landtags, soweit sie parlamentarische Aufgaben wahrnimmt, gelten die Vorschriften dieser Datenschutzordnung.

(2) Eine Wahrnehmung parlamentarischer Aufgaben liegt nicht vor, wenn es sich um Verwaltungsangelegenheiten nach § 30 Abs. 1 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) handelt. Werden personenbezogene Daten bei der Wahrnehmung von Verwaltungsaufgaben verarbeitet, gelten die Vorschriften der Datenschutz-Grundverordnung und des HDSIG.

(3) Besondere datenschutzrechtliche Bestimmungen des Landes, die die parlamentarische Arbeit betreffen können, bleiben unberührt.

Art. 6 DS-GVO

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

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

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

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

a) Unionsrecht oder

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

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.

Nicht mehr anwendbar ist jedoch die Regelung des § 15 DSO zu der Überwachung der Einhaltung der DSO durch das Datenschutzgremium.

§ 15 DSO des Hessischen Landtags

(1) Ein zu Beginn der Wahlperiode zu bestimmender Ausschuss überwacht die Einhaltung der Datenschutzordnung des Landtags. Er befasst sich mit Angelegenheiten des parlamentarischen Datenschutzes im Landtag und legt Konfliktfälle dem Ältestenrat zur Veranlassung entsprechender Maßnahmen vor.

(2) Die Beratungen zu Problemen des Datenschutzes sind geheim. Die Mitglieder des Ausschusses sind verpflichtet, auch nach ihrem Ausscheiden, über die ihnen bei ihrer Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Mangels einer den Maßgaben der Art. 51 ff. DS-GVO entsprechenden eigenen Aufsichtsbehörde für den Hessischen Landtag bin ich die zuständige Aufsichtsbehörde für alle Datenverarbeitungen des Hessischen Landtages. Damit stehen mir die Befugnisse nach Art. 58 DS-GVO i. V. m. § 14 Abs. 1 HDSIG (etwa die Anweisung der Bereitstellung von Informationen sowie zu der Änderung von Verarbeitungsvorgängen) zur Verfügung (s. zu aufsichtsrechtlichen Maßnahmen gegenüber öffentlichen Stellen 52. Tätigkeitsbericht, Kap. 5.3; sowie Friedrichsen/Rapp, ZD 2023, 535 ff.).

Rechtliche Maßgaben

Nachfolgend möchte ich einen Überblick der maßgeblichen Regelungen des Datenschutzes nach der DS-GVO für den Hessischen Landtag geben.

Die datenschutzrechtliche Verantwortlichkeit gemäß Art. 4 Nr. 7 DS-GVO richtet sich danach, welche Stelle im konkreten Einzelfall über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Es kann daher nicht nur der Hessische Landtag, sondern etwa ein einzelner Ausschuss (z. B. der Petitionsausschuss oder ein Untersuchungsausschuss), das Präsidium, eine Fraktion oder ein einzelner Abgeordneter „Verantwortlicher“ sein.

Art. 4 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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden; (…)

Der Hessische Landtag und die einzelnen Stellen wie etwa ein Ausschuss oder eine Fraktion sind grundsätzlich öffentliche Stellen gemäß § 2 Abs. 1 HDSIG. Daher gelten nach § 1 Abs. 1 HDSIG ergänzend zur DS-GVO und der DSO die Vorschriften des HDSIG. Die DSO geht gemäß § 1 Abs. 2 HDSIG grundsätzlich dem HDSIG vor.

§ 1 HDSIG

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise.

(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. (…)

§ 2 HDSIG

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

Rechtsgrundlagen zur Verarbeitung personenbezogener Daten für den Hessischen Landtag und die einzelnen Stellen bestehen insbesondere nach Art. 6 Abs. 1 UAbs. 1 Buchst. c oder e DS-GVO i. V. m. Abs. 2 und 3 DS-GVO i. V. m. §§ 3 ff. DSO (s. zu Rechtsgrundlagen für Datenverarbeitungen in Kommunen 53. Tätigkeitsbericht, Kap. 5.2; sowie vertiefend Rapp, KommJur 2024, 401, 404 ff.; die dortigen Ausführungen sind weitgehend übertragbar). Danach kann etwa die Verarbeitung personenbezogener Daten bei der Wahrnehmung

parlamentarischer Aufgaben oder die Übermittlung personenbezogener Daten für nicht parlamentarische Zwecke legitimiert werden.

Der Hessische Landtag sowie die einzelnen Stellen müssen gemäß Art. 37 Abs. 1 DS-GVO, § 5 Abs. 1 HDSIG einen Datenschutzbeauftragten sowie dessen Vertreter benennen (s. dazu „Behördliche und betriebliche Datenschutzbeauftragte“, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-10/behoerdliche_und_betriebliche_datenschutzbeauftragte_231009_1.pdf). Dabei kann (etwa durch die einzelnen Abgeordneten und die Fraktion) gemäß Art. 37 Abs. 3 DS-GVO, § 5 Abs. 2 HDSIG ein gemeinsamer Datenschutzbeauftragter oder entsprechend Art. 37 Abs. 6 DS-GVO, § 5 Abs. 2 HDSIG ein externer Dienstleister benannt werden.

Weitere Pflichten des Hessischen Landtages sowie der einzelnen Stellen sind insbesondere die Führung des Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO, § 18 DSO, die Informationspflichten der Art. 13, 14 DS-GVO sowie die Erfüllung der Rechte der betroffenen Personen wie vor allem des Auskunftsrechts gemäß Art. 15 DS-GVO, § 12 DSO sowie des Rechts auf Löschung nach Art. 17 DS-GVO, § 14 DSO.

Zudem müssen ggf. Verträge zur Auftragsverarbeitung gemäß Art. 28 DS-GVO, § 6 DSO (etwa bei dem Hosting einer Webseite) oder Vereinbarungen zur gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO (etwa bei gemeinsamen Datenverarbeitungen durch mehrere Ausschüsse oder durch eine Fraktion und eine Partei) abgeschlossen werden. Es sind gemäß Art. 32 DS-GVO, § 19 DSO geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten (etwa die Nutzung von kontinuierlich aktualisierten Betriebssystemen und Anwendungen sowie ein Benutzer-Rollen-Konzept). Bei Verarbeitungsformen, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben (z. B. bei der Verarbeitung von Gesundheitsdaten oder KI-Verfahren), muss gemäß Art. 35 DS-GVO vorab eine Datenschutz-Folgenabschätzung durchgeführt werden. Im Falle einer Verletzung des Schutzes personenbezogener Daten (etwa der Fehlversand von E-Mails, der Verlust von Laptops oder Hacking-Angriffe) sind die Meldepflicht des Art. 33 DS-GVO und die Benachrichtigungspflicht des Art. 34 DS-GVO zu berücksichtigen.

Handreichung zum Datenschutz für den Hessischen Landtag

Ich habe dem Hessischen Landtag, den Landtagsfraktionen, den Ausschüssen, den sonstigen Gremien und den Landtagsabgeordneten zur Unterstützung bei der Einhaltung der umfangreichen Anforderungen des Datenschutzes die

„Handreichung zum Datenschutz für den Hessischen Landtag“ zur Verfügung gestellt. Diese Handreichung behandelt ausführlich die Pflichten, die aus der Anwendbarkeit der DS-GVO resultieren. Ergänzend dazu habe ich „Fragen und Antworten zur Handreichung zum Datenschutz für den Hessischen Landtag“ erarbeitet, um die Ausführungen in der Handreichung im Zusammenhang mit Fragen aus dem praktischen Alltag von Abgeordneten zu erläutern. Die Handreichung ist im Intranet des Landtags zu finden. Darüber hinaus stehe ich zu einzelnen datenschutzrechtlichen Fragen beratend zur Verfügung.

5.2
Datenverarbeitung zum Schutz parlamentarischer Rechtsgüter

Das am 16. Dezember 2025 verabschiedete Gesetz zur Änderung des Hessischen Abgeordnetengesetzes und des Hessischen Fraktionsgesetzes (GVBl. 2025 Nr. 108) enthält Regelungen zum Schutz des Hessischen Landtags, die die Verarbeitung personenbezogener Daten betreffen. Zum Entwurf dieses Gesetzes der Fraktion der AfD vom 28. August 2025 (LT-Drs. 21/2598) und zum Entwurf der übrigen Fraktionen vom 2. September 2025 (LT-Drs. 21/2625) sowie in der Anhörung im Ältestenrat des Hessischen Landtags am 4. November 2025 habe ich im Wesentlichen folgende Stellungnahme abgegeben.

Beide Entwürfe beruhen auf einem ausgearbeiteten Vorschlag der Landtagspräsidentin und sind daher weitgehend wortgleich, unterscheiden sich jedoch in bestimmten Schritten der Datenverarbeitung. Sie zielen darauf, sowohl in das Abgeordnetengesetz (§ 6a) als auch in das Fraktionsgesetz (§ 4a) eine neue Vorschrift aufzunehmen.

Inhalt des Entwurfs der Mehrheitsfraktionen

Der Entwurf, der auch Gesetz geworden ist, zielt darauf ab, Beschäftigte von Abgeordneten und Fraktionen, die die parlamentarischen Schutzgüter gefährden, vom Landtag fernzuhalten. Ihnen soll die Nutzung der im Landtag vorhandenen Einrichtungen entzogen oder beschränkt und es soll die Erstattung der Aufwendungen für solche Mitarbeiter verhindert werden können. Damit die Präsidentin und das Präsidium im Einzelfall entscheiden können, ob eine solche Gefährdung besteht, sieht das Gesetz folgende Datenverarbeitungen vor.

Im ersten Schritt sollen die Beschäftigten „freiwillig“ eine Erklärung abgeben können, ob in ihrer Person Umstände vorliegen, die eine solche Gefährdung begründen können. Liegt ein sachlicher Grund für eine mögliche Gefährdung

vor, kann die Präsidentin zu der jeweiligen Person „ein Führungszeugnis für Behörden“ nach § 31 Abs. 1 BZRG einholen. Hierzu übermittelt sie im zweiten Schritt die Grunddaten der betroffenen Personen an das Bundeszentralregister und erhält im dritten Schritt von diesem das erbetene Führungszeugnis. Enthält das Führungszeugnis eine Eintragung, darf die Präsidentin im vierten Schritt „mit Einwilligung der betroffenen Person Einsicht in die zugrundeliegende Entscheidung nehmen“. „Soweit dies im Einzelfall zur Aufklärung geboten erscheint, ersucht die Präsidentin“ im fünften Schritt „mit Einwilligung der betroffenen Person“ das Landeskriminalamt und das Landesamt für Verfassungsschutz um Auskunft, ob und welche Erkenntnisse zu einem Ausschlussgrund dort vorhanden sind. Hierfür übermittelt sie die Grunddaten der betroffenen Person an die beiden Behörden. Diese übermitteln im sechsten Schritt ihre Erkenntnisse an die Präsidentin. Diese Informationen dürfen in einem siebten Schritt „auch für sonstige gegen die betroffene Person gerichtete Maßnahmen zum Schutz der parlamentarischen Schutzgüter verwendet werden“. Schließlich entscheidet die Präsidentin im achten Schritt „im Einvernehmen mit dem Präsidium“ unter Auswertung aller erlangten Informationen in Form eines Verwaltungsakts, ob „ein Ausschlussgrund besteht“, und gibt „die Feststellung dem Mitglied des Landtags, bei dem die betroffene Person beschäftigt ist, einschließlich der sie tragenden Gründe bekannt“.

Inhalt des Entwurfs der AfD-Fraktion

Der Entwurf enthält drei wesentliche Abweichungen vom Mehrheitsentwurf: Erstens beschränken sich die vorgesehenen Schutzmaßnahmen darauf, die Nutzung der im Landtag vorhandenen Einrichtungen auszuschließen. Dies ist zweitens nur zulässig, wenn eine Gefährdung der Schutzgüter des Landtages festgestellt wurde. Drittens kann die Erstattung von Aufwendungen für die Beschäftigung solcher Mitarbeitenden nicht ausgeschlossen werden. Aufgrund dieser Änderungen sind weniger Schritte zur Datenverarbeitung notwendig.

Datenschutzrechtliche Bewertung des Mehrheitsentwurfs

Mit den neuen Regelungen sollen Rechtsgrundlagen entsprechend Art. 6 Abs. 1 UAbs. 1 Buchst. c und e DS-GVO geschaffen werden. Nach Art. 6 Abs. 3 Satz 4 DS-GVO muss die mitgliedstaatliche Regelung ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen. Der Schutz des Landtages ist ein Ziel, das im öffentlichen Interesse liegt. Die vorgesehene Datenverarbeitung steht in einem angemessenen Verhältnis zu diesem legitimen Zweck.

Die zu verarbeitenden Daten betreffen überwiegend politische Meinungen und weltanschauliche Überzeugungen und sind insoweit besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO. Die Verarbeitung solcher Daten ist nach Art. 9 Abs. 2 DS-GVO zulässig, wenn sie „aus Gründen eines erheblichen öffentlichen Interesses erforderlich" ist und „das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht". Ein Gesetz zum Schutz der parlamentarischen Schutzgüter ist aus Gründen eines erheblichen öffentlichen Interesses erforderlich. Die vorgesehenen Verarbeitungsschritte sind auch angemessen.

Das Ausfüllen des Fragebogens ist für die jeweils betroffene Person freiwillig. Das freiwillige Ausfüllen ist jedoch keine Einwilligung im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 7, Art. 9a Abs. 2 Buchst. a DS-GVO und § 23 Abs. 2 HDSIG, weil sich aus der Verweigerung der Erklärung negative Schlussfolgerungen ergeben, die unweigerlich zu weiteren Datenverarbeitungen und eventuell weiteren Konsequenzen führen. Es wird jedoch der betroffenen Person überlassen, ob sie mitwirkt oder nicht. Sie kann sich selbst zu möglichen Ausschlussgründen erklären und frühzeitig Missverständnissen vorbeugen. Sie kann aber auch ihre Mitwirkung verweigern. Ihre informationelle Selbstbestimmung wird dadurch im größtmöglichen Ausmaß berücksichtigt, das die Erreichung des legitimen Ziels zulässt.

Um die Angaben in der Selbstauskunft zu prüfen und einen möglichen Verdacht zu konkretisieren, kann die Präsidentin ein Führungszeugnis für Behörden einholen. Hierfür muss sie die Grunddaten zu der betroffenen Person aus der Personalabteilung an das Bundeszentralregister übermitteln. Dies sind keine besonders schützenswerten Daten nach Art. 9 Abs. 1 DS-GVO. Das Gesetz darf die zweckändernde Übermittlung nach Art. 6 Abs. 4 DS-GVO vorsehen. Das Bundeszentralregister darf nach § 31 BZRG auf Anforderungen Führungszeugnisse an Behörden übermitteln.

Enthält das Führungszeugnis einen Hinweis auf die Verurteilung wegen einer einschlägigen Straftat, ist dies ein begründeter Anlass, um dem dadurch entstandenen Verdacht einer Gefährdung der parlamentarischen Schutzgüter nachzugehen. Auch hier ist die „Einwilligung" der betroffenen Person keine Einwilligung im Sinne der DS-GVO. Vielmehr ist die Mitwirkung der betroffenen Person ein Tatbestandsmerkmal des gesetzlichen Erlaubnistatbestands. Ohne Mitwirkung muss die abschließende Entscheidung ohne die Einsichtnahme getroffen werden. Die Regelung ist geeignet und erforderlich, um das legitime Ziel des Gesetzes zu erreichen, und wahrt dabei die informationelle Selbstbestimmung der betroffenen Person im größtmöglichen Ausmaß.

Anfragen beim Landeskriminalamt und beim Landesamt für Verfassungsschutz sind nur zulässig, „soweit dies im Einzelfall zur Aufklärung geboten erscheint“. Es müssen also belastbare Anhaltspunkte für eine Gefährdung der parlamentarischen Schutzgüter vorliegen. In diesem Fall sind die Anfragen bei den Ämtern und deren Auskünfte geeignet, erforderlich und angemessen.

Die Präsidentin darf Informationen über betroffene Personen, die in den zuvor untersuchten Verarbeitungsschritten gewonnen wurden, auch für sonstige gegen die betroffene Person gerichtete Maßnahmen zum Schutze der parlamentarischen Schutzgüter verwenden, insbesondere für Maßnahmen der Gefahrenabwehr. Auch diese Erlaubnis zu einer Zweckänderung ist nach Art. 6 Abs. 4 DS-GVO zulässig.

Datenschutzrechtliche Bewertung des Entwurfs der AfD

Soweit der Entwurf die gleichen Schritte der Datenverarbeitung wie im Mehrheitsentwurf vorsieht, gelten auch für diesen Entwurf die gleichen Bewertungen.

Er unterscheidet sich vom Mehrheitsentwurf dadurch, dass er weniger einschneidende Rechtsfolgen und damit geringere Grundrechtseingriffe vorsieht. Insofern könnte er dem Mehrheitsentwurf vorzuziehen sein. Er verfehlt jedoch einen angemessenen Ausgleich zwischen Allgemeininteressen und betroffenen Grundrechten, weil er keinen ausreichenden Schutz für die parlamentarischen Schutzgüter bewirkt. Nach ihm würde eine Person, die „die Arbeits- und Funktionsfähigkeit oder die Ordnung und Würde des Landtages gefährdet“ oder sich „an einer sicherheitsgefährdenden oder geheimdienstlichen Tätigkeit“ oder „an Bestrebungen der Organisierten Kriminalität (…) beteiligt hat oder selbst aktiv für die verfassungsfeindliche Ausrichtung oder Zielsetzung ihre Bestrebung (…) eingetreten ist“, weiterhin vom Landtag finanziert und seine gefährdende Tätigkeit weiterhin auf Kosten des Landtages ausüben. Insofern ist der Gesetzentwurf ungeeignet, das selbstgesetzte Ziel, den „Schutz der Arbeits- und Funktionsfähigkeit sowie Ordnung und Würde des Landtages“, zu erreichen.

6. 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. Diese haben sich im Berichtszeitraum weiterentwickelt (Kap. 6.1). Die Verwaltung setzt auch neue Techniken ein, wie etwa Luftbilder durch Drohnen für die Ermittlung von Abwassergebühren (Kap. 6.2). Ein eher älteres Instrument sind die Kehrbücher der Schornsteinfeger. Da diese mit Verwaltungsaufgaben beliehen sind, bestehen Grenzen für die Datenübermittlung aus diesen Büchern an Privatunternehmen (Kap. 6.3). Ebenso bestehen Grenzen für die Weitergabe von Meldedaten an den Beitragsservice für den öffentlich-rechtlichen Rundfunk (Kap. 6.4). Am Beispiel des digitalen Wohngeldverfahrens werden die Nutzung länderübergreifender Online-Dienste und die Rechtslage nach dem Onlinezugangsgesetz erörtert (Kap. 6.5).

6.1 Aktuelle Entwicklungen in der Landes- und Kommunalverwaltung

Die Entwicklungen des Datenschutzes in der Verwaltung waren auch im Berichtszeitraum sehr dynamisch. Neben Neuerungen des Kommunalrechts schreitet insbesondere die Umsetzung des Onlinezugangsgesetzes voran. Hinsichtlich der komplexen datenschutzrechtlichen Anforderungen werden die betroffenen Stellen mit zwei neuen Leitfäden unterstützt. Bei der Erstellung von datenschutzrechtlichen Rechtsgrundlagen hilft fortan ein „Rechtsgrundlagen-Generator“ für die öffentliche Verwaltung.

Reform des Kommunalrechts

Mit dem Gesetz zur Verbesserung der Funktionsfähigkeit der kommunalen Vertretungskörperschaften und zur Änderung kommunalrechtlicher Vorschriften vom 1. April 2025 (GVBl. Nr. 24 S. 1) soll das Kommunalverfassungsrecht mittels Erweiterung digitaler Teilhabe- und Veröffentlichungsmöglichkeiten zeitgemäß ausgestaltet werden. Dieses Ziel ist zu begrüßen. Im Rahmen einer Stellungnahme zum Gesetzentwurf habe ich Ergänzungen und Konkretisierungen hinsichtlich des Datenschutzes vorgeschlagen, die in der Gesetzesbegründung weitgehend übernommen worden sind.

Die auch datenschutzrechtlich relevanten Neuerungen möchte ich nachfolgend darstellen:

Gemäß § 52 Abs. 3 Satz 2 HGO können Kommunen nunmehr in der Hauptsatzung eine Echtzeitübertragung von öffentlichen Sitzungen der Gemeindevertretung in Bild und Ton im Internet zulassen und Bestimmungen treffen, in welchem Umfang Aufzeichnungen von öffentlichen Sitzungen zum Abruf bereitgestellt werden. Mit dieser Regelung wird der erhöhten Bedeutung von Übertragungen kommunaler Sitzungen im Internet und einem gewandelten Öffentlichkeitsbegriff in Richtung einer digitalen Partizipation entsprochen (s. 50. Tätigkeitsbericht, Kap. 8.2). Über § 32 HKO ist die Regelung auch für Kreistage anwendbar. Ausweislich der Gesetzesbegründung (LT-Drs. 21/1303, S. 25) sind die Bestimmungen des Datenschutzes zu berücksichtigen und es muss eine Abwägung mit den Rechten und Interessen betroffener Personen erfolgen, indem z. B. Einschränkungen der aufzunehmenden Personen geregelt werden, nur ein bestimmter Ausschnitt des Sitzungssaals aufgenommen wird oder unbeteiligte Personen wie Zuhörerinnen und Zuhörer oder Gemeindebedienstete nicht gezeigt werden. Dritten Personen (insbesondere Besucherinnen und Besuchern sowie Beschäftigten der Kommune) ist eine Teilnahme an der Sitzung auch ohne deren Aufzeichnung zu ermöglichen.

§ 52 HGO

(3) Die Hauptsatzung kann bestimmen, dass in öffentlichen Sitzungen Film- und Tonaufnahmen durch die Medien mit dem Ziel der Veröffentlichung zulässig sind. Ferner kann die Hauptsatzung eine Echtzeitübertragung von öffentlichen Sitzungen der Gemeindevertretung in Bild und Ton im Internet zulassen und Bestimmungen treffen, in welchem Umfang Aufzeichnungen von öffentlichen Sitzungen zum Abruf bereitgestellt werden.

Nach § 52a HGO können Mitglieder der Gemeindevertretung sowie der Gemeindevorstand auch ohne Anwesenheit am Sitzungsort per Bild-Ton-Übertragung an den Sitzungen der Gemeindevertretung teilnehmen, soweit die Hauptsatzung dies bestimmt. Damit können Kommunen eine digitale Sitzungsteilnahme ermöglichen. Volldigitale Sitzungen ohne Anwesenheit sind im Gegensatz zum Gemeindevorstand (s. unten) für die Gemeindevertretung jedoch nicht zulässig. Nach § 52a Abs. 5 HGO und über § 62 Abs. 5 und § 82 Abs. 6 HGO gelten die Regelungen für die digitale Sitzungsteilnahme für den Ausländerbeirat, die Integrations-Kommission, für Ausschüsse und Ortsbeiräte entsprechend. Für Kreistage ist die Regelung über § 32 HKO ebenfalls anwendbar.

Nach der Gesetzesbegründung (LT-Drs. 21/1303, S. 26) hat die Gemeinde die datenschutzrechtlichen Bestimmungen zu beachten. Mit Blick auf Art. 5 Abs. 1 Buchst. f, Art. 25 und Art. 32 DS-GVO hat die Gemeinde geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines dem

Risiko angemessenen Schutzniveaus vorzusehen sowie die Einhaltung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu gewährleisten.

§ 52a HGO

(1) Mitglieder der Gemeindevertretung sowie der Gemeindevorstand können auch ohne Anwesenheit am Sitzungsort per Bild-Ton-Übertragung an den Sitzungen teilnehmen, soweit die Hauptsatzung dies bestimmt. Satz 1 gilt nicht für den Vorsitzenden der Gemeindevertretung. Zugeschaltete Mitglieder der Gemeindevertretung gelten in diesem Fall als anwesend im Sinne von § 53 Abs. 1 Satz 1.

(2) Eine Teilnahme mittels Bild-Ton-Übertragung ist ausgeschlossen bei Wahlen nach § 55, Beschlussfassungen nach § 39a Abs. 3 Satz 2, § 57 Abs. 2, § 76 Abs. 1 und Abs. 4 Satz 3, § 76a und in der ersten Sitzung der Gemeindevertretung. Die Gemeinde kann in der Hauptsatzung die Zulässigkeit der Teilnahme mittels Bild-Ton-Übertragung in weiteren Fällen ausschließen. Lässt eine Gemeinde in der Hauptsatzung eine Teilnahme per Bild-Ton-Übertragung auch in nicht öffentlichen Sitzungen zu, haben die zugeschalteten Mitglieder der Gemeindevertretung sicherzustellen, dass keine weiteren Personen die Sitzung verfolgen können.

(3) Der Vorsitzende der Gemeindevertretung und die Mitglieder der Gemeindevertretung müssen sich in der Sitzung gegenseitig optisch und akustisch wahrnehmen können. In öffentlichen Sitzungen muss gewährleistet sein, dass per Bild-Ton-Übertragung teilnehmende Gemeindevertreter auch für die im Sitzungssaal anwesende Öffentlichkeit in Bild und Ton wahrnehmbar sind. Für die Zwecke des Satz 1 und 2 sind Bild- und Tonaufnahmen auch ohne Zustimmung der an der Sitzung teilnehmenden Personen zulässig.

(4) Die Gemeinde hat dafür Sorge zu tragen, dass in ihrem Verantwortungsbereich die technischen Voraussetzungen für eine Zuschaltung mittels Bild-Ton-Übertragung während der Sitzung durchgehend bestehen. Bei technisch bedingten Störungen der akustischen oder optischen Wahrnehmbarkeit, die im Verantwortungsbereich der Gemeinde liegen, darf die Sitzung nicht beginnen oder muss sie unterbrochen werden. Sonstige Störungen sind unbeachtlich und haben keinen Einfluss auf die Wirksamkeit der in der Sitzung gefassten Beschlüsse. Die Gemeinden können in der Hauptsatzung oder der Geschäftsordnung der Gemeindevertretung weitere Einzelheiten der Sitzungsteilnahme mittels Bild-Ton-Übertragung regeln.

(5) Für den Ausländerbeirat nach § 84 und die Integrations-Kommission nach § 89 gelten die Abs. 1 bis 4 entsprechend.

Gemäß § 61 Abs. 4 HGO ist die Einsichtnahme in die Niederschriften über öffentliche Sitzungen der Gemeindevertretung den Einwohnern zu ermöglichen. Zu diesem Zweck kann die Geschäftsordnung vorsehen, dass Niederschriften mit dem Inhalt nach Absatz 1 auf der Internetseite der Gemeinde veröffentlicht werden. Mit dieser Regelung wird eine Rechtsgrundlage zur Einsichtnahme in Niederschriften öffentlicher Sitzungen geschaffen. Die Möglichkeit für die Einwohner kann statt durch eine physische Einsichtnahme bei der Kommunalverwaltung auch durch eine Zurverfügungstellung dieser

Niederschriften (auch) im Internet (etwa in politischen Informationssystemen) geschaffen werden. Für Kreistage ist die Regelung über § 32 HKO ebenfalls anwendbar. Ausweislich der Gesetzesbegründung (LT-Drs. 21/1303, S. 27) müssen die Niederschriften inhaltlich datenschutzgerecht gestaltet werden und dürfen nicht über die nach Absatz 1 zwingenden Inhalte hinausgehen. Auf personenbezogene Daten von dritten Personen wie etwa Bürgerinnen und Bürgern ist im Rahmen der Veröffentlichung der Niederschriften möglichst zu verzichten (s. zum Datenschutz bei politischen Informationssystemen bereits 53. Tätigkeitsbericht, Kap. 5.4; 52. Tätigkeitsbericht, Kap. 5.3; 50. Tätigkeitsbericht, Kap. 8.2; die Handreichung auf meiner Webseite, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2024-07/handreichuing_datenschutz_bei_politischen_informationssystemen_240724.pdf; sowie ausführlich Rapp, KommJur 2025, 201 ff.).

§ 61 HGO

(4) Die Einsichtnahme in die Niederschriften über öffentliche Sitzungen der Gemeindevertretung ist den Einwohnern zu ermöglichen. Zu diesem Zweck kann die Geschäftsordnung vorsehen, dass Niederschriften mit dem Inhalt nach Abs. 1 auf der Internetseite der Gemeinde veröffentlicht werden.

Gemäß § 67 HGO können die Mitglieder des Gemeindevorstands auch ohne Anwesenheit am Sitzungsort per Bild-Ton-Übertragung an den Sitzungen des Gemeindevorstands teilnehmen, soweit die Geschäftsordnung dies bestimmt. Der Gemeindevorstand kann – weitergehend als die Gemeindevertretung – vollständig digitale Sitzungen durchführen. Die Regelungen gelten über § 72 Abs. 4 HGO für Kommissionen sowie über § 42 HKO für Kreisausschüsse entsprechend. Nach der Gesetzesbegründung (LT-Drs. 21/1303, S. 27) hat die Gemeinde die datenschutzrechtlichen Bestimmungen zu beachten. Mit Blick auf Art. 5 Abs. 1 Buchst. f, Art. 25 und Art. 32 DS-GVO hat die Gemeinde geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus vorzusehen sowie die Einhaltung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen zu gewährleisten.

§ 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. Die Mitglieder des Gemeindevorstandes können auch ohne Anwesenheit am Sitzungsort per Bild-Ton-Übertragung an den Sitzungen teilnehmen, soweit die Geschäftsordnung dies bestimmt. Zugeschaltete Mitglieder des Gemeindevorstandes gelten in diesem Fall

als anwesend im Sinne von § 68 Abs. 1 Satz 1. In einfachen Angelegenheiten können die Beschlüsse im Umlaufverfahren gefasst werden, wenn niemand widerspricht.

(2) Eine Teilnahme mittels Bild-Ton-Übertragung ist ausgeschlossen bei Wahlen nach § 55 und in der ersten Sitzung des Gemeindevorstandes. Der Gemeindevorstand kann in der Geschäftsordnung die Zulässigkeit der Teilnahme mittels Bild-Ton-Übertragung in weiteren Fällen ausschließen. Lässt der Gemeindevorstand eine Teilnahme per Bild-Ton-Übertragung in der Geschäftsordnung zu, haben die zugeschalteten Mitglieder des Gemeindevorstandes sicherzustellen, dass keine weiteren Personen die Sitzung verfolgen können. § 52a Abs. 3 und 4 gelten entsprechend.

Zusätzlich zu den bereits erfolgten Gesetzesänderungen empfehle ich, das Kommunalrecht um eine Regelung zu ergänzen, welche die Verarbeitung personenbezogener Daten mittels politischer Informationssysteme ausdrücklich normiert. Wenngleich eine derartige Verarbeitung grundsätzlich gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und Abs. 3 DS-GVO i. V. m. § 3 Abs. 1 HDSIG i. V. m. dem Öffentlichkeitsprinzip gemäß § 52 HGO zulässig ist und mit der Reform Teilaspekte (insbesondere betreffend Aufzeichnungen von öffentlichen Sitzungen der Gemeindevertretungen und Kreistage sowie Veröffentlichung der Niederschriften) geregelt worden sind, dient eine solche Regelung einer weiteren Verbesserung der Rechtssicherheit und der Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Eine solche Regelung erscheint angesichts der zunehmenden Relevanz politischer Informationssysteme in der Praxis umso vordringlicher.

Umsetzungshilfen zum Onlinezugangsgesetz

Im Dezember 2025 hat die DSK die Version 1.1 der „Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG) – Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen“ veröffentlicht (s. https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG_Version_1_1.pdf). Bereits in der Version 1.0 der Orientierungshilfe sind die wesentlichen datenschutzrelevanten Änderungen gegenüber der alten Rechtslage (vor dem Inkrafttreten des OZG-Änderungsgesetzes am 24. Juli 2024) beschrieben worden (insbesondere die Rechtsgrundlagen der Datenverarbeitung in einem länderübergreifenden Onlinedienst gemäß § 8a OZG sowie die Zuweisung der Verantwortlichkeit an die den länderübergreifenden Onlinedienst betreibende Behörde nach Abs. 4). Die ausführlich überarbeitete Version 1.1 befasst sich mit weiteren Fragestellungen aus der Praxis. Neben dem Erfordernis, datenschutzrechtliche Vereinbarungen aufzuheben, die § 8a OZG entgegenstehen (Auftragsverarbeitungsverträge oder Vereinbarungen zur gemeinsamen Verantwortlichkeit), die vor Inkrafttreten des OZG-Änderungsgesetzes ab-

geschlossen worden waren, befasst sich die Neufassung eingehend mit der Definition des „länderübergreifenden Onlinedienstes“ gemäß §§ 2 Abs. 8, 8a OZG. Es ist eine weite Auslegung zu befürworten, um eine Umgehung der Regelung des § 8a OZG (mit den darin enthaltenen Rechtsgrundlagen sowie der Verantwortungszuweisung) und der damit bezweckten rechtlichen Klarstellungen und Vereinfachungen im Gegensatz zu der Rechtslage vor Inkrafttreten des OZG-Änderungsgesetzes (s. dazu 51. Tätigkeitsbericht, Kap. 7.1) entgegenzuwirken.

Zudem wurde im Dezember 2025 von der DSK der „Standardisierte Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz (OZG)“ veröffentlicht (s. https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Standardisierter_Pruefprozess_OZG.pdf). Dieser bietet eine strukturierte Handlungsanleitung zu der Umsetzung der datenschutzrechtlichen Maßgaben bei der Entwicklung oder grundlegenden Überarbeitung von länderübergreifenden Onlinediensten im Sinne der §§ 2 Abs. 8, 8a OZG, mit denen das Nachnutzungsmodell „Einer-für-Alle“ (s. dazu 50. Tätigkeitsbericht, Kap. 8.1) umgesetzt wird („EfA-Onlinedienste“). Zudem werden die Vorgaben zum Datenschutz nach DIN SPEC 66336, 5.8 berücksichtigt und konkretisiert sowie zu der Bestimmung der verschiedenen Rollen auf die verbindlichen Mindestanforderungen an den Betrieb von „Einer für Alle“-Services des IT-Planungsrates zurückgegriffen. Der Standardprozess richtet sich primär an die Behörden, die „EfA-Onlinedienste“ betreiben und denen damit die datenschutzrechtliche Verantwortung zugewiesen ist. Er orientiert sich an den klassischen Phasen des Projektmanagements im Bund und in den Ländern: 1. Initialisierungsphase, 2. Definitionsphase, 3. Planungsphase, 4. Durchführungsphase, 5. Abschlussphase. Jeder Projektmanagementphase werden Standardprozessschritte (die wichtigsten Fragen, die aus datenschutzrechtlicher Sicht zu prüfen und zu klären sind) zugeordnet. Als Anlage findet sich unter Berücksichtigung aller Standardprozessschritte ein Vorschlag einer Standardstruktur für ein Datenschutzkonzept mit anschließender Datenschutz-Folgenabschätzung.

Diese beiden Papiere, an denen auch Beschäftigte meiner Behörde mitgearbeitet haben, unterstützen die betroffenen Stellen bei der Umsetzung der komplexen datenschutzrechtlichen Anforderungen des Onlinezugangsgesetzes.

„Rechtsgrundlagen-Generator“ für die öffentliche Verwaltung

Mit der „Blaupause und Handreichung zur Erstellung fachgesetzlicher datenschutzrechtlicher Rechtsgrundlagen (RGL-Generator)“ steht eine Unterstützung bei der Gestaltung von datenschutzrechtlichen Rechtsgrundlagen insbesondere für Referentinnen und Referenten in den (Bundes- und Landes-)

Ministerien, Beschäftigte der Fraktionen des Bundestages und der Landtage sowie Beschäftigte in Kommunalverwaltungen zur Verfügung (s. https://www.it-planungsrat.de/fileadmin/it-planungsrat/der-it-planungsrat/schwerpunktthemen/SPT-Datenschutz_Datennutzung_Rechtsgrundlagen-Generator_v1.docx). Der RGL-Generator wurde im Rahmen des Schwerpunktthemas Datennutzung des IT-Planungsrats im Kompetenzteam Datenschutz erstellt. Mitglieder des AK Verwaltung der DSK, auch von meiner Behörde, haben beratend daran mitgewirkt.

Der RGL-Generator bietet einen knappen und strukturierten Überblick zu den Formulierungen einer datenschutzrechtlichen Rechtsgrundlage. Neben Formulierungen zu der Verarbeitung einfacher personenbezogener Daten nach Art. 6 DS-GVO sind u. a. auch solche zu der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO sowie zu Löschungs- und Aufbewahrungsfristen enthalten.

Der RGL-Generator ist sehr zu begrüßen. Damit können die Qualität sowie eine stärkere Vereinheitlichung der datenschutzrechtlichen Rechtsgrundlagen, die auch der Rechtssicherheit dienen, gefördert werden. Aufgrund der – wegen des weiten Adressatenkreises notwendigen – eher allgemein gehaltenen Ausführungen muss jedoch stets ein Austausch mit den Fachabteilungen der Behörden und den Fachämtern der Kommunen erfolgen. Zudem sollten die Beschäftigten des operativen Datenschutzes sowie die behördlichen Datenschutzbeauftragten zu datenschutzrechtlichen Problemen kontaktiert werden.

6.2
Luftbilder für die Ermittlung von Abwassergebühren

Mehrere Beschwerden betrafen Drohnenbefliegungen mit dem Ziel, hochauflösende Luftbilder zu erstellen, um Abwassergebühren durch Gemeinden zu berechnen.

Drohnenbilder für Abwasserberechnung

Abwassergebühren und Abwasserbeiträge werden auf der Grundlage kommunaler Satzungen erhoben. Die Gebühren für Niederschlagswasser richten sich dabei nach Größe, Art und Beschaffenheit der versiegelten Grundstücksflächen (z. B. betonierte, befestigte oder überbaute Flächen). Um diese festzustellen, können Luftbilder unterstützen. Die betreffenden Gemeinden beauftragten daher gewerbliche Anbieter zur Erstellung von Luftbildern und/oder zur Verwaltung der Bilder in hierzu (verwaltungsintern) genutzten Geodaten-Anwendungen.

Datenschutzrechtliche Bewertung

Bei Luftbildaufnahmen von Grundstücken handelt es sich um personenbezogene Daten. Nach Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Eine Person gilt als identifizierbar, wenn sie direkt oder indirekt identifiziert werden kann. Auch wenn auf solchen Luftbildern primär sachbezogene Informationen wie Gebäudeumrisse, befestigte Flächen und keine Gesichter oder Kfz-Kennzeichen sichtbar sind, kann sich ein Personenbezug aus der Georeferenzierung der Daten ergeben, die eine eindeutige Zuordnung zum jeweiligen Grundstückseigentümer oder -nutzer ermöglicht. Dies geschieht durch ein Hinzuziehen weiterer Quellen, wie z. B. den Zugriff auf Melde- oder Eigentümerdaten, wodurch eine Zuordnung zum Eigentümer oder Nutzer erfolgen kann und Personen identifizierbar werden.

Luftbilder können dabei beispielsweise durch Sichtbarkeit von Gartengestaltung, Spielgeräten für Kinder, baulichen Besonderheiten oder anderer Merkmale Rückschlüsse auf private Lebensumstände zulassen, die Indizien zur familiären Situation, zu sozialen oder wirtschaftlichen Verhältnissen liefern können. Eine Identifizierung der Grundstückseigentümer und die Zuordnung der Bilder zu Personen ist im Falle der Abwassergebührenermittlung durch die Gemeinde sogar explizit vorgesehen, um die Beitragsschuldner zu ermitteln.

Im Vergleich zu den in meinem 51. Tätigkeitsbericht geprüften, durch Befahrung erstellten und durch öffentliche Stellen genutzten 360°- Panoramaaufnahmen ermöglichen hochauflösende Luftbilder darüber hinaus einen Blick „hinter den Zaun“. Sie weisen dadurch im Vergleich eine höhere Eingriffsintensität auf.

Zu den mir vorliegenden Eingaben habe ich die Verantwortlichen zu Stellungnahmen aufgefordert. Bei der Auswertung der Stellungnahmen von verantwortlichen Gemeinden zeigten sich große Unterschiede, was beispielsweise das Bewusstsein für den Datenschutz in diesem Kontext, die technischen und organisatorischen Maßnahmen (u. a. Qualität der Bilder, maximaler Maßstab, Auflösung, Verpixelung, Zugriffsrechte) und die Erfüllung von Informationspflichten betrifft. Es zeigte sich insbesondere, dass öffentliche Stellen zum Teil irrig davon ausgingen, dass bei den Luftbildern überhaupt kein Personenbezug gegeben sei. Weiterhin wurde mehrfach angenommen, dass eine Rechtsgrundlage für die Verarbeitung von Daten bereits in der Betriebsgenehmigung der Regierungspräsidien für die Drohnenflüge läge.

Zum Teil sind die Verantwortlichen aber auch davon ausgegangen, dass z. B. das Zutrittsrecht, das in der Regel in den jeweiligen Entwässerungssatzungen der Gemeinden geregelt ist, eine Rechtsgrundlage für die Verarbeitung der hochauflösenden Bilder zu diesem Zwecke darstellen kann. Zwar können grundsätzlich auch die Grundstücksentwässerungssatzungen sowie die da-

zugehörige Gebührensatzung, die als jeweilige Vorschriften des Fachrechts vorrangig in den Blick zu nehmen sind, taugliche Ermächtigungsgrundlagen im Sinne von Art. 6 Abs. 3 Satz 1 DS-GVO darstellen, jedoch ließ sich in den geprüften Fällen den jeweiligen Entwässerungssatzungen keine Befugnis zu einer Erhebung und Verwertung von Luftbilddaten herleiten.

Da mangels spezialgesetzlicher Regelung als Rechtsgrundlage für die öffentlichen Stellen Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO i. V. m. der Generalklausel des § 3 HDSIG herangezogen werden müsste, ist für die Beurteilung der Erforderlichkeit die Eingriffsintensität im Verhältnis zu den Zwecken maßgeblich. Hieraus folgt der Maßstab für die Anforderungen an technische und organisatorische Maßnahmen.

Was die Informationspflichten nach Art. 14 DS-GVO betrifft, wurden diese in keinem der in Prüfung befindlichen Fälle ausreichend erfüllt, worauf ich die jeweiligen Gemeinden hingewiesen habe. Es mussten zum Teil Informationen vollständig nachgeholt, korrigiert oder ergänzt werden.

Da Drohnenflüge zur Erstellung von Luftbildern im Rahmen der Erfüllung weiterer Aufgaben von öffentlichen Stellen zunehmend genutzt werden, sammle ich derzeit weitere Informationen, um Anforderungen an technische und organisatorische Maßnahmen gemessen an der Erforderlichkeit für die jeweilige Aufgabenerfüllung formulieren zu können und um diesbezüglich flächendeckend zu sensibilisieren und zu beraten.

6.3
Datenübermittlung aus den Kehrbüchern der Schornsteinfeger an Privatunternehmen

Die Übermittlung von Kontaktdaten der betroffenen Endkunden aus den Kehrbüchern der bevollmächtigten Bezirksschornsteinfeger an ein privates Unternehmen zu Produktwarn- oder -rückrufaktionen ist nicht zulässig.

Übermittlungsanforderung

Ein privates Unternehmen fragte bei mir an, ob die Übermittlung personenbezogener Daten aus den Kehrbüchern der bevollmächtigten Bezirksschornsteinfeger an ein Privatunternehmen zu Produktwarn- oder -rückrufaktionen zulässig ist. Das Kehrbuch ist gemäß § 19 Gesetz über das Berufsrecht und die Versorgung im Schornsteinfegerhandwerk (SchfHwG) eine Datenbank, die alle zur Verwaltung notwendigen Angaben (u. a. Eigentümer und Anschriften, Feuerstättendaten, Messdaten, Kehrfristen und Durchführungsdaten) enthält. Das Unternehmen begehre die in den Kehrbüchern eingetragenen Kontaktdaten der betroffenen Endkunden (Vor- und Familienname sowie

Anschrift des Eigentümers, Besitzers etc.). Als Hersteller müsse es den Verpflichtungen nach verschiedenen Produktsicherheitsvorschriften (u. a. § 6 Abs. 4 ProdSG, § 823 BGB, §§ 1, 3, 4 ProdHaftG) nachkommen. Die personenbezogenen Daten würden lediglich und ausschließlich im Falle von Produktwarn- oder -rückrufaktionen verwendet werden.

Eine Datenübermittlung ist zulässig, wenn dafür eine Rechtsgrundlage entsprechend Art. 5 Abs. 1 Buchst. a, Art. 6 DS-GVO besteht.

Auffassung des Unternehmens

Nach Auffassung des Unternehmens sei § 19 Abs. 5 Satz 3 SchfHwG in Verbindung mit § 22 Abs. 2 Satz 1 Nr. 2 HDSIG eine taugliche Rechtsgrundlage für die Datenübermittlung. Danach dürfen die personenbezogenen Daten aus dem Kehrbuch an nicht öffentliche Stellen nur übermittelt werden, soweit die Übermittlung nach dem Landesrecht zulässig ist und der Dritte, an den die Daten übermittelt werden, ein rechtliches Interesse an der Kenntnis der Daten und der Betroffene kein schutzwürdiges Interesse an dem Unterbleiben der Übermittlung hat.

§ 19 SchfHwG

(1) In das Kehrbuch sind die folgenden Daten einzutragen:

1. Vor- und Familienname sowie Anschrift

a) des Eigentümers und, falls davon abweichend, des Besitzers oder

b) des Verwalters im Sinne des Wohnungseigentumsgesetzes im Fall von Wohnungseigentum und, wenn die Anlage zum Sondereigentum gehört, des Wohnungseigentümers und, wenn davon abweichend, des Besitzers, oder

c) der Wohnungseigentümer, wenn kein Verwalter bestellt ist, und, wenn abweichend, der Besitzer;

2. Angaben zur Anlage hinsichtlich:

a) Art, Brennstoff, Nennwärmeleistung, Alter sowie die Angabe, ob es sich um einen Niedertemperatur-Heizkessel oder Brennwertkessel im Sinne des Gebäudeenergiegesetzes handelt,

b) Betrieb, Standort und Zuweisung zur Abgasanlage,

c) Angaben der Eigentümer zu Ausnahmetatbeständen nach den §§ 71 bis 71m, 72 und 73 sowie 102 des Gebäudeenergiegesetzes, auch in Verbindung mit § 69 des Gebäudeenergiegesetzes, sowie Angaben darüber, dass entsprechende Nachweise vorgelegen haben, und

d) im Falle von Einzelraumfeuerungsanlagen für feste Brennstoffe, die vor dem 22. März 2010 errichtet und in Betrieb genommen wurden, Angabe der Rechtsgrundlage für die Zulässigkeit des Weiterbetriebs nach § 26 der Verordnung über kleine und mittlere Feuerungsanlagen;

3. *die nach den Rechtsverordnungen nach § 1 Abs. 1 Satz 2 und 3 und die nach der Verordnung über kleine und mittlere Feuerungsanlagen vorgeschriebenen und nach § 14a festgesetzten Arbeiten und das Datum der Ausführung;*
4. *das Datum und das Ergebnis der letzten beiden Feuerstättenschauen sowie der Name der durchführenden Person;*
5. *in dem Formblatt nach § 4 vermerkte Mängel oder selbst festgestellte Mängel sowie Beanstandungen nach § 97 Absatz 1, 2 und 4 des Gebäudeenergiegesetzes und das Datum des Abstellens der Mängel oder der Beanstandungen;*
6. *das Datum und das Ergebnis einer Bescheinigung nach § 16 Absatz 1 sowie Name und Stellung der feststellenden Person;*
7. *der Anlass, das Datum und das Ergebnis einer Überprüfung nach § 15 Satz 1;*
8. *die für die Aufstellung von Emissionskatastern im Sinne des § 46 des Bundes-Immissionsschutzgesetzes erforderlichen Angaben nach Maßgabe der öffentlich-rechtlichen Vorschriften auf dem Gebiet des Immissionsschutzes.*

Soweit die in Satz 1 genannten Daten den bevollmächtigten Bezirksschornsteinfegern nicht ohnehin auf Grund ihrer Tätigkeit bekannt sind, entnehmen sie die Daten den ausgefüllten Formblättern nach § 4.

(5) Bevollmächtigte Bezirksschornsteinfeger verarbeiten die Daten nach Absatz 1, soweit das zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlich ist. Personenbezogene Daten aus dem Kehrbuch werden an die zuständige Behörde übermittelt, wenn und soweit dies zur Erfüllung der Aufgaben dieser Behörde nach diesem Gesetz erforderlich ist; im Übrigen werden Daten an öffentliche Stellen übermittelt, soweit das Landesrecht dies zulässt. An nicht öffentliche Stellen dürfen die Daten nur übermittelt werden, soweit

1. *die Übermittlung nach dem Landesrecht zulässig ist und*
2. *der Dritte, an den die Daten übermittelt werden, ein rechtliches Interesse an der Kenntnis der Daten und der Betroffene kein schutzwürdiges Interesse an dem Unterbleiben der Übermittlung hat.*

Die Verordnung (EU) 2016/679 bleibt unberührt.

§ 22 HDSIG

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

1. *sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden,*
2. *der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder*
3. *es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.*

Es gehe nicht darum, Produktwarnungen oder -rückrufe für ein Unternehmen wirtschaftlich günstiger zu gestalten, sondern die Betroffenen im konkreten Fall in angemessener Zeit erreichen zu können. Das von dem Unternehmen glaubhaft zu machende berechtigte Interesse sei die Verpflichtung zu der Gefahrenabwehr (Sicherheit der jeweils betroffenen Endkunden sowie etwaiger Dritter, zu deren Schutz das Unternehmen zu der Umsetzung entsprechender Rückrufe und Maßnahmen gesetzlich verpflichtet sei). Die Übermittlung der personenbezogenen Daten solle ausschließlich zum Schutz der Endkunden (und damit der betroffenen Personen) sowie zum Schutz der Rechte und Freiheiten anderer Personen (von eventuellen Konsequenzen nicht behobener Gefahren betroffene Dritte) erfolgen, um ganz konkret Gefahren für Leib, Leben und Eigentum abzuwenden. Ein entgegenstehendes schutzwürdiges Interesse der Betroffenen bestehe nicht. Ein Interesse, dass die Kontaktdaten eines Anlagenbetreibers im konkreten Fall eines Rückrufs oder sonstiger Maßnahmen zu der Gefahrenabwehr nicht an den Hersteller gegeben werden sollten, sei nicht ersichtlich. Selbst wenn ein solches angenommen werden sollte, dürfte es auch kein schutzwürdiges Interesse sein, weil es im konkreten Fall nur um Maßnahmen zu der Gefahrenabwehr gehen würde.

Die Regelung des § 1 Abs. 2 HDSIG sperre die Anwendung des § 22 Abs. 2 Satz 1 Nr. 2 HDSIG nicht vollständig. § 19 Abs. 5 Satz 3 SchfHwG treffe keine abschließende Regelung, sondern verweise pauschal auf die Zulässigkeit nach Landesrecht. Damit komme nach § 1 Abs. 2 Satz 2 HDSIG wieder das HDSIG zur Anwendung.

§ 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.

Datenschutzrechtliche Bewertung

Die seitens des Unternehmens genannten Aspekte kann ich grundsätzlich nachvollziehen. Gleichwohl besteht keine Rechtsgrundlage für die Datenübermittlung. Die Vorschrift des § 19 Abs. 5 Satz 3 SchfHwG stellt eine bereichsspezifische Datenschutzregelung des Bundes dar. Der dortige Verweis auf das Landesrecht („soweit die Übermittlung nach dem Landesrecht zulässig ist“) erfordert eine entsprechende bereichsspezifische Datenschutzregelung

des Landes. Eine solche Regelung gibt es in Hessen jedoch nicht. Ein ergänzender Rückgriff auf die allgemeine Regelung des § 22 Abs. 2 HDSIG ist nicht zulässig. Die Anwendbarkeit des § 22 Abs. 2 Satz 1 Nr. 2 HDSIG ist grundsätzlich gemäß § 1 Abs. 2 HDSIG gesperrt. Zudem ist § 19 Abs. 5 S. 3 SchfHwG ausweislich der Gesetzesbegründung (BT-Drs. 16/9794, Satz 18) restriktiv auszulegen: *„Die Möglichkeit der Übermittlung von Daten an nicht öffentliche Stellen wird erheblich eingeschränkt. Es genügt nicht, dass der Dritte ein rechtliches Interesse glaubhaft macht. Die übermittelnde Stelle muss vielmehr die volle Überzeugung gewinnen, dass der Dritte ein rechtliches Interesse an der Kenntnis der Daten hat. Dies ist eine hohe Schwelle."*

Selbst wenn die Regelung des § 22 Abs. 2 Satz 1 Nr. 2 HDSIG anwendbar wäre, würde dies keine Pflicht zu der Übermittlung personenbezogener Daten (also keinen Herausgabeanspruch Dritter gegenüber den Bezirksschornsteinfegern) begründen, sondern eine im Ermessen der Bezirksschornsteinfeger stehende Befugnis. Äußerst zweifelhaft ist dann auch die Erforderlichkeit hinsichtlich der Übermittlung von Kundendaten „auf Vorrat". Als milderes Mittel kommt etwa die Kontaktaufnahme zu den unmittelbaren Abnehmern des Herstellers, die ihrerseits ihre Kunden informieren können, soweit eine Gefahr tatsächlich besteht, in Betracht. Die Kunden verfügen überdies in aller Regel nicht über die notwendige Fachkenntnis, um das Vorhandensein des mangelhaften Bauteils in ihrer Heizungsanlage oder dessen potenzielle Gefährlichkeit einschätzen zu können.

Da auch keine andere Rechtsgrundlage diese Datenübermittlung legitimieren kann, ist sie nicht zulässig. Insbesondere ist eine Übermittlung aufgrund berechtigter Interessen gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO nicht möglich. Bezirksschornsteinfeger sind als Beliehene (s. § 8 SchfHwG) gemäß § 2 Abs. 1 Satz 2 HDSIG eine öffentliche Stelle. Damit können sie sich ausweislich Art. 6 Abs. 1 UAbs. 2 DS-GVO nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO berufen.

§ 8 SchfHwG

(1) Bevollmächtigter Bezirksschornsteinfeger ist, wer von der zuständigen Behörde für einen Bezirk bestellt ist.

(2) Die bevollmächtigten Bezirksschornsteinfeger gehören als Gewerbetreibende dem Schornsteinfegerhandwerk an. Sie üben ihre hoheitlichen Tätigkeiten als natürliche Personen aus und unterliegen auch hinsichtlich der hoheitlichen Tätigkeiten der Rolleneintragungspflicht nach der Handwerksordnung.

§ 2 HDSIG

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

Art. 6 DS-GVO

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

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

6.4
Meldedatenweitergabe an den Beitragsservice und das Auskunftsrecht

Die Datenübermittlung von Meldebehörden an den Beitragsservice ist grundsätzlich zulässig. Das Auskunftsrecht ermöglicht eine Überprüfung der Rechtmäßigkeit dieser Verarbeitung für betroffene Personen.

Im Berichtszeitraum erreichten mich mehrere Anfragen und Beschwerden, die eine Datenübermittlung von Meldebehörden an den Beitragsservice betrafen. An den Beitragsservice müssen Bürgerinnen und Bürger den Rundfunkbeitrag entrichten. Es kursieren verschiedene (Muster-)Schreiben, mit denen den Meldebehörden eine rechtswidrige Übermittlung von Meldedaten an den Beitragsservice vorgeworfen und der Auskunftsanspruch nach Art. 15 DS-GVO geltend gemacht wird. Nachfolgend möchte ich die rechtlichen Maßgaben erläutern.

Datenübermittlung von Meldebehörden an den Beitragsservice

Die Übermittlung von Meldedaten der Meldebehörden an den Beitragsservice stellt eine grundsätzlich zulässige Datenverarbeitung dar. Diese ist gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. c, Abs. 2 und Abs. 3 DS-GVO in Verbindung mit § 15 Abs. 1 MeldDüV rechtmäßig. Danach übermittelt die Meldebehörde

nach § 11 Abs. 4 RStV dem Hessischen Rundfunk oder der von ihm aufgrund des § 10 Abs. 7 Satz 2 Rundfunkbeitragsstaatsvertrag (RStV) beauftragten Stelle automatisiert mehrere personenbezogene Daten (Familienname, Vornamen, Anschrift etc.). Diese Übermittlung dient dem Zweck festzustellen, ob eine Beitragspflicht besteht und welcher Landesrundfunkanstalt der Beitrag zusteht, sowie den Beitrag zu erheben. Die Übermittlungspflicht entsteht mit der Anmeldung, Abmeldung oder dem Tod von volljährigen Einwohnerinnen und Einwohnern, soweit keine Auskunftssperre nach § 51 Bundesmeldegesetz eingetragen ist. Aufgrund der bestehenden rechtlichen Verpflichtung ist die Datenübermittlung rechtmäßig.

§ 15 MeldDüV

(1) Die Meldebehörde übermittelt dem Hessischen Rundfunk oder der von ihm aufgrund des § 10 Abs. 7 Satz 2 des Rundfunkbeitragsstaatsvertrages vom 15. bis 21. Dezember 2010 (GVBl. I 2011, S. 382), zuletzt geändert durch Staatsvertrag vom 14. bis 28. April 2020 (GVBl. S. 607), beauftragten Stelle zum Zwecke der Beitragserhebung sowie zur Feststellung, ob eine Beitragspflicht besteht und welcher Landesrundfunkanstalt der Beitrag zusteht, nach § 11 Abs. 4 des Rundfunkbeitragsstaatsvertrages im Falle der Anmeldung, Abmeldung oder des Todes von volljährigen Einwohnerinnen und Einwohnern, soweit keine Auskunftssperre nach § 51 des Bundesmeldegesetzes eingetragen ist, automatisiert folgende Daten:

1. *Familienname*
2. *frühere Namen*
3. *Vornamen*
4. *Doktorgrad*
5. *Geburtsdatum*
6. *gegenwärtige und letzte Anschrift von Haupt- und Nebenwohnungen, einschließlich aller vorhandenen Angaben zur Lage der Wohnung*
7. *Einzugsdatum, Auszugsdatum*
8. *Familienstand*
9. *bedingter Sperrvermerk nach § 52 des Bundesmeldegesetzes*
10. *Sterbedatum*

(2) Der Hessische Rundfunk und die von ihm aufgrund des § 10 Abs. 7 Satz 2 des Rundfunkbeitragsstaatsvertrages beauftragte Stelle haben durch technische und organisatorische Maßnahmen sicherzustellen, dass die Daten nur berechtigten Bediensteten zur rechtmäßigen Aufgabenerfüllung zur Kenntnis gelangen. Die erhobenen Daten sind unverzüglich zu löschen, wenn feststeht, dass sie nicht mehr benötigt werden oder eine Beitragspflicht dem Grunde nach nicht besteht. Nicht überprüfte Daten sind spätestens nach zwölf Monaten zu löschen.

Auskunftsrecht

Betroffene Personen können mit ihrem Auskunftsrecht nach Art. 15 DS-GVO in Erfahrung bringen, ob die Datenübermittlung an den Beitragsservice den oben genannten rechtlichen Maßgaben entsprochen hat. Damit wird die Datenverarbeitung transparent und Betroffene werden in die Lage versetzt, die Rechtmäßigkeit der Datenübermittlung zu überprüfen.

Im Berichtszeitraum hat die Geltendmachung des Auskunftsrechts durch betroffene Personen gegenüber Kommunen – nicht nur in der dargestellten Konstellation der Übermittlung an den Beitragsservice – stark zugenommen. Oftmals verlangen betroffene Personen umfangreiche Kopien von Dokumenten, die ihre personenbezogenen Daten enthalten. Dies stellt Kommunen in der Praxis teilweise vor große Herausforderungen. Zur Unterstützung bei der Erfüllung des komplexen Anspruchs biete ich Kommunen die Handreichung „Auskunftsrecht gemäß Art. 15 DS-GVO gegenüber Kommunen“ an, die auf meiner Webseite abrufbar ist (s. https://datenschutz.hessen.de/datenschutz/kommunen/auskunftsrecht-gemaess-art-15-ds-gvo-gegenueber-kommunen).

6.5
Verantwortlichkeit bei Nutzung länderübergreifender Online-Dienste

Obgleich das Onlinezugangsgesetz (OZG) hilfreiche Klarstellungen zum Datenschutz bei länderübergreifenden Onlinediensten geschaffen hat, bleiben auf Landesebene zur datenschutzrechtlichen Verantwortlichkeit Fragen offen, die zwischen den Beteiligten der hessischen Landes- und Kommunalverwaltung zu klären sind. Der Beitrag veranschaulicht die Thematik am Beispiel des elektronischen Wohngeldverfahrens.

Wohngeldverfahren

Das Wohngeld dient nach § 1 Wohngeldgesetz (WoGG) der wirtschaftlichen Sicherung angemessenen und familiengerechten Wohnens. Wenn das Einkommen einer Person nicht ausreichend ist, um für die Miete der Wohnung aufzukommen, kann für diese nach den Regelungen des WoGG ein Anspruch auf Wohngeld bestehen. Sie können einen Antrag auf Wohngeld stellen (Antragsteller).

§ 1 WoGG

(1) Das Wohngeld dient der wirtschaftlichen Sicherung angemessenen und familiengerechten Wohnens.

(2) Das Wohngeld wird als Zuschuss zur Miete (Mietzuschuss) oder zur Belastung (Lastenzuschuss) für den selbst genutzten Wohnraum geleistet.

Zuständige Wohngeldbehörde

Zuständig für die Bearbeitung des Wohngeldantrags sind nach § 24 Abs. 1 WoGG die Wohngeldbehörden. Nach § 1 des hessischen Wohngeldzuständigkeitsgesetzes (WoGZustG) i. V. m. § 1 der hessischen Wohngeldzuständigkeitsverordnung (WoGZustV) sind die Wohngeldbehörden in Hessen die Magistrate der kreisfreien Städte und die Kreisausschüsse der Landkreise sowie die Städte Bad Homburg vor der Höhe, Hanau, Marburg, Rüsselsheim am Main und Wetzlar. Eine Übersicht der hessischen Wohngeldbehörden findet sich auf der Webseite des Hessischen Ministeriums für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum (HMWEVW, https://wirtschaft.hessen.de/wohnen-und-bauen/wohngeld).

§ 1 WoGZustG

Die Landesregierung wird ermächtigt, durch Rechtsverordnung die nach § 24 Abs. 1 des Wohngeldgesetzes vom 24. September 2008 (BGBl. I S. 1856), zuletzt geändert durch Gesetz vom 22. Dezember 2023 (BGBl. 2023 I Nr. 408), zuständigen Stellen für die Durchführung des Wohngeldgesetzes zu bestimmen.

§ 1 WoGZustV

(1) Wohngeldbehörden im Sinne des § 24 Abs. 1 Satz 1 des Wohngeldgesetzes sind die Magistrate der kreisfreien Städte und die Kreisausschüsse der Landkreise. Sie erfüllen diese Aufgabe nach Weisung im Sinne des § 4 Abs. 1 der Hessischen Gemeindeordnung und des § 4 Abs. 1 der Hessischen Landkreisordnung.

(2) Abweichend von Abs. 1 wird die Wahrnehmung der Aufgabe nach Abs. 1 den Magistraten der Städte Bad Homburg vor der Höhe, Hanau, Marburg, Rüsselsheim am Main und Wetzlar jeweils für ihren Bereich übertragen.

Elektronisches Wohngeldverfahren

Das Wohngeld kann vom Antragsteller über den Onlinedienst Wohngeld auch elektronisch beantragt werden.

Der Onlinedienst Wohngeld wurde nach dem „Einer-für-Alle“-Prinzip (EfA-Prinzip) durch das Bundesland Schleswig-Holstein und dessen IT-Dienstleister (Dataport) entwickelt (s. Anbindungsleitfaden für den EfA Online-Dienst Wohngeld vom 21. März 2022, https://www.fitko.de/fileadmin/user_upload/03b_Anbindungsleitfaden_Wohngeld.pdf). Er wird den Wohngeldbehörden der

anderen Bundesländer zur Nachnutzung angeboten. Auch die hessischen Wohngeldbehörden sind an den Onlinedienst Wohngeld angeschlossen (Pressemitteilung des HMWEVW vom 27. Dezember 2023, https://hessen.de/presse/pressearchiv/antrag-auch-digital-moeglich).

Unterscheidung zwischen Onlinedienst Wohngeld und Wohngeldfachverfahren

Wichtig ist in diesem Zusammenhang, zwischen zwei Komponenten des elektronischen Wohngeldverfahrens zu unterscheiden: dem Frontend und dem Backend.

Als Frontend wird die Oberfläche (Webseite) bezeichnet, mit der der Benutzer (Antragsteller) interagiert. Die Frontend-Komponente ist diejenige, die zuvor als Onlinedienst Wohngeld beschrieben wurde. Beim Frontend des elektronischen Wohngeldverfahrens (Onlinedienst Wohngeld) handelt es sich um einen länderübergreifenden Onlinedienst i. S. d. § 2 Abs. 8 OZG.

§ 2 Abs. 8 OZG

(8) Ein „Onlinedienst" ist eine IT-Komponente, die ein eigenständiges elektronisches Angebot an die Nutzer darstellt, welches die Abwicklung einer oder mehrerer elektronischer Verwaltungsleistungen von Bund oder Ländern ermöglicht. Der Onlinedienst dient dem elektronischen Ausfüllen der Online-Formulare für Verwaltungsleistungen von Bund oder Ländern, der Offenlegung dieser Daten an die zuständige Fachbehörde sowie der Übermittlung elektronischer Dokumente und Informationen zu Verwaltungsvorgängen an die Nutzer, gegebenenfalls unter Einbindung von Nutzerkonten einschließlich deren Funktion zur Übermittlung von Daten aus einem Nutzerkonto an eine für die Verwaltungsleistung zuständige Behörde. Der Onlinedienst kann auch verfahrensunabhängig und länderübergreifend, insbesondere in der Verantwortung einer Landesbehörde zur Nutzung durch weitere Länder, bereitgestellt werden.

Der Onlinedienst Wohngeld wird vom Antragsteller über das Serviceportal des Landes Schleswig-Holstein aufgerufen. Um den Dienst nutzen zu können, erfolgt die Registrierung und Anmeldung des Antragstellers über die Antragsmaske des Onlinedienstes. Nach Eingabe der für die Antragstellung erforderlichen Daten kann der Antrag abgeschlossen und versandt werden. Der Antragsteller kann den Antrag im Portable Document Format (PDF) speichern und ausdrucken. Die Interaktion des Antragstellers mit dem – nach dem EfA-Prinzip entwickelten und den Regelungen des OZG unterfallenden – Onlinedienst Wohngeld (Frontend) ist damit abgeschlossen.

Als Backend bezeichnet man die funktionale Komponente des digitalen Dienstes. Im Backend findet die eigentliche Bearbeitung des elektronischen

Wohngeldantrags statt. Über eine Schnittstelle kommuniziert der Onlinedienst Wohngeld (Frontend) nach erfolgreicher Antragstellung mit dem hessischen Wohngeldfachverfahren (eWoG/Backend). Hierfür wird das vom Antragsteller ausgefüllte Wohngeldantragsformular an das Wohngeldfachverfahren (eWoG) übermittelt.

Das Wohngeldfachverfahren (eWoG) wird von der Hessischen Zentrale für Datenverarbeitung (HZD), dem zentralen Dienstleister für Informations- und Kommunikationstechnik der Hessischen Landesverwaltung, betrieben und von den Wohngeldbehörden genutzt. Sobald der Antrag im Wohngeldfachverfahren (eWoG) der HZD eingegangen ist, erhält der Antragsteller automatisiert per E-Mail-Nachricht eine Bestätigung über den Antragseingang bei der zuständigen hessischen Wohngeldbehörde. Die weitere Kommunikation erfolgt sodann direkt zwischen der zuständigen kommunalen Wohngeldbehörde und dem Antragsteller. Diese nutzt für die Bearbeitung des Antrags das Wohngeldfachverfahren (eWoG).

Rolle des HMWEVW im elektronischen Wohngeldverfahren

Das HMWEVW ist als oberste Landesbehörde zuständig für das Wohnungswesen und erfüllt folgende Aufgaben:

– Es beschafft den nach dem EfA-Prinzip entwickelten und dem OZG unterfallenden Onlinedienst Wohngeld (Frontend) und stellt den Dienst der HZD und den Wohngeldbehörden zur Nachnutzung kostenlos zur Verfügung.
– Es nimmt am Steuerungskreis des Onlinedienstes Wohngeld teil und kann in dieser Rolle Anforderungen zur Weiterentwicklung des Onlinedienstes Wohngeld (Frontend) an das Land Schleswig-Holstein kommunizieren.
– Es ist Auftraggeber für den Betrieb, die Wartung und Pflege sowie die Weiterentwicklung des Wohngeldfachverfahrens (eWoG/Backend) bei der HZD und dessen kostenlose Bereitstellung gegenüber den hessischen Wohngeldbehörden.
– Es ist nach § 3 WoGZustV oberste Fachaufsichtsbehörde für das Wohngeld.
– Es ist an der Setzung von Rechtsvorschriften bezüglich der Durchführung des Wohngeldverfahrens beteiligt.

Hintergrund zur Klärung der Frage der datenschutzrechtlichen Verantwortlichkeit

Im Berichtsjahr erreichten mich Hinweise darauf, dass es bei dem elektronischen Wohngeldverfahren zu einem Vorfall und dadurch zu einer Verletzung des Schutzes personenbezogener Daten i. S. d. Art. 4 Nr. 12 DS-GVO gekommen sein könnte.

Art. 4 Nr. 12 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck: (…)

12. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, (…)

Durch diesen Vorfall seien Wohngeldanträge von ca. 100 betroffenen Personen verloren gegangen. Indem offenbar die Verfügbarkeit personenbezogener Daten in Form der Anträge gefährdet und ein unbeabsichtigter Verlust dieser Daten im Zuge der Verarbeitung eingetreten war, erfüllte der Vorfall die Voraussetzungen einer Verletzung des Schutzes personenbezogener Daten i. S. d. Art. 4 Nr. 12 DS-GVO.

Eine Verletzung des Schutzes personenbezogener Daten kann für den nach Art. 4 Nr. 7 DS-GVO datenschutzrechtlich Verantwortlichen Meldepflichten zur Aufsichtsbehörde gemäß Art. 33 DS-GVO sowie Informationspflichten gegenüber Betroffenen nach Art. 34 DS-GVO auslösen.

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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden; (…)

Art. 33 Abs. 1 DS-GVO

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. (…)

Art. 34 Abs. 1 DS-GVO

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung. (…)

Der Verantwortliche hätte somit eine Risikobewertung anstellen und prüfen müssen, ob er den Vorfall meiner Behörde gemäß Art. 33 Abs. 1 DS-GVO unverzüglich melden und die betroffenen Personen gemäß Art. 34 Abs. 1 DS-GVO benachrichtigen musste. Eine Meldung nach Art. 33 Abs. 1 DS-GVO lag mir jedoch auch 72 Stunden nach Bekanntwerden des Vorfalls nicht vor. Gleichzeitig ergab meine erste Einschätzung, dass es wegen der möglichen finanziellen Schäden für die betroffenen Personen eher unwahrscheinlich wäre, dass dieser Vorfall nicht zu einem Risiko für ihre Rechte und Freiheiten führen würde, so dass ich einen Anfangsverdacht dafür hatte, dass das HMWEVW als potenziell datenschutzrechtlich Verantwortlicher gegen seine Melde- und Informationspflichten nach Art. 33 und 34 DS-GVO verstoßen haben könnte.

Daher startete ich eine darauf gerichtete Überprüfung und befragte das Ministerium u. a. dazu, wann und auf welchem Weg es von dem Vorfall erfahren hatte, welche personenbezogenen Daten genau betroffen waren, welche Folgen für die betroffenen Personen wahrscheinlich waren und aus welchem Grund keine Meldung gegenüber meiner Behörde erfolgt war.

Die Zusammenarbeit des HMWEVW mit mir war durchweg positiv. Meine Fragen wurden fristgemäß und ausführlich beantwortet. Mit Blick auf die Frage der Verantwortlichkeit gab das HMWEVW aber zu verstehen, dass es sich für das Verfahren nicht als datenschutzrechtlich Verantwortlicher erachtete. Dies begründete das HMWEVW damit, dass der nach dem EfA-Prinzip entwickelte Onlinedienst Wohngeld der Vorschrift des § 8a OZG unterfalle und das HMWEVW insoweit lediglich als Intermediär für die zentrale Beschaffung des Verfahrens für das Land Hessen tätig werde. Für das Wohngeldfachverfahren (eWoG) verwies das HMWEVW ebenfalls auf seine Rolle als Intermediär. Es führte aus, dass lediglich die Betriebs-, Entwicklungs-, Wartungs- und Pflegekosten für das Wohngeldfachverfahren übernommen würden. Es selbst habe aber keinerlei Zugriff auf die Daten im Wohngeldfachverfahren, so dass es als datenschutzrechtlich „unbeteiligt“ anzusehen sei.

Aufgrund der mir bekannten Informationen konnte ich nicht ausschließen, dass das HMWEVW – entgegen der dort vertretenen Rechtsauffassung – datenschutzrechtlich verantwortlich sein könnte, da es u. a. als übergeordnete Behörde der Wohngeldbehörden diesen gegenüber weisungsbefugt ist, die

oberste Fachaufsicht ausübt, an der Setzung von Rechtsvorschriften bezüglich der Durchführung des Wohngeldverfahrens beteiligt ist, sowohl den Onlinedienst Wohngeld als auch das Wohngeldfachverfahren (eWoG) zentral beschafft und als Anforderungsgeber beider Verfahren über die technische Ausgestaltung mitbestimmt.

Um die Sach- und Rechtslage zur Verantwortlichkeit des HMWEVW mit den Beteiligten diskutieren und einer Lösung zuführen zu können, habe ich einen gemeinsamen Termin mit dem HMWEVW und der HZD in meiner Dienststelle durchgeführt, um die Sach- und Rechtsfragen konstruktiv und lösungsorientiert zu diskutieren.

Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO

Wer aus datenschutzrechtlicher Sicht Verantwortlicher ist und damit ggf. die Melde- und Informationspflichten nach Art. 33 und 34 DS-GVO erfüllen muss, ergibt sich aus Art. 4 Nr. 7 DS-GVO. Demnach ist Verantwortlicher, wer über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Die Bestimmung der Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO kann in der Praxis Schwierigkeiten bereiten. Auch der EuGH hat sich daher bereits mehrfach mit den Merkmalen des Art. 4 Nr. 7 DS-GVO befasst. Der EDSA hat unter Berücksichtigung der Entscheidungen des EuGH umfangreiche Leitlinien zu den Begriffen Verantwortlicher und Auftragsverarbeiter erarbeitet (Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf, Version 2.0 vom 7. Juli 2021). Öffentliche und nicht-öffentliche Stellen können sich hieran bei der Bestimmung der Rolle als Verantwortlicher, gemeinsam Verantwortlicher und Auftragsverarbeiter orientieren.

Nicht nur die Bestimmung der Rolle des Verantwortlichen nach Art. 4 Nr. 7 DS-GVO bringt Herausforderungen mit sich. Als weitere Komplexitätsstufe kommt mit Blick auf das elektronische Wohngeldverfahren hinzu, dass zwischen dem nach dem EfA-Prinzip entwickelten und dem OZG unterfallenden Onlinedienst Wohngeld (Frontend) und dem von der HZD im Auftrag des HMWEVW betriebenen Wohngeldfachverfahren (eWoG) zu unterscheiden ist (Backend).

Verantwortlichkeit für den Onlinedienst Wohngeld

Wie sich aus der Definition des Art. 4 Nr. 7 HS 2 DS-GVO ergibt, kann die Rolle des Verantwortlichen auch durch eine Regelung des Unionsrechts oder

des Rechts der Mitgliedstaaten gesetzlich zugewiesen werden. Eine solche gesetzliche Verantwortungszuweisung enthält § 8a Abs. 4 OZG.

§ 8a Abs. 4 OZG

(4) Verantwortlicher im Sinne von Artikel 4 Nummer 7 der Verordnung (EU) 2016/679 für die Verarbeitung personenbezogener Daten im länderübergreifenden Onlinedienst nach den Absätzen 1 bis 3 ist ausschließlich die den länderübergreifenden Onlinedienst betreibende Behörde. Die datenschutzrechtliche Verantwortlichkeit der Behörde, an die zum Zwecke der Durchführung des Verwaltungsverfahrens personenbezogene Daten übermittelt werden, bleibt unberührt.

Für den Onlinedienst Wohngeld folgt hieraus, dass die im Land Schleswig-Holstein zuständige Behörde ausschließlicher Verantwortlicher i. S. v. Art. 4 Nr. 7 DS-GVO ist. Davon unberührt bleibt die datenschutzrechtliche Verantwortlichkeit der für die Durchführung des Verwaltungsverfahrens zuständigen Behörde. Beim Wohngeldverfahren handelt es sich hierbei um die nach § 1 WoGZustG i. V. m. § 1 WoGZustG zuständigen Behörden.

Die datenschutzrechtliche Verantwortlichkeit für länderübergreifende Onlinedienste ist durch § 8a Abs. 4 OZG somit erfreulich klar geregelt. Im Hinblick auf die Ausgangsfrage, ob das HMWEVW gegen die Melde- und Informationspflicht der Art. 33 und 34 DS-GVO verstoßen hat, ist daher festzustellen, dass ein solcher Verstoß mangels datenschutzrechtlicher Verantwortlichkeit für den Onlinedienst Wohngeld nicht vorliegt.

Hier hilft es, sich die technischen Abläufe zu verdeutlichen. Denn aus technischer Sicht stellt sich der Datenfluss so dar, dass die betroffenen Personen zunächst ihren Antrag auf Wohngeld über den Onlinedienst Wohngeld einreichten, der in Schleswig-Holstein als EfA-Dienst bereitgestellt wird. Die Anträge werden dort zwischengespeichert. Die ebenfalls dort betriebene Schnittstelle wird von der HZD regelmäßig angesprochen, um die bereitliegenden Anträge in das bei der HZD betriebene Wohngeldfachverfahren abzurufen, auf das letztlich dann die Wohngeldbehörden zur Antragsbearbeitung zugreifen. Im Zeitraum des Vorfalls waren bei der HZD im Kontext der Landtagswahlen technische Härtungsmaßnahmen vorgenommen worden, die für das Wohngeldverfahren unbeabsichtigte Nebenwirkungen hatten. Ein einmal gescheiterter Antragsabruf über die Schnittstelle wurde dadurch nicht wiederholt. So konnten die ca. 100 betroffenen Anträge in Verbindung mit einer vorübergehenden Störung verfallen, da der auf Seiten des Onlinedienst-Betreibers vorgesehene Zwischenspeicher mit einer Ablaufzeit versehen war, nach der die Antragsdaten – trotz unterbliebenen Antragsabrufs – gelöscht wurden.

Datenschutzrechtliche Fragen rund um länderübergreifende Onlinedienste wie den Onlinedienst Wohngeld behandelt auch die Orientierungshilfe zu ausgewählten Fragestellungen des OZG der DSK (Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG) Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen, https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG_Version_1_1.pdf, Version 1.1, Stand Dezember 2025).

Verantwortlichkeit für das Wohngeldfachverfahren

Das Wohngeldfachverfahren (Backend), das sich an den Onlinedienst Wohngeld (Frontend) anschließt, ist von der Regelung des § 8a Abs. 4 OZG nicht umfasst, da es sich nicht um einen länderübergreifenden Onlinedienst i. S. d. § 2 Abs. 8 OZG handelt.

§ 2 Abs. 8 OZG

(8) Ein „Onlinedienst" ist eine IT-Komponente, die ein eigenständiges elektronisches Angebot an die Nutzer darstellt, welches die Abwicklung einer oder mehrerer elektronischer Verwaltungsleistungen von Bund oder Ländern ermöglicht. Der Onlinedienst dient dem elektronischen Ausfüllen der Online-Formulare für Verwaltungsleistungen von Bund oder Ländern, der Offenlegung dieser Daten an die zuständige Fachbehörde sowie der Übermittlung elektronischer Dokumente und Informationen zu Verwaltungsvorgängen an die Nutzer, gegebenenfalls unter Einbindung von Nutzerkonten einschließlich deren Funktion zur Übermittlung von Daten aus einem Nutzerkonto an eine für die Verwaltungsleistung zuständige Behörde. Der Onlinedienst kann auch verfahrensunabhängig und länderübergreifend, insbesondere in der Verantwortung einer Landesbehörde zur Nutzung durch weitere Länder, bereitgestellt werden.

Die Bestimmung der Verantwortlichkeit muss für das Wohngeldfachverfahren somit nach Art. 4 Nr. 7 DS-GVO unter Berücksichtigung der Rechtsprechung des EuGH und der Leitlinien des Europäischen Datenschutzausschusses erfolgen. Da das HMWEVW den Betrieb, die Wartung und Pflege sowie die Weiterentwicklung des Wohngeldfachverfahrens (eWoG/Backend) bei der HZD beauftragt, die oberste Fachaufsichtsbehörde für das Wohngeld ist und an der Setzung von Rechtsvorschriften bezüglich der Durchführung des Wohngeldverfahrens beteiligt ist, wirkt es sowohl auf die Zwecke als auch auf die Mittel der Verarbeitung personenbezogener Daten bestimmend ein. Der Umstand, dass das HMWEVW keinen Zugang zu personenbezogenen Daten im Wohngeldfachverfahren hat, ist nach der Rechtsprechung des EuGH und den Leitlinien des EDSA unbeachtlich (EuGH, Urteil vom 5. Juni 2018, C-210/16, ECLI:EU:C:2018:388, Rn. 38 – Wirtschaftsakademie; EDSA,

Leitlinien 07/2020 zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_de.pdf, Version 2.0 vom 7. Juli 2021, Rn. 45).

Neben den Wohngeldbehörden ist daher auch das HMWEVW für das Wohngeldfachverfahren Verantwortlicher i. S. v. Art. 4 Nr. 7 DS-GVO. Sie sind nach Art. 26 DS-GVO gemeinsam Verantwortliche und müssen daher in einer Vereinbarung festlegen, wer von ihnen welche Verpflichtung nach der DS-GVO erfüllt.

Der HZD kommt als Dienstleister für Informations- und Kommunikationstechnik der Hessischen Landesverwaltung die Rolle des Auftragsverarbeiters i. S. d. Art. 4 Nr. 8 i. V. m. Art. 28 DS-GVO zu. Das Datenverarbeitungsverbundgesetz (DV-VerbundG), das in § 1 Abs. 2 DV-VerbundG unter anderem die datenschutzrechtliche Rolle der HZD regelt, stellt insoweit ein anderes Rechtsinstrument i. S. d. Art. 28 Abs. 3 DS-GVO dar.

Art. 26 Abs. 1 DS-GVO

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt, sofern und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der Union oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind. In der Vereinbarung kann eine Anlaufstelle für die betroffenen Personen angegeben werden.

Art. 4 Nr. 8 DS-GVO

8. „Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

Art. 28 Abs. 1 und 3 DS-GVO

(1) Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. (…)

(3) Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, der bzw. das den Auftragsverarbeiter in Bezug auf den Verantwortlichen

bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind.

§ 1 Abs. 1 und 2 DV-VerbundG

(1) Die Hessische Zentrale für Datenverarbeitung ist zentraler Dienstleister für Informations- und Kommunikationstechnik für alle Behörden, Gerichte und sonstigen öffentlichen Stellen des Landes Hessen. Sie arbeitet mit den Kommunalen Gebietsrechenzentren zusammen.

(2) Die Hessische Zentrale für Datenverarbeitung kann durch die Landesregierung oder die jeweils zuständige Landesbehörde bei zentralen oder sonstigen gemeinsamen Verfahren beauftragt werden, verbindlich für alle beteiligten Stellen des Landes den Betrieb des Verfahrens zur automatisierten Datenverarbeitung als Auftragsnehmerin im Sinne des Art. 28 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) (ABI. EU Nr. L 119 S. 1, Nr. L 314 S. 72, 2018 Nr. L 127 S. 2) und des § 57 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes vom 3. Mai 2018 (GVBI. S. 82), geändert durch Gesetz vom 12. September 2018 (GVBI. S. 570), durchzuführen. Zur Erfüllung der nach diesem Gesetz vorgesehenen Aufgaben unterhält und pflegt sie ein auf das jeweilige Verfahren abgestimmtes Betriebshandbuch, aus dem sich die nach Art. 28 Datenschutz- Grundverordnung erforderlichen Garantien, Rechte und Pflichten eines Auftragsverarbeiters ergeben.

Im Rahmen des gemeinsamen Gesprächstermins des HMWEVW, der HZD und mir wurde bezüglich des Wohngeldfachverfahrens herausgearbeitet, dass das HMWEVW seinerseits Auftraggeber der HZD ist. Für die Thematik der gemeinsamen Verantwortlichkeit des HMWEVW und der Wohngeldbehörden bezüglich des Wohngeldfachverfahrens wurde in Abstimmung mit mir ein Vertragsentwurf vorbereitet. Mit diesem geht das HMWEVW auf die hessischen Wohngeldbehörden zur Unterzeichnung zu.

Problemlösung durch Zusammenarbeit

Der Fall zeigt, dass die Beantwortung datenschutzrechtlicher Fragestellungen erhebliche Komplexitäten mit sich bringen kann und der „Teufel häufig im (technischen und juristischen) Detail steckt“. Er ist aber auch ein positives Beispiel. Denn er zeigt auf, dass mit einer offenen, konstruktiven und lösungsorientierten Herangehensweise aller Beteiligten datenschutzrechtliche Fragen abschließend, rechtssicher und mit vertretbarem Aufwand geklärt werden können.

7. Schulen, Hochschulen, Archiv

Das Hessische Landesarchiv bewahrt Dokumente auf, die für das Verständnis der gesellschaftlichen und politischen Entwicklung Hessens von Bedeutung sein können. Dadurch steht die Archivierung in einem Spannungsverhältnis zum Datenschutz (Kap. 7.1). Zur Unterstützung langfristig kranker Kinder werden in manchen hessischen Schulen Avatare eingesetzt, die diese Kinder im Klassenzimmer vertreten sollen. Hierzu wird erläutert, unter welchen Voraussetzungen dies datenschutzrechtlich zulässig ist (Kap. 7.2).

7.1
Handreichung Löschsurrogat des Hessischen Landesarchivs

Im Berichtsjahr habe ich Vertreter des Hessischen Landesarchivs dabei unterstützt, die Handreichung Löschsurrogat des Hessischen Landesarchivs zu erarbeiten. Eine besondere Herausforderung lag darin, sowohl den Interessen des Archivs als auch dem Datenschutz gerecht zu werden.

Zielsetzung des Landesarchivs

Wie in § 1 HArchivG zu lesen ist, regelt das HArchivG die Anbietung und Archivierung von Unterlagen in den Archiven des Landes. Es soll das öffentliche Archivgut als Kulturgut vor Beschädigung, Verlust, Vernichtung und Zersplitterung schützen und stellt seine Nutzung sicher. Zugleich soll es die Nachvollziehbarkeit von Verwaltungshandeln gewährleisten, eine authentische Überlieferung zur Geschichte des Landes Hessen in seiner Vielfalt nachhaltig sichern und sein kulturelles Erbe bewahren. Dies soll vor dem Hintergrund der Einhaltung datenschutzrechtlicher Vorschriften geschehen. Das HArchivG selbst weist einige Regelungen zum Datenschutz auf, die allerdings auch Spielraum zur Interpretation lassen.

Spannungsfeld zum Datenschutz

Beispielsweise führt das Verhältnis zwischen archivgesetzlicher Anbietungspflicht und ggf. bestehenden Löschpflichten immer wieder zu Unsicherheiten bei den Rechtsanwendern. Sie stellen sich die Frage, ob Unterlagen, die nach dem Unions-, Bundes- oder Landesrecht gelöscht werden müssten oder könnten, dennoch dem zuständigen Archiv anzubieten sind.

Archivrechtliche Anbietungspflicht

Grundsätzlich sind gemäß § 4 Abs. 1 HArchivG sämtliche Unterlagen, die in den in § 2 Abs. 6 und 7 HArchivG genannten Stellen (wie beispielsweise

Behörden, Gerichten und sonstigen öffentlichen Stellen) entstanden sind, nach Ablauf der Aufbewahrungsfrist dem zuständigen Staatsarchiv anzubieten. Dies schließt personenbezogene Daten ausdrücklich mit ein. Die Vernichtung von Unterlagen oder die Löschung von Daten ist gemäß § 4 Abs. 3 HArchivG nur dann zulässig, wenn das zuständige Archiv diese zur Vernichtung oder Löschung freigegeben hat. Dem stehen die geltenden datenschutzrechtlichen Vorschriften grundsätzlich nicht entgegen. Die DS-GVO enthält zahlreiche Regelungen, die dem Schutz personenbezogener Daten dienen. Es gibt jedoch auch eine Öffnungsklausel („Archivprivileg“) in Art. 89 der DS-GVO, die eine Weiterverarbeitung personenbezogener Daten im Archiv grundsätzlich zulässt.

Löschsurrogat

In vielen Fällen tritt demnach die Archivierung der Unterlagen an die Stelle der Löschung dieser Daten, was als sogenanntes Löschsurrogat (Löschungsersatz) bezeichnet wird.

In der Praxis nutzen Archive die Option, mit einer weitreichenden Kassationserlaubnis die Löschung von Daten bei den aktenführenden Stellen während der Aktenführung und eine Aufbewahrungsfrist ohne Anbietung zu ermöglichen. Grundsätzlich gilt bei der Aktenführung bis zur Anbietung der Unterlagen die Löschpflicht nach Art. 17 Abs. 1 DS-GVO durch die aktenführende Stelle. Eine Löschung darf während der Bearbeitung oder während der Aufbewahrungsfrist, beispielsweise aufgrund einer widerrufenen Einwilligung (Art. 17 Abs. 1 Buchst. b DS-GVO) oder der unrechtmäßigen Verarbeitung personenbezogener Daten (Art. 17 Abs. 1 Buchst. d) DS-GVO), nicht unterlassen werden. Insbesondere kann auch eine Löschung zur Erfüllung einer rechtlichen Verpflichtung gemäß Art. 17 Abs. 1 Buchst. e DS-GVO erforderlich sein, etwa wenn spezialgesetzliche Vorgaben eine Löschung verlangen, während die Vorgangsbearbeitung noch andauert.

Die rechtlich anerkannte, umfängliche Ersatzwirkung der Archivierung findet sich auch in der Ausgestaltung des hessischen Aktenführungserlasses in Anlage D wieder, in der es heißt: „Die Anbietungspflicht für Personalakten schließt insbesondere auch alle Unterlagen über Beurteilungen, Befähigungen und Disziplinarvorgänge mit ein.“

Nach Ablauf der Aufbewahrungsfrist sind Unterlagen dem Archiv so anzubieten, wie sie zu diesem Zeitpunkt bestehen, ggf. also auch inklusive noch zur Löschung anstehender Teile. Ab der Anbietung besteht der Vorrang des Löschsurrogats nach Art. 17 Abs. 3 Buchst. d DS-GVO in der Übergabe durch die aktenführende Stelle an das zuständige Archiv. Nach der Übergabe wird

die Löschung durch die Archivierung ersetzt. Ein Antrag auf Löschung hat dann keinen Erfolg mehr.

Aufbewahrungsfrist und Anbietung

Aufgrund der heterogenen Zusammensetzung von Akten können unterschiedliche Aufbewahrungsfristen entstehen. Eine Anbietung an das zuständige öffentliche Archiv hat spätestens 30 Jahre nach Entstehung der Unterlagen zu erfolgen, sofern das HArchivG, der geltende Aktenführungserlass sowie gegebenenfalls andere geltende Rechtsvorschriften keine abweichenden Aufbewahrungsfristen festlegen. Eine vorfristige Übernahme von Unterlagen mit noch laufenden Aufbewahrungsfristen wird durch § 4 Abs. 1 HArchivG ermöglicht. In solchen Fällen regeln die abgebenden Stellen im Einvernehmen mit dem zuständigen öffentlichen Archiv die Anbietung und Übernahme der Unterlagen.

Fazit

Zwischen dem Archivrecht und dem Datenschutzrecht gibt es aufgrund von widerstreitenden Zielen ein natürliches Spannungsverhältnis, das bei den handelnden Personen oftmals Unsicherheit auslöst. Durch die Handreichung Löschsurrogat des Hessischen Landesarchivs konnte ein Teil dieser Unsicherheit ausgeräumt werden. Auch zukünftig stehe ich verantwortlichen Stellen gerne gemeinsam mit meinen Mitarbeiterinnen und Mitarbeitern unterstützend bei der Erarbeitung derartiger Papiere zur Seite.

7.2
Einsatz von Avataren in hessischen Schulen

Von Schulen und Eltern erreichten mich viele Anfragen, unter welchen datenschutzrechtlichen Rahmenbedingungen Avatare (auch Telepräsenz-Roboter genannt) in hessischen Schulen genutzt werden dürfen. Die folgenden Erläuterungen geben eine Anleitung für Schulen, wie der Einsatz der Avatare aus der Sicht des Datenschutzes in Schulen in Hessen möglich sein kann.

Avatar als Vertreter eines langzeiterkrankten Kindes

Ein Avatar ist ein kleiner Roboter, der an den Platz eines langzeiterkrankten Kindes in seiner Schulklasse gestellt werden kann. Er ist circa 30 Zentimeter groß, hat zwei Augen aus Lichtern, ein integriertes Mikrofon, einen Lautsprecher, eine Kamera und kann seinen Kopf drehen. Er ist mittels eines Tablets mit dem kranken Kind verbunden. So kann es den Unterricht in Echtzeit verfolgen. Der Avatar hat eine integrierte SIM-Karte, so dass das kranke

Kind auch beispielsweise an dem Schulleben auf dem Pausenhof oder bei Klassenausflügen dabei sein kann.

Die Beschulung langzeiterkrankter Kinder stellt für alle Beteiligten vor Ort immer wieder eine große Herausforderung dar. Beispielsweise kommt es bei dem Einsatz von Avataren neben räumlichen und baulichen Aspekten in den jeweiligen Schulen auch ganz besonders auf die pädagogische Einordnung einer solchen Maßnahme durch die Lehrkräfte und Schulleitungen in den Schulen vor Ort an. Hinzu kommen datenschutzrechtliche Aspekte, die erfüllt sein müssen, da bei dem Einsatz der Avatare die personenbezogenen Daten von Schülerinnen und Schülern wie auch von Lehrkräften verarbeitet werden. Dies hat zur Folge, dass die verantwortliche Schule vor dem Einsatz eines Avatars eine datenschutzrechtliche Prüfung vornehmen muss.

Zulässigkeit

Damit personenbezogene Daten rechtmäßig verarbeitet werden können, bedarf es einer datenschutzrechtlichen Rechtsgrundlage. Im Falle des Einsatzes von Avataren in hessischen Schulen stellt § 83b Abs. 1 HSchG eine geeignete rechtliche Grundlage für die Verarbeitung personenbezogener Daten dar. § 83b Abs. 1 HSchG regelt die Übertragung von Bild und Ton im Rahmen von Distanzunterricht und lautet wie folgt:

§ 83b HSchG

(1) Werden Schülerinnen und Schüler, die nicht in Präsenzform am Unterricht teilnehmen können, mittels Videokonferenzsystem zum Unterricht zugeschaltet, dürfen zum Zweck der Übertragung von Bild und Ton die erforderlichen personenbezogenen Daten der im Unterrichtsraum anwesenden Schülerinnen und Schüler sowie der Lehrkraft und sonstiger in der Schule beschäftigter Personen verarbeitet werden. (…)

In § 83b Abs. 1 HSchG ist aus datenschutzrechtlicher Sicht genau der Fall beschrieben, dass ein Kind nicht die Schule besuchen kann und deshalb auf die Übertragung von Bild und Ton aus dem Unterrichtsraum heraus angewiesen ist, um an dem Schulgeschehen teilzuhaben. Zu diesem Zweck erlaubt § 83b Abs. 1 HSchG die Übertragung der personenbezogenen Daten von Schülerinnen und Schülern wie auch der Lehrkräfte. Es ist demnach keine Einwilligung dieser Personen in die Verarbeitung ihrer personenbezogenen Daten erforderlich.

Einhaltung weiterer datenschutzrechtlicher Vorgaben

Wenn sich nun eine Schule für den Einsatz eines Avatars mittels zuvor genannter Rechtsgrundlage entschieden hat, muss sie als datenschutzrechtlich verantwortliche Stelle dafür Sorge tragen, dass die allgemeinen Vorgaben des Datenschutzrechts eingehalten werden. Hierbei sollte insbesondere beachtet werden, dass nicht jedes auf dem Markt befindliche Produkt diese Vorgaben erfüllt.

Folgende Aspekte sind an dieser Stelle besonders relevant:

– Überprüfung der Datenschutzerklärung der jeweiligen Anbieterfirma und der Datenverarbeitung.
– Ggf. Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO.
– Abschluss einer Vereinbarung zur Auftragsdatenverarbeitung mit dem Anbieter: Bei einem solchen Abschluss obliegt der Schule – als verantwortlicher Stelle – die Einhaltung der rechtlichen Vorgaben aus Art. 28 DS-GVO.
– Aufnahme der mit dem Einsatz des Avatars einhergehenden Verarbeitungstätigkeit in das Verarbeitungsverzeichnis der Schule gemäß Art. 30 DS-GVO.
– Information aller betroffenen Personen über die Verarbeitung ihrer personenbezogenen Daten gemäß Art. 13 Abs. 1 bis 3 DS-GVO.

Darüber hinaus müssen die Vorgaben von § 18 SchDSV für den Einsatz von Videokonferenzsystemen auch im Fall des Einsatzes eines Avatars beachtet werden.

Technische und organisatorische Maßnahmen

Auch mit Blick auf die technische Ausgestaltung muss beim Einsatz eines Avatars geprüft werden, dass die datenschutzrechtlichen Vorgaben eingehalten werden können. Dies beinhaltet insbesondere, dass die verantwortlichen Schulen verpflichtet sind, die Grundsätze der Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DS-GVO durch geeignete technische und organisatorische Maßnahmen angemessen umzusetzen. Dazu sind sie aufgrund von Art. 24 und 25 DS-GVO verpflichtet.

Neben den Grundsätzen wie der Zweckbindung, der Datenminimierung oder der Rechtmäßigkeit liegt ein besonderes Augenmerk auf dem Grundsatz zur vertraulichen Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 Buchst. f DS-GVO. Um diese gewährleisten zu können, sind in der Regel Maßnahmen angezeigt, zu denen die folgenden als Beispiele dienen

können. So sollte zunächst sichergestellt sein, dass nur das Kind, das den Avatar nutzt, auf das übertragene Video zugreifen kann. Dies dient sowohl dem Schutz der Rechte und Freiheiten der betrachteten Schülerinnen und Schüler und Lehrkräfte als auch des betrachtenden Kindes. Die Personen, die am Unterricht in Präsenz teilnehmen, sollen sich sicher sein können, nicht durch Dritte, sondern nur durch die zugeschaltete Mitschülerin oder den Mitschüler gesehen zu werden. Um dies technisch sicherzustellen, soll immer nur eine einzige Verbindung zu dem Avatar zwischen dem Endgerät des Kindes und dem Avatar möglich sein.

Es soll für die in Präsenz teilnehmenden Personen außerdem klar erkennbar sein, dass der Avatar aktiv ist und sie gesehen werden können. Das kann beispielsweise dadurch erreicht werden, dass der Avatar durch Leuchtelemente sichtlich „belebt“ dargestellt wird.

Eine Speicherung von Video- oder Tonaufnahmen auf Servern von Diensteanbietern oder sonstigen Stellen soll ausgeschlossen sein.

Die Übertragung der Bild- und Tondaten zwischen dem Avatar und dem Endgerät des Kindes muss verschlüsselt stattfinden. Zumindest ist eine wirksame Transportverschlüsselung entsprechend dem Stand der Technik erforderlich. Die Verschlüsselung darf insbesondere nicht durch Diensteanbieter aufgehoben werden können, etwa indem diese das verwendete Schlüsselmaterial kontrollieren. Der Verantwortliche muss überprüfen, ob im Einzelfall aufgrund des mit der Verarbeitung personenbezogener Daten verbundenen Risikos über die Transportverschlüsselung hinaus auch eine Inhaltsverschlüsselung als Ende-zu-Ende-Verschlüsselung erforderlich ist.

Solche technischen und organisatorischen Maßnahmen können darauf hinwirken, dass die Grundsätze des Datenschutzes wirksam umgesetzt werden.

Fazit

Telepräsenz-Avatare sind eine moderne Lösung, um Kindern, die durch ihre Lebensumstände darin eingeschränkt sind, am Unterricht in der Schule vor Ort teilzunehmen, eine bessere Teilhabe zu ermöglichen und ein Stück Lebensqualität zu erhalten oder herzustellen. Dieser digitale Ansatz bringt grundsätzlich datenschutzrechtliche Anforderungen mit sich, die durch die verantwortlichen Schulen umgesetzt werden können, so dass hierbei auch der Schutz der Rechte und Freiheiten aller beteiligten Personen gut gewahrt wird.

8. Beschäftigungsverhältnisse

Im Beschäftigungsverhältnis findet Datenverarbeitung in einem asymmetrischen Informations- und Machtverhältnis statt. Datenschutz hat hier auch die Aufgabe, dieses ungleiche Verhältnis auszugleichen. Das darf aber Verantwortliche nicht daran hindern, ihre berechtigten und überwiegenden Interessen wahrzunehmen. Eine solche Situation kann entstehen, wenn in einem Konzern Daten über Straftaten eines Beschäftigten in einem Konzernunternehmen an ein anderes Konzernunternehmen weitergegeben werden sollen (Kap. 8.1). Umgekehrt ist die Situation zu bewerten, wenn ein Arbeitgeber von seinen Beschäftigten die Angabe der privaten Telefonnummern verlangt (Kap. 8.3). Zu klären war im Berichtszeitraum auch, unter welchen Voraussetzungen das Amt als Datenschutzbeauftragter oder Datenschutzbeauftragte niedergelegt werden kann (Kap. 8.2).

8.1
Weitergabe von Beschäftigtendaten über Straftaten in einem Konzern

Auch Straftäterinnen und Straftäter haben Datenschutzrechte. Jedoch können diese nicht dazu führen, dass Verantwortliche ihre berechtigten Interessen zur Verteidigung gegen Straftaten nicht wahrnehmen können. Die zeigt ein weiteres Mal: Datenschutz ist kein Täterschutz!

Austausch über einen Verdacht innerhalb eines Versicherungskonzerns

Eine ehemalige Beschäftigte eines Versicherungsunternehmens beschwerte sich über die unzulässige Weitergabe personenbezogener Daten. Dieses Versicherungsunternehmen (A) gehört zu einem Konzern. Bei einem anderen Versicherungsunternehmen (H) innerhalb des Konzerns hatte die Beschwerdeführerin eine Privathaftpflichtversicherung abgeschlossen. Die Beschwerdeführerin gab an, das Versicherungsunternehmen (H) habe Informationen aus einem privaten Schadensfall, für den sie eine Schadensregulierung beantragt hatte, an das Versicherungsunternehmen (A) weitergegeben. Daraufhin sei sie zur Unterzeichnung eines Aufhebungsvertrags für ihren Arbeitsvertrag gedrängt worden. Sie sah sich durch die Weitergabe der Informationen innerhalb des Konzernunternehmens in ihren Datenschutzrechten verletzt.

Ich habe das Versicherungsunternehmen (A) zu dem Sachverhalt angehört. Dieses machte geltend, bei dem Antrag der Beschwerdeführerin auf Schadensregulierung bei ihrer Privathaftpflichtversicherung habe das Versicherungsunternehmen (H) begründete Anhaltspunkte für einen versuchten

Versicherungsbetrug. Hierzu machte das Unternehmen ausführliche Angaben. Es lagen dokumentierte Anhaltspunkte dafür vor, dass die Beschwerdeführerin den Schaden bei der Ausübung einer genehmigten Nebentätigkeit, einer handwerklichen Tätigkeit, verursacht hatte. Handwerkliche Tätigkeiten waren aber gemäß den Versicherungsbedingungen vom Versicherungsschutz der Privathaftpflicht ausgenommen. Die Beschwerdeführerin habe auf Rückfrage Angaben zum Schadenshergang gemacht, die sich nach Anhörung der geschädigten Person als wahrheitswidrig herausgestellt hätten. Es lagen damit ausreichende Verdachtspunkte dafür vor, dass die Beschwerdeführerin gegenüber dem Unternehmen (H) bewusst falsche Angaben gemacht hatte, um die Deckung des Schadens über ihre Privathaftpflichtversicherung zu erreichen. Nach den Schilderungen der Beschwerdeführerin in der Schadensmeldung habe man außerdem davon ausgehen müssen, dass die Beschwerdeführerin der an sich genehmigten Nebentätigkeit innerhalb der Arbeitszeit ihrer Haupttätigkeit beim Versicherungsunternehmen (A) nachgegangen sei und dafür den ihr zur Verfügung gestellten Firmenwagen genutzt habe. Daher sei auch der Verdacht auf Arbeitszeitbetrug entstanden. Die verantwortliche Stelle berief sich darauf, dass sie die Informationen aufgrund gesetzlicher Bestimmungen, aber auch aufgrund berechtigter Interessen an die Konzernrevision habe weitergeben müssen. Man habe zunächst versucht, Einzelgespräche mit der Beschwerdeführerin zu führen, die aber nicht zur Sachverhaltsaufklärung bezüglich des vermuteten Arbeitszeitbetrugs beigetragen hätten. Die Beschwerdeführerin habe sich in Widersprüche verstrickt. Daher habe die Führungskraft der Beschwerdeführerin im Versicherungsunternehmen (A) informiert werden müssen, um mit dieser ein Gespräch über die vereinbarte Arbeitszeit zu führen.

Die Ausführungen der verantwortlichen Stelle waren plausibel und nachvollziehbar. Daher habe ich gegenüber der verantwortlichen Stelle keine Maßnahmen ergriffen und das Beschwerdeverfahren beendet.

Keine generelle Erlaubnis innerhalb eines Konzerns

Die DS-GVO kennt kein sogenanntes „großes Konzernprivileg“, das die Weitergabe von personenbezogenen Daten von einem Konzernunternehmen zum anderen per se erlauben würde. Daher muss für einen solchen Verarbeitungsvorgang immer ein Erlaubnistatbestand nach Art. 6 Abs. 1 und eventuell Art. 9 oder Art. 10 DS-GVO erfüllt sein.

Keine Anwendbarkeit von Art. 10 DS-GVO

Art. 10 DS-GVO

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

Art. 10 DS-GVO regelt die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten als besonders sensible personenbezogene Daten. Dieser Erlaubnistatbestand ist hier jedoch nicht einschlägig. Unter Daten über Straftaten im Sinne dieser Vorschrift ist primär die hoheitliche Feststellung zu verstehen, dass die betroffene Person tatbestandlich und rechtswidrig eine bestimmte Straftat begangen hat (BeckOK DatenschutzR/Bäcker DS-GVO Art. 10 Rn. 2). Nicht erfasst von dieser Vorschrift sind Daten über Handlungen von betroffenen Personen, die einen Straftatbestand verwirklichen (BeckOK DatenschutzR/Bäcker DS-GVO Art. 10 Rn. 4).

Weitergabe der Daten zur Erfüllung einer gesetzlichen Verpflichtung

Gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO ist die Verarbeitung von personenbezogenen Daten rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der die verantwortliche Stelle unterliegt. Dabei muss nach Art. 6 Abs. 3 Satz 1 DS-GVO eine Rechtsgrundlage aus dem Unionsrecht oder dem Recht eines Mitgliedstaates diese rechtliche Verpflichtung begründen.

Art. 6 Abs. 1 UAbs. 1 Buchst. c 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. (…)

Art. 6 Abs. 3 Satz 1 DS-GVO

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

a) Unionsrecht oder

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

Nach § 30 Abs. 1 des Gesetzes über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz – VAG) müssen Versicherungsunternehmen über eine interne Revision verfügen, deren Ziel es unter anderem ist, sachlichen Schaden z. B. durch Versicherungsbetrug von dem jeweiligen Unternehmen abzuwenden.

§ 30 Abs. 1 VAG

(1) Versicherungsunternehmen müssen über eine wirksame interne Revision verfügen, welche die gesamte Geschäftsorganisation und insbesondere das interne Kontrollsystem auf deren Angemessenheit und Wirksamkeit überprüft.

Das Versicherungsunternehmen konnte sich also auf die rechtliche Verpflichtung, einen Verdacht auf Versicherungsbetrug der Konzernrevision zu melden, berufen. Allerdings ist das Unternehmen (A) nicht die Konzernrevision. Doch kann ein effektives Kontrollsystem eine Einbeziehung auch des Unternehmens (A) in die Kommunikation über den Vorfall sein.

Wahrung der berechtigten Interessen der beteiligten Unternehmen

Neben dem Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO war hier auch der Erlaubnistatbestand des Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO erfüllt.

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

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

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

Da Art. 6 Abs. 1 UAbs. 1 DS-GVO darauf verweist, dass *mindestens* eine der nachstehenden Bedingungen erfüllt sein muss, können diese Erlaubnistatbestände nebeneinanderstehen und gleichzeitig zur Anwendung kommen.

Die DS-GVO kennt kein „großes Konzernprivileg", jedoch ein „kleines Konzernprivileg", wonach die Verantwortlichen ein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO an der Übermittlung personenbezogener Daten innerhalb eines Konzerns haben können. Dies ergibt sich aus ErwG 48 Satz 1 DS-GVO:

ErwG 48 Satz 1 DS-GVO

Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.

Im Fall eines versuchten Versicherungsbetrugs kann also die Übermittlung von personenbezogenen Daten innerhalb eines Konzerns zulässig sein, da das Interesse eines Versicherungsunternehmens am Schutz vor illoyalen Mitarbeitern als berechtigtes Interesse anzuerkennen ist. Auch die Verhinderung von Betrug gilt nach ErwG 47 Satz 6 zur DS-GVO als berechtigtes Interesse.

ErwG 47 Satz 6 DS-GVO

Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar.

Hier bestand die Gefahr, dass das Versicherungsunternehmen (H) einen Schaden bezahlt hätte, der nicht von den Bedingungen der Privathaftpflichtversicherung umfasst war. Zudem hatte auch das Versicherungsunternehmen (A) ein berechtigtes (Dritt-)Interesse daran, dass die Ausübung der Nebentätigkeit nicht innerhalb der Arbeitszeit für die Haupttätigkeit erfolgte und der Dienstwagen dafür genutzt wurde.

Die Datenverarbeitung war auch erforderlich zur Wahrung des berechtigten Interesses des Versicherungsunternehmens (A), da die Verdachtsmomente des Arbeitszeitbetrugs ohne das Hinzuziehen des Vorgesetzten der Beschwerdeführerin nicht hätten aufgeklärt werden können. Ferner gab es kein Interesse der Beschwerdeführerin, das die berechtigten Interessen der Versicherungsunternehmen überwog, da sich die Beschwerdeführerin schon

nicht in einer durch die geltenden Gesetze abgedeckten Rechtsposition befand. Dass der Schutz einer Person, die einen Betrug begehen will, kein Recht sein kann, das dem berechtigten Interesse des Verantwortlichen oder eines Dritten entgegensteht, zeigt etwa die in ErwG 47 Satz 6 zur DS-GVO vorgenommene Wertung. Danach sind die datenschutzrechtlichen Bestimmungen nicht dazu gedacht, Täter bei der Begehung einer Straftat zu schützen.

8.2
Niederlegung des Amts als Datenschutzbeauftragte

Mich haben einige Anfragen von Datenschutzbeauftragten erreicht, in denen ich um Beratung gebeten wurde, *ob* und falls ja, *wie* sie ihr Amt als Datenschutzbeauftragte selbst niederlegen können. Die Beratungsanfragen behandelten nicht den Fall, dass ein Datenschutzbeauftragter durch den Verantwortlichen abberufen wird, sondern den Fall, dass der Datenschutzbeauftragte selbst sein Amt niederlegen möchte. Gründe dafür waren sowohl persönliche als auch intern berufliche. Der Beratungsbedarf ergab sich insbesondere daraus, dass weder die DS-GVO noch das BDSG oder das HDSIG eine gesetzliche Regelung für diesen Fall enthalten.

Grundsätzliches

Bei der Beantwortung der Beratungsanfragen ist zu unterscheiden, ob es sich um einen Datenschutzbeauftragten einer öffentlichen Stelle i. S. d. § 2 Abs. 1 und 3 HDSIG oder einer nicht-öffentlichen Stelle i. S. d. § 1 Abs. 2 HDSIG und ob es sich um einen internen oder einen externen Datenschutzbeauftragten handelte.

Trotz fehlender ausdrücklicher gesetzlicher Regelung geht die Kommentarliteratur im Ergebnis davon aus, dass interne und externe Datenschutzbeauftragte von öffentlichen und von nicht-öffentlichen Stellen ihr Amt beenden können (s. z. B. Wilmer, in: Roßnagel, Kommentar HDSIG, 2021, § 5 Rn. 13; Rapp, in: Ronellenfitsch u. a., Kommentar HDSIG, 21. EL Sept. 2025, § 5 Rn. 17). Dabei ist eine entsprechende Frist, die eine Nachfolgeregelung ermöglicht, einzuhalten. Gründe für die Beendigung des Amts sind grundsätzlich nicht vom Datenschutzbeauftragten zu benennen.

Je nachdem, um welchen Datenschutzbeauftragten es geht, sind die folgenden Spezifika zu beachten.

Interne Datenschutzbeauftragte

Bei internen Datenschutzbeauftragten begründet sich die Möglichkeit der Amtsniederlegung daraus, dass der Datenschutzbeauftragte nicht gegen seinen Willen verpflichtet werden kann, das Amt weiter fortzuführen. Anderes gilt, wenn die Beschäftigung ausschließlich auf die Tätigkeit des Datenschutzbeauftragten abzielt. Die Amtsniederlegung ist vom internen Datenschutzbeauftragten gegenüber dem Verantwortlichen zu erklären. Aus Gründen der Nachweisbarkeit sollte diese Erklärung schriftlich erfolgen. Auch sollten hier Vorkehrungen getroffen werden, die den Zugang des Schreibens nachweisen können (z. B. Einschreiben, Zeuge bei der Übergabe). In dem Schreiben ist außerdem zu erklären, zu welchem Datum das Amt niedergelegt werden soll. Dabei ist dem Verantwortlichen ausreichend Zeit für die Benennung eines Nachfolgers einzuräumen. Wie lange dieser Zeitraum sein sollte, ist gesetzlich nicht geregelt und hängt individuell von der Situation beim jeweiligen Verantwortlichen ab (z. B. aktuelle Ausgestaltung der personellen Ressourcen beim Verantwortlichen).

Räumt der Datenschutzbeauftragte, der sein Amt niederlegen möchte, dem Verantwortlichen nicht genügend Zeit für die Benennung eines Nachfolgers ein, so kann er sich gegenüber dem Verantwortlichen schadensersatzpflichtig machen (so z. B. Scheja, in: Taeger/Gabel, Kommentar DS-GVO, BDSG und TDDG, 4. Aufl. 2022, § 6 BDSG, Rn. 15).

Darüber hinaus sind bei der Amtsniederlegung von internen Datenschutzbeauftragten dienst- und arbeitsrechtliche Aspekte zu berücksichtigen. Denn die Benennung eines internen Datenschutzbeauftragten findet bei Beamten regelmäßig im Wege des Direktionsrechts (z. B. als Aufgabenübertragung, Abordnung oder als Versetzung) statt. Bei Arbeitnehmern werden entsprechende Anpassungen in den jeweiligen Arbeitsverträgen vorgenommen.

Besonderheiten bei einer nicht-öffentlichen Stelle

Wie bereits erwähnt, sind bei der Amtsniederlegung keine Gründe anzugeben. Legt der interne Datenschutzbeauftragte einer nicht-öffentlichen Stelle jedoch sein Amt aufgrund eines wichtigen Grundes i. S. d. § 626 BGB nieder, so hat er diesen Schritt gegenüber dem Verantwortlichen zu begründen.

Im Falle der Amtsniederlegung durch den internen Datenschutzbeauftragten einer nicht-öffentlichen Stelle gilt auch der Kündigungsschutz nach § 6 Abs. 4 Satz 3 BDSG.

Besonderheiten bei einer öffentlichen Stelle

Eine öffentliche Stelle i. S. d. HDSIG ist gemäß § 5 Abs. 1 HDSIG verpflichtet, auch einen stellvertretenden Datenschutzbeauftragten zu benennen. Die bisherigen Ausführungen (außer den Besonderheiten bei internen Datenschutzbeauftragten einer nicht-öffentlichen Stelle) gelten auch für den internen stellvertretenden Datenschutzbeauftragten einer öffentlichen Stelle, der sein Amt niederlegen möchte. Dass die öffentliche Stelle einen Stellvertreter bereits benannt hat, ist bei der Berechnung der Frist für das Wirksamwerden der Niederlegung des Amtes zu berücksichtigen.

Externe Datenschutzbeauftragte

Externe Datenschutzbeauftragte schließen mit der Stelle, die sie benennt, i. d. R. einen Dienstleistungsvertrag ab. Möchte ein externer Datenschutzbeauftragter auf eigenen Wunsch seinem Amt nicht mehr nachkommen, so hat er die im Dienstleistungsvertrag vereinbarten Kündigungsregeln einzuhalten. Aus diesen ergibt sich auch die Möglichkeit der Beendigung seines Amts als externer Datenschutzbeauftragter. Hier sind die jeweiligen Kündigungsfristen des Dienstleistungsvertrags zu beachten. Die Beendigung des Amtes ist folglich in der Art und Weise zu erklären, wie dies der Dienstvertrag vorsieht. Regelmäßig wird dies eine schriftliche (fristgerechte) Kündigung sein, die gegenüber dem Verantwortlichen erklärt werden muss.

8.3
Erhebung privater Telefonnummern im Beschäftigungsverhältnis

Anlässlich einer Meldung nach dem Hinweisgeberschutzgesetz, die mich durch das Bundesamt der Justiz erreichte, habe ich mich im Berichtszeitraum mit der Frage der datenschutzrechtlichen Zulässigkeit der Erhebung privater Telefonnummern im Beschäftigungsverhältnis befasst. In der Meldung wurde mir durch den Hinweisgeber u. a. mitgeteilt, dass ein großes Speditionsunternehmen mit Sitz in Hessen die privaten Telefonnummern (d. h. die private Mobilnummer oder die private Festnetznummer) seiner Beschäftigten speichere.

Begründungen für die Erhebung

Das Landesarbeitsgericht Thüringen hatte zu dieser Frage bereits im Jahr 2018 entschieden, dass die Erhebung oder Erfassung der privaten Telefonnummer eines Beschäftigten gegen seinen Willen wegen des darin liegenden Eingriffs in das allgemeine Persönlichkeitsrecht nur dann zulässig ist, wenn der Arbeitgeber ohne Kenntnis der Mobiltelefonnummer im Einzelfall eine

legitime Aufgabe andernfalls nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und ihm eine andere Organisation der Aufgabenerfüllung nicht möglich oder zumutbar ist (Urt. vom 16. Mai 2018, Rs. 6 Sa 442/17, Leitsatz und Rn. 44 ff.).

Nachdem ich den Verantwortlichen auf das o. g. Urteil hingewiesen hatte, trug dieser vor, dass die Erfassung der privaten Telefonnummern für die Planung der An- und Abfahrtszeiten, der An- und Abfahrtswege und des Einsatzes der überwiegend im Ausland wohnenden Beschäftigten erforderlich sei. Obgleich die beschäftigten Fahrer der Spedition ein dienstliches Mobiltelefon besäßen, ließen sie es in den sog. Freiwochen oftmals ausgeschaltet oder in der Spedition liegen. Dies mache die Erfassung der privaten Telefonnummern zwingend erforderlich. Ergänzend trug der Verantwortliche vor, dass die Erfassung auch aufgrund der Gefahrgeneigtheit der Tätigkeit erforderlich sei, damit Angehörige des Fahrers im Falle eines Verkehrsunfalles benachrichtigt werden könnten.

Die Erfassung der privaten Telefonnummer sei daher sowohl aufgrund des berechtigten Interesses des Speditionsunternehmens als auch des Beschäftigten nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gerechtfertigt. Sofern das berechtigte Interesse nicht greife, würden die privaten Telefonnummern der Beschäftigten aufgrund einer Einwilligung erfasst.

Grundsätzlich sind die Ausführungen des Speditionsunternehmens nachvollziehbar. Aus datenschutzrechtlicher Sicht ist die Erfassung privater Telefonnummern von Beschäftigten dennoch problematisch.

Datenschutzrechtliche Rechtfertigung?

Als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO ist das Speditionsunternehmen nach Art. 5 DS-GVO gesetzlich verpflichtet, die Grundsätze ordnungsgemäßer Datenverarbeitung einzuhalten. Art. 5 Abs. 1 Buchst. a DS-GVO verlangt, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Art. 5 Abs. 1 Buchst. a 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“); (…)

Die Verarbeitung personenbezogener Daten richtete sich für Beschäftigte im nicht-öffentlichen Bereich bis vor wenigen Jahren nach dem Erlaubnistatbestand des § 26 Abs. 1 Satz 1 BDSG. Aufgrund der Ausführungen des EuGH in seinem Urteil vom 30. März 2023 in der Rechtssache C-34/21 ist jedoch davon auszugehen, dass der Erlaubnistatbestand des § 26 Abs. 1 Satz 1 BDSG nicht mit der Öffnungsklausel des Art. 88 DS-GVO vereinbar ist (siehe Handreichung – Verarbeitung personenbezogener Daten von Beschäftigten im Lichte des EuGH-Urteils vom 30. März 2023, abzurufen unter: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-05/handreichung_beschaeftigtendatenschutz_eugh-urteil.pdf). Daher wird nachfolgend auf die Rechtsgrundlagen des Art. 6 Abs. 1 Abs. 1 UAbs. 1 DS-GVO zurückgegriffen.

Durchführung eines Vertrags oder überwiegende berechtigte Interessen?

Soweit das Speditionsunternehmen die Erfassung der privaten Telefonnummern auf die Planung der An- und Abfahrtszeiten, der An- und Abfahrtswege und des Einsatzes stützt, käme aufgrund des unmittelbaren Zusammenhangs zum Beschäftigungsverhältnis vorrangig Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO (Erfüllung des Arbeitsvertrags) zur Anwendung. Die Erfassung der privaten Telefonnummern zur Benachrichtigung von Angehörigen eines verunglückten Beschäftigten stützt sich hingegen auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO (Wahrung berechtigter Interessen).

Art. 6 Abs. 1 UAbs. 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; (…)

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.

Sowohl Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO als auch Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO verlangen, dass die Verarbeitung zur Zweckerreichung erforderlich ist. Erforderlichkeit bedeutet, dass personenbezogene Daten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht

in zumutbarer Weise durch andere, die Grundrechte und Grundfreiheiten der betroffenen Person weniger beeinträchtigende Mittel erreicht werden kann.

Grundsätzlich hat der Arbeitgeber die zur Erfüllung der Arbeitsleistung erforderlichen Mittel zur Verfügung zu stellen (s. LAG Thüringen, Urt. vom 16. Mai 2018, Rs. 6 Sa 442/17, Rn. 41 ff.). Beschäftigte sind insoweit nicht verpflichtet, ihre privaten Kommunikationsmittel zur Erfüllung der Arbeitsleistung anzubieten oder zu nutzen.

Vor diesem Hintergrund konnten mich die Ausführungen zur Erforderlichkeit der Erfassung privater Telefonnummern nicht überzeugen. Zwar ist nachvollziehbar, dass die An- und Abfahrtszeiten, die An- und Abfahrtswege und auch ein bevorstehender Einsatz vorbesprochen werden müssen. Es ist jedoch nicht nachvollziehbar, weshalb das bereits zur Verfügung stehende dienstliche Mobiltelefon nicht auch für diese Kommunikation genutzt werden kann. Soweit die Beschäftigten ihr dienstliches Mobiltelefon in den Räumlichkeiten des Speditionsunternehmens belassen, käme als milderes Mittel zudem auch eine organisatorische Maßnahme, etwa eine Anweisung zur Erreichbarkeit unmittelbar vor Dienstantritt über das dienstliche Mobiltelefon, in Betracht.

Wenn private Telefonnummern von Beschäftigten aufgrund der Unfallgeneigtheit des Berufs als Speditionsfahrer erfasst werden sollen, ist bereits das Mittel nicht geeignet, den verfolgten Zweck zu erreichen. Da die privaten Mobilnummern gerade den Beschäftigten (und nicht einem Familienangehörigen) zugehörig sind und diese ihre privaten Mobiltelefone in der Regel bei sich führen, dürfte die Information von Angehörigen hierüber kaum möglich sein. Ergänzend ist darauf hinzuweisen, dass – sollte die Festnetznummer eines Beschäftigten erfasst werden, die mehreren Familienmitgliedern oder sonstigen Mitbewohnern zugeordnet ist – dies eine Einwilligung zur Erhebung der Kontaktdaten auch des Familienmitglieds sowie dessen Information nach Art. 14 DS-GVO voraussetzen würde.

Da die Erforderlichkeit nicht gegeben war, rechtfertigten weder Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO noch Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO die Erfassung der privaten Telefonnummern der Beschäftigten des Speditionsunternehmens.

Einwilligung?

Soweit eine Datenverarbeitung auf Grundlage einer Einwilligung erfolgt, sind die Art. 4 Nr. 11, Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO und Art. 7 DS-GVO zu beachten. Im Beschäftigungsverhältnis ist zusätzlich § 26 Abs. 2 BDSG zu beachten.

Im Beschäftigungsverhältnis kommt der Frage nach der Freiwilligkeit der Einwilligung besondere Bedeutung zu. Dies trägt dem Umstand Rechnung, dass zwischen Arbeitgebern und Beschäftigten ein Über-/ Unterordnungsverhältnis besteht und die einseitige wirtschaftliche Abhängigkeit der Beschäftigten der freien Willensbildung entgegenstehen kann. Die Freiwilligkeit ist daher regelmäßig etwa dann ausgeschlossen, wenn der betroffenen Person kein rechtmäßiges Alternativverhalten angeboten wird, sie sich zur Einwilligung gedrängt fühlt oder negative Auswirkungen erdulden muss, wenn sie nicht einwilligt (Europäischer Datenschutzausschuss, Leitlinien 5/2020 zur Einwilligung gemäß Verordnung 2016/679, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf, Seite 8 Rn. 13). Die Einwilligung kommt für Verarbeitungen von Beschäftigtendaten daher nur selten nicht in Betracht (s. auch Kurzpapier Nr. 14 „Beschäftigtendatenschutz“ der DSK, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_14.pdf).

Der Verantwortliche konnte während des gesamten Verwaltungsverfahrens nicht schlüssig darlegen, wie die Einwilligungserklärung von Beschäftigten eingeholt wird und ob sie den gesetzlichen Anforderungen entspricht. Daher war die Erfassung privater Telefonnummern aufgrund einer Einwilligung nach Art. 6 Abs.1 UAbs. 1 Buchst. a DS-GVO nicht gerechtfertigt.

Ergebnis

Die Erfassung der privaten Telefonnummern der Beschäftigten verstieß gegen den Grundsatz der Rechtmäßigkeit nach Art. 5 Abs. 1 Buchst. a, 6 Abs. 1 UAbs. 1 DS-GVO.

Aufgrund des Datenschutzverstoßes habe ich das Speditionsunternehmen angewiesen, die Verarbeitungsvorgänge in Einklang mit der DS-GVO zu bringen, indem es die privaten Telefonnummern der Beschäftigten löscht oder eine den Anforderungen des Art. 6 Abs. 1 UAbs. 1 Buchst. a, 7 DS-GVO i. V. m. § 26 Abs. 2 BDSG entsprechend wirksame Einwilligung für die Speicherung der privaten Telefonnummern ihrer Beschäftigten einholt.

9. Künstliche Intelligenz

Im Berichtszeitraum zeigte sich erneut die steigende Bedeutung des Einsatzes Künstlicher Intelligenz (KI) in der öffentlichen Verwaltung. Dieser Bedeutung wird die Datenschutzkonferenz gerecht, indem sie einen eigenen Arbeitskreis „Künstliche Intelligenz" eingerichtet hat, in dem meine Behörde intensiv mitarbeitet (Kap. 9.1). Dieser hat eine Orientierungshilfe für Retrieval Augmented Generation (RAG) erarbeitet, eine Form der Nutzung von intelligenten Sprachmodellen, die besondere Vorteile für lokale Anwendungen, digitale Souveränität und Datenschutz bietet (Kap. 9.2). Wie die KI-Verordnung in Art. 4 fordert, sind für den Einsatz von KI-Systemen besondere Kompetenzen erforderlich, um Voraussetzungen und Wirkungen des KI-Einsatzes beurteilen und verantworten zu können. Ich biete für die Verwaltung in Hessen vielfach Fortbildungen für den datenschutzgerechten KI-Einsatz in der öffentlichen Verwaltung an (Kap. 9.3). Die Rechtsentwicklungen in der EU und in anderen Bundesländern zeigen an, dass ein spezifischer Rechtsrahmen erforderlich ist, um Hindernisse und Rechtsunsicherheiten für den KI-Einsatz in der öffentlichen Verwaltung zu beseitigen (Kap. 9.4).

9.1 Der Arbeitskreis „Künstliche Intelligenz" der Datenschutzkonferenz

Innerhalb kurzer Zeit sind Anwendungen, die auf dem Prinzip der Künstlichen Intelligenz (KI) beruhen, fester Bestandteil der Arbeitswelt und des Privatlebens vieler Menschen geworden. Um die zahlreichen, mit der Entwicklung und Nutzung von KI-Anwendungen einhergehenden datenschutzrechtlichen Fragen und Probleme effizient und bundesweit einheitlich adressieren zu können, hat die Datenschutzkonferenz den Arbeitskreis KI ins Leben gerufen.

Den Begriff und das Konzept der „Künstlichen Intelligenz" gibt es bereits seit den 1950er Jahren. Allerdings war die Wahrnehmung dieses Teilgebiets der Informatik jahrzehntelang im Wesentlichen auf den akademischen Bereich beschränkt. Grund dafür war vor allem das Fehlen ausreichender maschineller Rechenleistung, um die wissenschaftlichen Konzepte und Ideen zur Künstlichen Intelligenz, insbesondere die des maschinellen Lernens, auch in die Tat umsetzen und in größerem Umfang nutzbar machen zu können. Mit der Zeit ist jedoch die Rechenleistung von modernen Computern kontinuierlich angestiegen und wurden speziell auf das Training und die Inferenz moderner KI-Anwendungen ausgelegte Prozessoren, Plattformen und Programmierschnittstellen weiterentwickelt. Damit rückten Anwendungen, die auf modernen Prinzipien der Künstlichen Intelligenz basieren, in immer greifbarere Nähe und konnten seit den 2010er Jahren in größerem Umfang

entwickelt und angewendet werden. Mittlerweile sind KI-Anwendungen auf fast jedem modernen Smartphone, Computer und auch anderen vernetzten Geräten angekommen und werden zunehmend Bestandteil des Arbeits- und Privatlebens vieler Menschen.

Schon zu Beginn des weltweiten Erfolgs moderner KI-Systeme und -Dienstleistungen hatte die Datenschutzkonferenz die nahende Entwicklung und die Bedeutung des Themas für den Datenschutz erkannt. Bei ihrer Sitzung im geschichtsträchtigen Hambacher Schloss wurde im April 2019 die „Hambacher Erklärung zur Künstlichen Intelligenz“ verabschiedet (https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf). Diese betrachtet Künstliche Intelligenz im Lichte der wichtigsten Grundpfeiler des Datenschutzrechts und benennt grundlegende datenschutzrechtliche Anforderungen an die Entwicklung und den Einsatz von KI-Systemen. Im Zuge dessen wurde zunächst eine themenspezifische Taskforce und damit eine erste Plattform geschaffen, die den deutschen Datenschutzbehörden eine gezielte Zusammenarbeit zu einzelnen KI-Themen und das Erarbeiten gemeinsamer Positionen ermöglichte.

Mit dem Markteintritt von ChatGPT im November 2022 rückten die Möglichkeiten großer Sprachmodelle (Large Language Models – LLM) die Möglichkeiten der KI stärker in den Fokus der öffentlichen Wahrnehmung. Das Thema KI nahm durch die alltägliche Nutzung von Chatbots innerhalb kurzer Zeit massiv an Bedeutung zu. Es stellten sich neue und erstmals auch in der Praxis relevante Fragen zum Umgang mit KI. Neben Fragen u. a. zur Richtigkeit von KI-Antworten, zu KI-Bias oder zu ethischen Problemen wie Diskriminierung waren dies natürlich auch grundlegende datenschutzrechtliche Fragen. Schließlich gehen Training und Nutzung von textgebundenen, generativen KI-Anwendungen, wie den im Fokus der öffentlichen Wahrnehmung stehenden Large Language Models, immer auch mit der Verarbeitung personenbezogener Daten einher, oft sogar in ganz erheblichem Umfang. Anders als bei klassischer Datenverarbeitung lassen sich aus heutiger Sicht einzelne personenbezogene Daten in neuronalen Netzwerken jedoch weder einfach aufrufen noch beauskunften oder mit angemessenem Aufwand korrigieren oder gar löschen.

Um dieser Entwicklung Rechnung zu tragen, hat die Datenschutzkonferenz Ende 2024 den Arbeitskreis KI gegründet. Darin kommen Vertreter aller Datenschutzaufsichtsbehörden des Bundes und der Länder zusammen, die sich schwerpunktmäßig mit KI-Themen und -Anwendungen befassen. Damit wurde innerhalb der Struktur der Datenschutzkonferenz eine dauerhafte Einrichtung geschaffen, in der die Aufsichtsbehörden des Bundes und der

Länder gemeinsam die Vielzahl der datenschutzrechtlichen Probleme beim Einsatz von KI bearbeiten und letztlich auch beantworten können.

Der Arbeitskreis traf sich erstmals Anfang 2025 zu seiner konstituierenden Sitzung. An dieser nahmen neben den Mitgliedern der DSK auch Vertreter zahlreicher interessierter, spezifischer Aufsichtsbehörden teil, die jeweils für bestimmte Stellen aus dem Bereich Rundfunk und Kirche zuständig sind. Seither finden in regelmäßigem Turnus Sitzungen statt. Zudem existiert ein kontinuierlicher Austausch zwischen den Mitgliedern des Arbeitskreises, um sich angesichts der dynamischen Entwicklungen im KI-Bereich zeitnah über den Stand aktueller Entwicklungen auszutauschen. Daneben dient der Arbeitskreis auch dem allgemeinen Erfahrungsaustausch sowie der Koordination gemeinsamer Prüfungen der Aufsichtsbehörden. Beispiele letzterer sind die Prüfungen von OpenAI oder von DeepSeek (Kap. 10.2), an denen ich ebenfalls beteiligt bin.

Aufgrund der Vielzahl und der Komplexität der datenschutzrechtlichen Fragen im Zusammenhang mit KI-Anwendungen hat der Arbeitskreis von Beginn an ein reichlich gefülltes Arbeitsprogramm. Es gilt, Antworten und gemeinsame Positionen zu verschiedenen datenschutzrechtlichen Grundsatzfragen zu finden. Beispiele hierfür sind die Auswirkungen des KI-Trainings mit unzulässigerweise genutzten personenbezogenen Daten oder die Umsetzung der in der DS-GVO geregelten Betroffenenrechte (z. B. Recht auf Auskunft, Berichtigung, Löschung etc.) bei KI-Systemen. An diesen und vielen weiteren Fragen wird seither kontinuierlich gearbeitet. Hierdurch sollen bundesweit einheitliche Festlegungen getroffen werden, um Herstellern und Anwendern von KI-Systemen Orientierung und Unterstützung bei der datenschutzgerechten Umsetzung ihrer jeweiligen Ziele zu geben. Erste Ergebnisse wie z. B. die Erstellung der Orientierungshilfe zu KI-Systemen mit Retrieval Augmented Generation (RAG) (s. hierzu Kap. 9.2) konnten bereits erzielt werden.

Auch in Zukunft wird sich der Arbeitskreis mit den noch zu klärenden und immer wieder neuen datenschutzrechtlichen Fragen bei der Entwicklung und Anwendung von KI-Diensten beschäftigen. Er wird dem kontinuierlichen Austausch der Aufsichtsbehörden zu neuen Entwicklungen sowie der Koordination mit europäischen Aufsichtsbehörden dienen und Entscheidungen der Datenschutzkonferenz vorbereiten.

9.2
Orientierungshilfe für Retrieval Augmented Generation (RAG)

Retrieval Augmented Generation (RAG) ist eine KI-System-Architektur, die weltweit an Popularität gewonnen hat. Deshalb hat sich die DSK mit Blick auf den Datenschutz damit befasst und am 17. Oktober 2025 eine Orientierungshilfe für Unternehmen und Behörden herausgegeben, an der meine Behörde im vergangenen Berichtszeitraum mitgewirkt hat. RAG-Systeme bieten aus Sicht des Datenschutzes zusätzliche Herausforderungen, aber auch Erleichterungen, die mit der Erweiterung des Sprachmodells um ein RAG-Subsystem einhergehen. Im Folgenden werde ich deshalb auf Chancen und Risiken bei der Nutzung dieser KI-Systeme durch verantwortliche Stellen und Auftragsverarbeiter eingehen.

Der Forschungsbereich der Künstlichen Intelligenz (KI) befasst sich mit der Entwicklung intelligenter IT-Systeme, die Probleme lösen und Aufgaben erfüllen können, die normalerweise Menschen vorbehalten sind. Ein Teilgebiet der KI ist das maschinelle Lernen (ML), bei dem KI-Systeme aus gegebenen Daten lernen, um ihre Aufgaben zu erfüllen und ihre Leistung zu verbessern. Ein spezielles ML-Modell ist das Large Language Model (LLM, großes Sprachmodell), das auf dem Training großer Textmengen beruht, um Bedeutungen zu erkennen und beispielsweise Textgenerierung zu ermöglichen. In diesem Umfeld ist Retrieval-Augmented Generation (RAG) eine beliebte KI-System-Architektur, die LLMs mit externem Wissen kombiniert, das von den LLMs nicht erlernt wurde, um relevantere Antworten zu erzeugen (generative KI). Sie können in unterschiedlichen Kontexten eingesetzt werden, wie z. B. für natürliche Sprache, multimodale Daten-Formate oder in Kombination mit nicht-generativer KI. Um die grundlegende Funktionsweise anschaulich zu erläutern, wird im Folgenden exemplarisch ein RAG-System dargestellt, das natürliche Sprache mit einem generativen Sprachmodell (LLM) verarbeitet. Das RAG-System wird hierbei stark vereinfacht dargestellt. Eine ausführlichere, tiefergehende Darstellung mit weiteren Verweisen findet sich in der bereits erwähnten Orientierungshilfe der DSK (Datenschutzrechtliche Besonderheiten generativer KI-Systeme mit RAG-Methode, Version 1.0, https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_RAG.pdf)

Technische Komponenten und Funktion eines RAG-Systems

Ein RAG-Subsystem ergänzt in diesem Beispiel LLM vereinfacht dargestellt um eine Datenbasis und eine Suchfunktion. Dies dient dem Zweck, Informationen, die zum Beispiel nicht Teil der Trainingsdaten des LLM sind, zugänglich und nutzbar zu machen. Im einfachsten Fall kann es sich bei der Datenbasis

um PDF-Dateien oder eine in der heutigen Verwendung übliche Datenbank handeln. Die folgende Darstellung enthält eine vereinfachte Darstellung der wesentlichen Komponenten eines exemplarischen RAG-Systems.

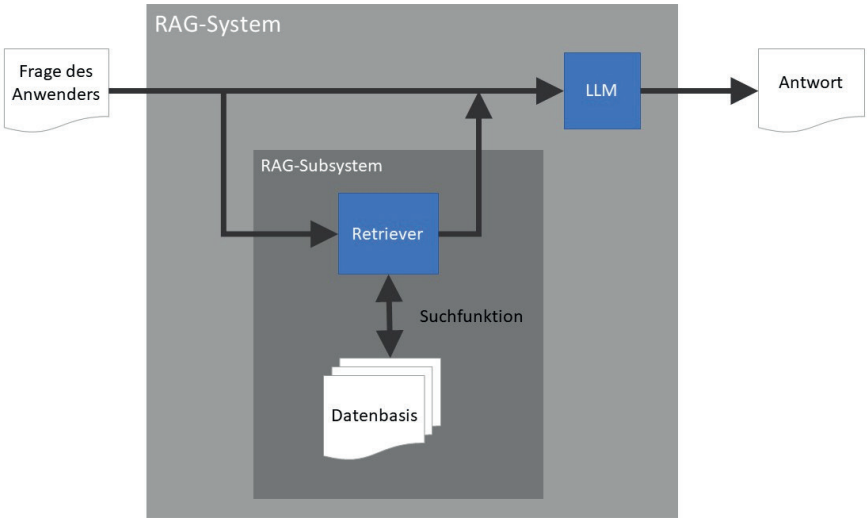


Abb. 1 Vereinfachte Darstellung eines RAG-Systems

Die Suchfunktion des RAG-Subsystems durchsucht die verwendete Datenbasis nach Textabschnitten, die für die vom Benutzer eingegebene Frage relevant sind. Dabei kommt keine rein syntaktische Suche zur Anwendung, sondern in der Regel die Suche nach der semantischen, sinnhaften Nähe zur gestellten Anfrage. Dieser Vorgang wird als Embedding bezeichnet. Embedding dient dazu, sowohl Anfragen als auch alle Textabschnitte der Datenbank in eine vergleichbare Darstellung zu überführen, um relevante Textabschnitte für die Anfrage ermitteln zu können. Dabei werden die Textabschnitte nicht wortwörtlich mit der Anfrage abgeglichen, sondern in eine strukturierte Form transformiert, die semantische Ähnlichkeiten abbildet.

Besser vorstellen lässt sich dieser Vorgang, wenn man einen Vergleich zur Katalogisierung in einer Bibliothek zieht: Statt Bücher nach ihrem vollständigen Inhalt zu durchsuchen, werden sie anhand von Schlagworten und Themen katalogisiert. Wenn eine Nutzeranfrage gestellt wird, sucht das System nicht nach exakten Wortübereinstimmungen, sondern nach inhaltlich passenden Einträgen im Index. Das Embedding übernimmt dabei, metaphorisch gespro-

chen, die Rolle der Verschlagwortung, allerdings auf deutlich komplexerer, mathematischer Ebene. Es erkennt Bedeutungszusammenhänge, die über die reine Wortwahl hinausgehen. Durch diese semantische Kodierung in mehrdimensionalen Vektoren können RAG-Subsysteme die Bedeutungsnähe zwischen Textabschnitten und der Anfrage ermitteln, indem sie die Distanz der jeweiligen Vektoren berechnen. Dadurch findet das RAG-Subsystem auch dann relevante Informationen, wenn die Formulierungen zwischen Anfrage und Dokumenten stark variieren.

Sobald das RAG-Subsystem die relevanten Textabschnitte in der Datenbasis ermittelt hat, ergänzt es die Frage um diesen Kontext und stellt sie dem LLM zur Verfügung. Durch die Hinzufügung der entsprechenden Textpassagen aus der Datenbasis zur Anfrage des Anwenders erzeugt das LLM eine Antwort auf die gestellte Frage. Dabei konzentriert sich das LLM hauptsächlich auf die in der Datenbank gefundenen Daten. Dadurch rücken seine sprachlichen Fähigkeiten in den Vordergrund und es kommt weniger auf das „Wissen“ an, das während des Trainings erworben wurde und inhaltlich möglicherweise eingeschränkt oder bereits überholt sein kann. Je nach konkreter Konzeption und Verwendungszweck ist es möglich, auch kleinere LLMs einzusetzen, für die möglicherweise weniger Trainingsdaten verwendet wurden. Das grundlegende Prinzip kann in der praktischen Ausgestaltung eines RAG-Systems in vielen unterschiedlichen Formen erfolgen. So kann z. B. die Datenbasis oder das LLM sowohl vor Ort (On-Premise) als auch bei einem Dienstleister (z. B. bei einem Cloud-Computing-Anbieter) betrieben werden, was aus Sicht des Datenschutzes zu unterschiedlichen Herausforderungen führt.

Datenschutzrechtliche Wirkung eines RAG-Systems

Die RAG-Methode kann positive Effekte auf die Richtigkeit und Nachvollziehbarkeit der Ausgaben eines KI-Systems entfalten, aber auch neue datenschutzrechtliche Herausforderungen schaffen. Der Ansatz ermöglicht in vielen Fällen, ein LLM ggf. vor Ort zu betreiben, das weniger umfangreiche Trainingsdaten benötigt. Das ergibt sich aus der Möglichkeit, die Ressourcen für den Betrieb zu reduzieren. Abhängig von der konkreten Konzeption kann z. B. ein kleineres LLM eingesetzt werden. Zusätzlich kommt diesem kleinen Modell zugute, dass es mit weniger Daten auskommt, was als Datenminimierung zu verstehen ist. Die geringere Größe des LLMs führt zusätzlich dazu, dass weniger Daten memorisiert werden. Dadurch sind ggf. weniger personenbezogene Daten aus dem KI-Modell extrahierbar. Zwar bleibt insbesondere die datenschutzrechtliche Beurteilung des Trainings des verwendeten Sprachmodells als solches unberührt, doch kann die Implementierung der RAG-Methode in einem KI-System im Ergebnis zu

einer differenzierten datenschutzrechtlichen Bewertung führen. Beispielhaft und nicht abschließend sei auf die Betroffenenrechte in den Art. 15 bis 17 DS-GVO verwiesen.

Bei richtiger Anwendung des Konzepts in einem RAG-System erfolgt die inhaltliche Beantwortung einer Anfrage zum überwiegenden Teil auf der Datenbasis, während das LLM hauptsächlich für die Aufbereitung der Antwort zuständig ist. Alternativ könnte das LLM auch mit den Daten aus der Datenbasis nachtrainiert werden. Im Vergleich zum durch nachträgliches Training eines LLMs (Fine Tuning) erzielten Ergebnis bietet das RAG-System aber realistische Möglichkeiten, den Betroffenenrechten gerecht zu werden. Mit Hilfe der Datenbasis können bei Bedarf Auskunftsanfragen der Betroffenen beantwortet (Art. 15 DS-GVO), Berichtigungen durchgeführt (Art. 16 DS-GVO) und daraus auch Daten gelöscht werden (Art. 17 DS-GVO). Auf der anderen Seite müssen Betreiber von RAG-Systemen über die auch für andere KI-Systeme geltenden Anforderungen hinaus besonderes Augenmerk u. a. auf die Qualität und Aktualität der Referenzdokumente sowie auf die Qualität der Datenaufbereitung und des Embeddings richten.

Rechtsgrundlagen für das Training mit personenbezogenen Daten

Auch die RAG-Methode lässt datenschutzrechtliche Fragen offen, z. B. zu den Rechtsgrundlagen des Trainings mit personenbezogenen Daten, zum Webscraping, zur Nutzung des Modells trotz unrechtmäßiger Datenverarbeitung bei dessen Training oder zur Wahrnehmung der Betroffenenrechte. Die Orientierungshilfe der DSK betrachtet diese Fragestellungen eingehender und gibt darüber hinaus eine Orientierung zur datenschutzkonformen Umsetzung in RAG-Systemen. Es soll auch erwähnt werden, dass unabhängig von hier angesprochenen LLMs in modernen RAG-Subsystemen bei der Suche zusätzlich spezialisierte LLMs zum Einsatz kommen, deren Verwendung erneut die bereits angesprochenen Fragen aufwirft.

Trotz der zu erwartenden positiven Wirkung von RAG-Systemen bei einigen datenschutzrechtlichen Problemfeldern von KI ist deshalb davon auszugehen, dass weitere technische und organisatorische Maßnahmen (z. B. Filter) ergriffen werden müssen. Dies ist notwendig, um einer Antwort auf die Frage nach der datenschutzkonformen Nutzung nicht datenschutzkonform trainierter LLMs näherzukommen. Als weitergehende Quelle sei auf die Stellungnahme 28/2024 des EDSA zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen verwiesen (Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, https://

www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_de).

Fazit

Das Prinzip des RAG kann bei sorgfältiger Konzeption positive Effekte auf die Richtigkeit und Nachvollziehbarkeit der Ausgaben eines KI-Systems entfalten. Es ermöglicht, einfacher als bei LLMs, Betroffenenrechte umzusetzen. Sprachsysteme lassen sich unabhängiger von den großen Tech-Konzernen aus USA oder China nutzen, indem man neben einem europäischen Small Language Model auf die Datenbasis einheimischer Unternehmen oder Verwaltungen zurückgreift. Dadurch kann nicht nur europäische KI wettbewerbsfähiger werden, sondern auch die digitale Souveränität Europas gestärkt und die Einhaltung datenschutzrechtlicher Vorgaben unterstützt werden.

RAG-Funktionen erzeugen aber auch neue datenschutzrechtliche Herausforderungen. Die Implementierung des Prinzips in einem KI-System erfordert eine sorgfältige datenschutzrechtliche Bewertung, insbesondere im Hinblick auf die Rechtsgrundlagen für das Training mit personenbezogenen Daten und die Wahrnehmung der Betroffenenrechte. Dies und die große Bandbreite möglicher Varianten erfordern hinsichtlich einer datenschutzrechtlichen Bewertung immer eine Betrachtung des Einzelfalls. Abschließend sei erwähnt, dass dieses Kapitel unter Zuhilfenahme eines in der hessischen Verwaltung in der Erprobung befindlichen KI-Systems erstellt wurde, das auch über RAG-Funktionen verfügt.

9.3
Kompetenzen für den KI-Einsatz in der öffentlichen Verwaltung

Um die Potenziale von Künstlicher Intelligenz zu nutzen und einen verantwortungsvollen und grundrechtskonformen KI-Einsatz in der Verwaltung zu stärken, unterstütze ich die Einführung von KI-Entwicklungen und -Anwendungen in der Landes- und Kommunalverwaltung in Hessen durch Schulungs- und Beratungsangebote.

Nach Art. 57 Abs. 1 Buchst. b und d und ErwG 132 DS-GVO gehört es zu meinen Aufgaben, die Öffentlichkeit zu den Risiken, Vorschriften, Garantien und Rechten im Zusammenhang mit der Verarbeitung personenbezogener Daten aufzuklären und die Verantwortlichen und die Auftragsverarbeiter zu den ihnen aus der Verordnung entstehenden Pflichten zu sensibilisieren.

Art. 57 DS-GVO

(1) Unbeschadet anderer in dieser Verordnung dargelegter Aufgaben muss jede Aufsichtsbehörde in ihrem Hoheitsgebiet

a) die Anwendung dieser Verordnung überwachen und durchsetzen;

b) die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung sensibilisieren und sie darüber aufklären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder;

c) im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten;

d) die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus dieser Verordnung entstehenden Pflichten sensibilisieren; (…)

ErwG 132 DS-GVO

Auf die Öffentlichkeit ausgerichtete Sensibilisierungsmaßnahmen der Aufsichtsbehörden sollten spezifische Maßnahmen einschließen, die sich an die Verantwortlichen und die Auftragsverarbeiter, einschließlich Kleinstunternehmen sowie kleiner und mittlerer Unternehmen, und an natürliche Personen, insbesondere im Bildungsbereich, richten.

Im Rahmen einer strategischen Initiative zur Unterstützung der öffentlichen Verwaltung in Hessen habe ich ein Fortbildungskonzept erarbeitet und hessischen Kommunen kostenfreie Schulungen angeboten. Hiermit habe ich das Ziel verfolgt, einerseits frühzeitig für die datenschutzrechtlichen, organisatorischen und technischen Herausforderungen des KI-Einsatzes zu sensibilisieren und andererseits zu erfahren, welche Themen und Fragestellungen aus Sicht der verantwortlichen Stellen von besonderer Bedeutung sind.

Diese Schulungen vermitteln Grundkenntnisse zur KI-VO, zur datenschutzrechtlichen und technischen Einschätzung von KI-Systemen sowie zur praktischen Anwendung der DS-GVO im Kontext der Anwendung von KI. Die vermittelten rechtlichen Inhalte wurden durch technische Erläuterungen ergänzt. In den zwei- bis dreistündigen Veranstaltungen wurden etwa die folgenden Fragestellungen behandelt:

– kritische Aspekte des Datenschutzes bei der Nutzung von KI-Systemen,
– KI-Systeme, generative KI-Systeme, verbotene Praktiken und Hochrisiko-KI-Systeme im Sinne der KI-Verordnung,
– Funktionsweise von Large Language Models,
– KI-Systeme mit Retrieval Augmented Generation (RAG),
– Einführung in die KI-Verordnung.

Neben diesem Fortbildungskonzept unterstützten Referentinnen und Referenten meiner Behörde auch andere Veranstaltungsformate rund um den KI-Einsatz in der Verwaltung. So fand in den Sitzungssälen des Hessischen Ministeriums des Innern, für Sicherheit und Heimatschutz (HMdI) beispielsweise ein „KI-Café“ statt, bei dem sich Mitarbeiterinnen und Mitarbeiter des HMdI an verschiedenen Ständen zu KI-Themen informieren und KI im praktischen Einsatz erleben konnten. Meine Behörde war mit einem eigenen Stand vertreten und erläuterte unter dem Motto „Grundrechte im Fokus – Datenschutz für eine vertrauenswürdige KI“ die Datenschutzimplikationen für KI-Systeme.

Zudem wurde in Kooperation mit dem Berufsverband der Datenschutzbeauftragten sowie mit Unterstützung der ekom21, des Hessischen Ministeriums für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum (HMWVW) und hessian.AI der Austausch zwischen verschiedenen Stakeholdern und kommunalen Datenschutzbeauftragten zu aktuellen KI-Themen ermöglicht. Für die Hessische Justiz wurde eine Fortbildungsveranstaltung mit dem Schwerpunkt „KI im Spannungsfeld zwischen Datenschutzrecht und Technik“ durchgeführt. Schließlich haben Referenten meiner Behörde im Rahmen der Personalversammlung des Regierungspräsidiums Gießen zu Fragen des Datenschutzes bei der Einführung von KI-Systemen referiert.

Außerdem habe ich im Forum des Competence Center for Applied Security Technologies (CAST) e. V. in Darmstadt am 6. März 2025 eine Tagung zum Thema „Datenschutzgerechter Umgang mit Künstlicher Intelligenz – Anforderungen der KI-VO und DS-GVO in der Praxis“ durchgeführt. Die Vorträge dieser Tagung wurden in Heft 5 der Zeitschrift „Datenschutz und Datensicherheit“ (DuD) publiziert (DuD 2025, 273 ff.).

Daneben habe ich selbst sowie Mitarbeiter und Mitarbeiterinnen meiner Behörde mehrere Vorträge zum Datenschutz bei der Entwicklung, dem Training und der Nutzung von Künstlicher Intelligenz gehalten (s. detailliert Kap. 17).

Ausblick

Die hohe Teilnehmerzahl, die angeregten Diskussionen und die positive Rückmeldung der Teilnehmenden bestätigen nicht nur den Bedarf entsprechender Angebote, sie bestärken mich auch darin, das Schulungs- und Beratungsangebot weiter auszubauen.

Für 2026 sind daher bereits weitere Schulungen, Vorträge und Austauschformate geplant, die sich beispielsweise vertiefend mit der Umsetzung der KI-VO und ihren Schnittstellen zur DS-GVO befassen.

9.4
Rechtsrahmen für die öffentliche Verwaltung

Immer öfter setzen Behörden aus unterschiedlichen Bereichen der öffentlichen Verwaltung für die Erfüllung ihrer Aufgaben Systeme Künstlicher Intelligenz ein. Um zu vermeiden, dass dies unter Verstoß gegen datenschutzrechtliche Vorgaben erfolgt, könnten gesetzliche Regelungen zum Einsatz von KI in der öffentlichen Verwaltung hilfreich sein. Anlass dafür, sich mit dieser Frage zu befassen, bot die öffentliche Anhörung des Ausschusses für Digitales, Innovation und Datenschutz zum Gesetzentwurf der Fraktion BÜNDNIS 90/ DIE GRÜNEN zu einem Gesetz zur Anwendung von Künstlicher Intelligenz in der Verwaltung (HKIVerwG) – LT-Drs. 21/2273.

Regelungsbedarf

Art. 2 Abs. 7 KI-VO bestimmt, dass die KI-VO die DS-GVO „unberührt" lässt. Die DS-GVO enthält jedoch keine spezifischen Regelungen zur Verarbeitung personenbezogener Daten im Kontext der Herstellung oder des Betriebs von KI-Systemen. Sie enthält im Gegenteil Regelungen, die im Widerspruch dazu stehen (z. B. Grundsätze der Datenverarbeitung in Art. 5 Abs. 1 DS-GVO wie z. B. das Minimierungsgebot), die in KI-Systemen (insbesondere in Large Language Models) nicht umgesetzt werden können (wie z. B. Berichtigung und Löschung nach Art. 16 und 17 DS-GVO) und die Regelungslücken aufweisen. Solche Regelungslücken ergeben sich aus fehlenden Erlaubnistatbeständen für verschiedene Phasen der Nutzung von personenbezogenen Daten bei der Herstellung und beim Betrieb von KI-Systemen.

Eine solche Lücke ergibt sich insbesondere aus einer fehlenden datenschutzrechtlichen Erlaubnis in Art. 6 Abs. 1 und 9 Abs. 2 DS-GVO für das Training von LLMs mit personenbezogenen Daten durch Behörden. Während sich private Verantwortliche dafür unter Umständen auf die Erlaubnis für überwiegende berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO berufen können (s. EDSA, Stellungnahme 28/2024, Ziff. 3.3.), ist dies Behörden in Ausübung ihrer hoheitlichen Aufgaben nach Art. 6 Abs. 1 UAbs. 2 DS-GVO verwehrt. Auch eine datenschutzrechtliche Erlaubnis für die Verarbeitung von besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 2 Buchst. g DS-GVO fehlt.

Nach Art. 22 Abs. 1 DS-GVO ist die Übertragung automatisierter Entscheidungen auf ein KI-System verboten, die die betroffene Person erheblich beeinträchtigen. Nach Art. 22 Abs. 2 Buchst. b DS-GVO kann eine Regelung in einem Mitgliedstaat solche Entscheidungen ermöglichen. Eine solche Regelung besteht jedoch bisher nicht. § 35a HVwVfG eröffnet nur die Möglichkeit einer solchen Regelung, enthält diese aber selbst nicht.

Auch das HDSIG enthält keine spezifischen Regelungen für die besonderen Probleme der Herstellung und des Einsatzes von KI-Systemen in der hessischen Verwaltung.

In der Praxis wird versucht, die fehlenden Regelungen durch teleologische Interpretationen bestehender Regelungen zu ersetzen. Dies gelingt aber nur mit sehr unterschiedlichem Erfolg. Diese Versuche hinterlassen oft eine hohe Rechtsunsicherheit, weil auch immer gegenteilige Interpretationen möglich erscheinen.

Spezifische datenschutzrechtliche Regelungen zu den besonderen Bedingungen der Verarbeitung personenbezogener Daten in KI-Systemen sind somit zumindest zur Gewährleistung der erforderlichen Rechtssicherheit für den Einsatz von KI in der hessischen Verwaltung notwendig, in der Frage der Erlaubnistatbestände sogar für deren Rechtmäßigkeit. Diese Rechtssicherheit ist zum einen notwendig, um den Einsatz von KI-Systemen in der öffentlichen Verwaltung zu beschleunigen, und zum anderen, um den Mitarbeitenden in der öffentlichen Verwaltung, die KI-Systeme einsetzen, ausreichende Handlungssicherheit zu geben.

Daher haben andere Bundesländer bereits vergleichbare Regelungen zu den datenschutzrechtlichen Problemen beim Einsatz von KI-Systemen in der öffentlichen Verwaltung getroffen: Die Hansestadt Hamburg hat in § 13 ihres Gesetzes für die Digitale Verwaltung (HmbVwDiG) vom 19. November 2024 (HmbGVBl. 2024, 575; Senats-Drs. 22/15763) einen eigenen Erlaubnistatbestand für den Einsatz von KI-Systemen in der öffentlichen Verwaltung geschaffen und hierfür Rahmenbedingungen festgelegt. Schleswig-Holstein hat zumindest in § 12 des IT-Einsatzgesetzes (ITEG) vom 16. März 2022 (GVOBl. SH 2022, 285) eine Regelung zur KI-Rüge getroffen. In Baden-Württemberg hat die Landesregierung am 23. September 2025 einen Entwurf für Änderungen des Landesdatenschutzgesetzes beschlossen, in dem ein Erlaubnistatbestand für die Nutzung von KI-Systemen in der öffentlichen Verwaltung (§ 3a), ein Erlaubnistatbestand für die Anonymisierung (§ 4 Abs. 2), Regelungen zur Berichtigung (§ 9a) und Löschung (§ 10 Abs. 4) in KI-Systemen, ein Erlaubnistatbestand für das Training von KI-Systemen (§ 11a), eine Regelung zum Einsatz von KI-Systemen im Beschäftigungsverhältnis (§ 15 Abs. 9) sowie Erlaubnistatbestände für Video- und technische Überwachung (§§ 18 Abs. 6, 18a und 18b) enthalten sind. In Berlin wird ebenfalls eine Regelung mit Erlaubnistatbeständen und Schutzmaßnahmen vorbereitet. Schließlich hat die Europäische Kommission in ihrem Vorschlag für eine Reform der DS-GVO im Rahmen ihrer Digitalen Omnibus-Verordnung vom 15. November 2025 spezifische Regelungen für das Training und den

Einsatz von KI-Systemen in einem neuen Art. 9 Abs. 2 Buchst. k und Abs. 5 und einem neuen Art. 88c DS-GVO vorgesehen.

Zulässigkeit spezifischer Regelungen

Für die hessische Verwaltung darf der hessische Gesetzgeber gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. e, Abs. 2 und 3 DS-GVO spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen und spezifische Bestimmungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen erlassen. Für Regelungen zur Verarbeitung besonderer Kategorien personenbezogener Daten, die aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist, kann er sich auf Art. 9 Abs. 2 Buchst. g DS-GVO berufen. Nach Art. 22 Abs. 2 Buchst. b DS-GVO kann er Ausnahmen vom Verbot automatisierter Entscheidungen des Art. 22 Abs. 1 DS-GVO vorsehen. Schließlich sind Beschränkungen der Grundsätze der Datenverarbeitung in Art. 5 DS-GVO und der Rechte der betroffenen Person etwa nach Art. 16 und 17 DS-GVO nach Art. 23 Abs. 1 DS-GVO möglich.

Spezifische Datenschutzregelungen sind auch nach der KI-Verordnung zulässig. Sie kann nach ihrem ErwG 63 Satz 3 „nicht so verstanden werden, dass sie eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten, gegebenenfalls einschließlich besonderer Kategorien personenbezogener Daten, bildet, es sei denn, in dieser Verordnung ist ausdrücklich etwas anderes vorgesehen“.

Im Ergebnis sind somit die datenschutzrechtlich notwendigen Regelungen auch unionsrechtlich zulässig.

Notwendigkeit spezifischer Regelungen

Die KI-VO regelt umfangreich und detailliert Künstliche Intelligenz als Produkt. Ihre Regelungen erstrecken sich daher auf das Herstellen, das Anbieten, die Einfuhr und den Betrieb von KI-Systemen. Sie regelt jedoch nicht den Einsatz dieser Produkte in unterschiedlichen Bereichen. Ob KI-Systeme in der Verwaltung eingesetzt werden dürfen oder sollen und welche Bedingungen dabei zu beachten sind, lässt die KI-VO offen. Auch der Vorschlag der Europäischen Kommission zu einem neuen Art. 88c DS-GVO gilt nur für nicht-öffentliche Stellen und würde eine Regelung für öffentliche Stellen in Hessen nicht überflüssig machen.

Sofern beim Einsatz von KI-Systemen in der öffentlichen Verwaltung bestimmte grundrechtsrelevante Anforderungen zu beachten sind, erfordert der Wesentlichkeitsgrundsatz eine gesetzliche Regelung des Schutzes

der betroffenen Grundrechte. Auf die Aufgaben der hessischen Verwaltung bezogen fehlen aber bisher grundrechtsschützende Voraussetzungen für den Einsatz von KI.

Auch hier gilt, dass diese Voraussetzungen für den Einsatz und Bedingungen während des Einsatzes unter Umständen aus allgemeinen verfassungsrechtlichen Vorgaben abgeleitet werden können. Soll der schnelle Einsatz von KI durch die Rechtsunsicherheit solcher Ableitungen nicht beeinträchtigt oder in Frage gestellt werden, sind klare Regelungen zu Voraussetzungen und Bedingungen notwendig.

Regelungsthemen

Diese Regelungen sollten u. a. folgende Inhalte betreffen:

Der Anwendungsbereich sollte die gesamte öffentliche Verwaltung des Landes umfassen, für bestimmte Anwendungen von KI-Systemen wie etwa oder zur Erfüllung der Aufgaben der Polizei oder des Verfassungsschutzes aber Ausnahmen vorsehen.

Training und Einsatz von KI sollten den Behörden ausdrücklich erlaubt sein. Um die Verarbeitung personenbezogener Daten zu vermeiden, sollten diese zuvor anonymisiert oder pseudonymisiert werden. Die Verarbeitung personenbezogener Daten sollte nur erlaubt sein, wenn ein effektives Training oder ein effektiver Einsatz der KI-Systeme ohne sie nur mit unverhältnismäßigem Aufwand oder nicht auf andere Weise erfolgen kann. Hierfür dürfen rechtmäßig erhobene Daten zweckändernd eingesetzt werden. Für die Verarbeitung besonderer Kategorien von Daten sollte eine Regelung in Ausfüllung von Art. 9 Abs. 2 Buchst. g DS-GVO feststellen, unter welchen Umständen ein Training mit besonderen Kategorien personenbezogener Daten „aus Gründen eines erheblichen öffentlichen Interesses erforderlich“ ist.

Zur Ausfüllung der Regelungen zum automatisierten Verwaltungsakt in § 35a HVwVfG und zur Begründung von Verwaltungsakten in § 39 HVwVfG sollte ein KI-Gesetz spezifische verwaltungsverfahrensrechtliche Regelungen enthalten, die automatisierte Verwaltungsakte bei gebundenen Verwaltungsakten erlaubt und die Anforderungen an ihre Begründung regelt und dabei spezifische Eigenschaften von KI-Systemen berücksichtigt. Mit dieser Regelung sollte eine Ausnahme nach Art. 22 Abs. 2 Buchst. c DS-GVO vom Verbot automatisierter Entscheidungen, die Rechtswirkungen nach Art. 22 Abs. 1 DS-GVO aufweisen, begründet werden.

Zu regeln wäre auch, wie Betroffenenrechte auf Berichtigung nach Art. 16 DS-GVO, auf Löschung nach Art. 17 DS-GVO und auf Einschränkung der

Datenverarbeitung nach Art. 18 DS-GVO unter den eingeschränkten Bedingungen von KI verwirklicht werden können.

Schließlich wäre zu erwägen, KI-Rüge einzuführen, wie sie § 12 des IT-Einsatz-Gesetzes (ITEG) Schleswig-Holstein vom 16. März 2022 kennt. Mit der KI-Rüge soll jeder Adressat einer auf KI-Systemen beruhenden Entscheidung innerhalb eines Monats ab Bekanntgabe der Entscheidung verlangen können, dass diese durch eine natürliche Person überprüft und bestätigt oder geändert oder aufgehoben wird.

Ausblick

Auch wenn der konkrete Gesetzentwurf in LT-Drs. 21/2273 von der Mehrheit des Ausschusses abgelehnt wurde, besteht die Notwendigkeit spezifischer Regelungen des Datenschutzes und des Verwaltungsverfahrens weiterhin. Dem hessischen Gesetzgeber ist daher zu empfehlen, die angesprochenen Regelungsthemen – wie auch in anderen Bundesländern – in spezifischen gesetzlichen Regelungen aufzugreifen.

10. Internet und Medien

Viele Privatpersonen nutzen Onlinedienste, um Daten, Bilder und Filme einer großen Anzahl von Empfängern zugänglich zu machen. Sie überschreiten damit die Grenze der rein privaten Datenverarbeitung, unterfallen dadurch der DS-GVO, können aber deren Anforderungen für diese Form der Datenverarbeitung nicht erfüllen (Kap. 10.1). Im Berichtszeitraum wurde ein Prüfverfahren gegen die chinesische intelligente Chatbot-Anwendung DeepSeek durchgeführt, weil der Verdacht besteht, dass bei der Nutzung von DeepSeek personenbezogene Daten unberechtigt nach China übertragen werden (10.2).

10.1
Datenschutzverstöße in Onlinediensten durch Privatpersonen

Bei unzähligen Internetdiensten kann man zu privaten Zwecken Informationen, Fotos, Videos und sonstige Daten speichern, veröffentlichen oder mit anderen teilen. Wenn Nutzerinnen und Nutzer dort jedoch nicht nur Daten, Bilder oder Videos von sich selbst, sondern auch von anderen Personen veröffentlichen, steht immer die mögliche Anwendbarkeit der DS-GVO im Raum. Diese Konstellation birgt Schwierigkeiten für alle Beteiligten, da Privatpersonen oft kaum in der Lage sind, datenschutzrechtliche Anforderungen ausreichend zu erfüllen, und sich ihrer Verpflichtung dazu regelmäßig auch gar nicht bewusst sind.

Das Datenschutzrecht soll insbesondere Schutz davor bieten, dass staatliche und größere private Stellen wie Unternehmen oder Vereine bei der Verarbeitung von Daten zu weit in das Persönlichkeitsrecht der Betroffenen eingreifen. Um Betroffene umfassend zu schützen, ist der Anwendungsbereich der DS-GVO aber bewusst weiter gefasst als nur auf Behörden oder Unternehmen bezogen. Vielmehr ist jede „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“ (Art. 4 Nr. 7 DS-GVO) „Verantwortlicher“ im Sinne des Datenschutzrechts und muss dieses beachten und alle datenschutzrechtlichen Anforderungen erfüllen. Diese Pflichten können somit auch jede Privatperson treffen, die personenbezogene Daten anderer verarbeitet.

Fallgruppen

Die Konstellation, dass Privatpersonen für die Verarbeitung von Daten anderer Personen datenschutzrechtlich verantwortlich sind, ergibt sich besonders häufig bei der Nutzung von Onlinediensten. Diese stehen jedermann offen,

um Informationen, Fotos, Videos und sonstige Daten – auch von anderen Personen – zu allen möglichen Zwecken zu speichern, zu veröffentlichen oder anderweitig mit anderen zu teilen. Mich erreicht daher jedes Jahr eine Vielzahl von Beschwerden und Hinweisen zu Privatpersonen, die Daten oder Bilder anderer Personen in irgendeiner Form online preisgegeben haben.

Am häufigsten betrifft dies die Nutzung von Social Media. Viele Nutzer von Social Media-Diensten teilen darüber Informationen aus ihrem Leben mit der Öffentlichkeit. Nicht selten beinhaltet dies auch Namen, Bilder oder Informationen von anderen Personen und nicht immer sind diese mit der Veröffentlichung einverstanden.

Aber auch sowohl selbst betriebene als auch fremde Websites (z. B. Webforen) werden immer wieder dazu genutzt, Bilder und Informationen von anderen Personen zu veröffentlichen und zu verbreiten. Vereinzelt werden auch auf Plattformen für Rezensionen, die der Bewertung von Produkten und Dienstleistungen dienen, beispielsweise einzelne Mitarbeiter eines bewerteten Geschäfts namentlich genannt. Schließlich kommt es gelegentlich auch vor, dass bei privaten Verkaufsanzeigen auf den zahllosen Verkaufsplattformen Daten oder Abbildungen von Dritten in Produktbeschreibungen oder Produktfotos veröffentlicht werden.

Die Gründe für die Veröffentlichung von Daten und Bildern anderer Personen durch Privatpersonen sind dabei vielfältig. Bei der Nutzung von Social Media geschieht dies oft mehr oder weniger beiläufig im Rahmen des sozialen Austauschs, der diesen Diensten schon namentlich inhärent ist. Auch in vielen Webforen findet ein intensiver Meinungsaustausch zwischen untereinander häufig bekannten Teilnehmern statt, der letztlich einer lebhaften Diskussion unter Bekannten oder Vereinsmitgliedern ähnelt, aber eben dauerhaft gespeichert und öffentlich abrufbar ist. In solchen Konstellationen erfolgt die Nennung von Daten Dritter teilweise einfach unbedarft und ohne Bewusstsein dafür, dass dies, anders als bei persönlichem Kontakt, von einer Vielzahl von Menschen wahrgenommen werden und die Betroffenen auch beeinträchtigen kann. Häufig dient die namentliche Nennung einzelner Personen oder die Veröffentlichung von deren Daten und Bildern allerdings auch ganz bewusst und gezielt dem Zweck, Streitigkeiten mit diesen Personen öffentlich zu machen und auf den Onlinebereich auszuweiten. Dabei werden die Betroffenen häufig gezielt beleidigt und vor einer möglichst breiten Online-Öffentlichkeit bloßgestellt.

Anwendbarkeit der DS-GVO

In all diesen Fällen initiieren jeweils Privatpersonen die digitale Verarbeitung und Veröffentlichung von Daten anderer Personen. Dabei bestimmen sie

die Zwecke und Mittel der Verarbeitung, indem sie sich für eine bestimmte Plattform und einen bestimmten Weg der Veröffentlichung entscheiden, die sie für ihre jeweiligen individuellen Zwecke nutzen. Auch wenn sie die dafür genutzte Plattform (z. B. Social Media-Dienst) in aller Regel nicht selbst betreiben, sind sie dafür verantwortlich, dass die Daten auf der Plattform zu finden sind und somit Verantwortliche im Sinne des Datenschutzrechts.

Allerdings dient das Datenschutzrecht primär der Regulierung von staatlichen Stellen und Unternehmen, die für ihre jeweiligen Ziele in großem Umfang personenbezogene Daten verarbeiten. Viel mehr als Privatpersonen können diese mit ihrer staatlichen oder wirtschaftlichen Macht Druck auf Betroffene ausüben und haben daher deutlich größeres Potenzial, Gefahren für die Privatsphäre darzustellen und Betroffene in der Ausübung ihrer Freiheiten einzuschränken. Dem Datenschutzrecht liegt somit auch die Annahme eines üblicherweise bestehenden Machtgefälles zwischen den Verantwortlichen und den Betroffenen zugrunde.

Um ein Ausufern der Anwendung des Datenschutzrechts über solche Konstellationen hinaus zu verhindern, hat der Gesetzgeber bestimmte Voraussetzungen für die Anwendbarkeit der DS-GVO bzw. Ausnahmen von dieser vorgesehen. Diese sind in den o. g. Fallgruppen allerdings nur teilweise einschlägig.

Ein einstmals wichtiges Kriterium im Datenschutzrecht ist und war das der „automatisierten Verarbeitung“, das auch heute noch eine der Voraussetzungen für die Anwendbarkeit der DS-GVO ist. In den „Kindertagen“ des Datenschutzrechts war die automatisierte Datenverarbeitung ein Privileg staatlicher Stellen und großer Unternehmen, da nur diese die finanziellen und technischen Ressourcen aufbringen konnten, die die automatisierte Verarbeitung von Daten damals erforderte. So konnte früher allein anhand dieses Kriteriums der Anwendungsbereich des Datenschutzrechts auf größere staatliche und wirtschaftliche Akteure beschränkt und der Umgang mit Daten durch Privatpersonen weitgehend von der Datenschutzgesetzgebung ausgeschlossen werden.

Allerdings haben sich seit den ersten Datenschutzgesetzen die technischen Hintergründe der Datenverarbeitung komplett verändert. Ausnahmslos alle staatlichen Stellen, Unternehmen, Vereine und andere Stellen verarbeiten Daten heute selbstverständlich digital, aber auch nahezu jede Privatperson besitzt mehrere Geräte, die die Rechenleistung früherer Großrechner um ein Vielfaches übertreffen. Da heute auch im Privaten die digitale Datenverarbeitung der Normalfall ist, ist das Kriterium der automatisierten Verarbeitung zur Abgrenzung geringer Fälle heute nahezu irrelevant.

Relevant ist hingegen die in Art. 2 Abs. 2 Buchst. c DS-GVO geregelte sog. Haushaltsausnahme, mit der der Gesetzgeber rein private Sachverhalte vom Datenschutzrecht ausgenommen hat. Danach findet die DS-GVO keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Obwohl diese Ausnahme gerade verhindern soll, dass Privatpersonen mit datenschutzrechtlichen Pflichten konfrontiert werden, wenn sie zu rein privaten oder familiären Zwecken Daten verarbeiten, ist ihre Reichweite umstritten und ihre Anwendung im Zusammenhang mit Onlinediensten nicht unproblematisch. Die Verarbeitung und Veröffentlichung von personenbezogenen Daten im Internet bringt es mit sich, dass diese Daten zumindest theoretisch weltweit abrufbar sind. Auch wenn der oder die Verantwortliche mit der Veröffentlichung nur private Zwecke verfolgt, kann diese doch enorme Auswirkungen haben und die Daten des oder der Betroffenen können von einem Personenkreis wahrgenommen werden, der weit über private oder familiäre Kreise hinausgeht.

Letztlich kommt es auf die jeweilige Konstellation im Einzelfall an, ob ausnahmsweise die Haushaltsausnahme greift, wie es ErwG 18 DS-GVO z. B. bei der Nutzung von Social Media zumindest für möglich erachtet. So erreichte mich beispielsweise eine Beschwerde, deren Hintergrund eine Meinungsverschiedenheit unter Verwandten war. Jemand hatte ein Foto seines eigenen Unterschenkels, auf dem Porträts eines kürzlich verstorbenen und eines noch lebenden Familienmitglieds tätowiert sind, auf einem privaten Social Media Account veröffentlicht, worüber sich der lebende Porträtierte beschwerte. In dieser Konstellation stehen innerfamiliäre und höchstpersönliche Aspekte (Trauerverarbeitung) im Vordergrund, weshalb diese Datenverarbeitung nur schwierig nach Datenschutzrecht zu bewerten ist.

Schwierigkeiten bei der Anwendung des Datenschutzrechts

Wenn die Haushaltsausnahme nicht zum Tragen kommt, kann die Anwendbarkeit des Datenschutzrechts in solchen Konstellationen aus verschiedenen Gründen Schwierigkeiten mit sich bringen.

Die DS-GVO gilt uneingeschränkt und nimmt aufgrund ihrer Risikoneutralität kaum Abstufungen hinsichtlich der Anforderungen an verschiedene Arten von Verantwortlichen vor. Somit unterliegen verantwortliche Privatpersonen weitgehend den gleichen Pflichten wie internationale Konzerne. Damit benötigen sie insbesondere eine Rechtsgrundlage für die Datenverarbeitung und müssen die Rechte der Betroffenen beachten und z. B. auf deren Wunsch Auskunft über die von ihnen verarbeiteten Daten erteilen oder deren Daten löschen. Daneben müssen sie gegebenenfalls technische und/oder organi-

satorische Maßnahmen ergreifen, um die Sicherheit der Datenverarbeitung sicherzustellen und möglicherweise weitere Anforderungen zu erfüllen. All dies ist den meisten Privatpersonen nicht einmal bekannt und von ihnen, im Gegensatz zu professionellen datenverarbeitenden Stellen, kaum sinnvoll und hinreichend umzusetzen.

Vereinzelt kommt es sogar vor, dass die oder der Verantwortliche noch gar nicht volljährig ist. Viele Social Media-Anbieter sehen ein Mindestalter für ihre Nutzerinnen und Nutzer von 16 oder sogar nur 13 Jahren vor, so dass auch Jugendliche diese Dienste nutzen können. Veröffentlichen sie dabei Daten von anderen, können auch sie grundsätzlich dafür datenschutzrechtlich verantwortlich sein. Die DS-GVO sieht zwar einige Regelungen zum Schutz von minderjährigen Betroffenen vor, kennt aber keine Einschränkungen oder spezielle Regeln für den Fall, dass Minderjährige selbst datenschutzrechtlich Verantwortliche sind. Dabei ist es in solchen Fällen noch unwahrscheinlicher als bei volljährigen Verantwortlichen, dass datenschutzrechtliche Pflichten beachtet und erfüllt werden können und zudem fraglich ist, ob überhaupt bereits die nötige geistige Reife dafür vorliegt. Schließlich erachtet der Gesetzgeber in Art. 8 DS-GVO für Jugendliche als Betroffene (aber nicht als Verantwortliche) in der Regel erst ab 16 Jahren eine ausreichende Einsichtsfähigkeit für gegeben. Auch eine Konfrontation mit der Aufsichtsbehörde wäre in solchen Fällen schwierig, da Minderjährige im Verwaltungsverfahren von Erziehungsberechtigten vertreten werden müssen.

Auch wenn sich Betroffene mit einer Beschwerde an mich oder eine andere Datenschutzaufsichtsbehörde wenden, führt die Befassung mit Streitigkeiten zwischen Privatpersonen häufig zu Problemen. So sind datenschutzrechtlich verantwortliche Privatpersonen teilweise mit dem Kontakt mit meiner Behörde überfordert oder z. B. aus gesundheitlichen Gründen gar nicht in der Lage, angemessen in einem Verwaltungsverfahren zu agieren. Anders als bei der zivilrechtlichen Rechtsverfolgung, die auf die Beilegung von Streitigkeiten zwischen Privatpersonen ausgerichtet ist, sind das datenschutzrechtliche Beschwerdeverfahren und das Verwaltungsrecht nicht darauf ausgelegt und nicht optimal geeignet, solche Streitigkeiten zu klären. Oftmals stehen in solchen Fällen hinter einem vordergründig thematisierten Datenschutzverstoß viel grundlegendere Streitigkeiten mit anderen rechtlichen und tatsächlichen Hintergründen (z. B. Streitigkeiten unter Ex-Lebenspartnern, Nachbarschaftsstreitigkeiten, Auseinandersetzungen mit gewerblichen Konkurrenten etc.). In diesen Fällen kann eine auf das Datenschutzrecht beschränkte Entscheidung ohnehin keine dauerhafte Lösung des Konflikts herbeiführen.

Letztlich geht es in entsprechenden Fällen häufig um verhältnismäßig geringe Verletzungen des Persönlichkeitsrechts, die zwar theoretisch einer

breiten Internet-Öffentlichkeit zugänglich sind, faktisch aber doch nur von einer geringen Anzahl von Personen wahrgenommen werden. Gerade im Bereich von Social Media oder Webforen ist der Kreis derjenigen, die die entsprechenden Posts lesen und wahrnehmen, oft relativ klein und auf einen gemeinsamen Bekanntenkreis begrenzt. Eine ausführliche Befassung meiner Behörde mit solchen Fällen erscheint daher nicht immer verhältnismäßig. Dies gilt insbesondere vor dem Hintergrund der vielfältigen Aufgaben einer Datenschutzbehörde und der Notwendigkeit, sich mit schwerwiegenden Verstößen solcher Verantwortlicher auseinanderzusetzen, die in großem Maße personenbezogene Daten verarbeiten.

Umgang mit entsprechenden Fällen

Erreichen mich Beschwerden oder Hinweise aus den oben genannten Fallgruppen, ist zunächst zu klären, ob das Datenschutzrecht trotz der Ausübung privater Tätigkeiten anwendbar ist. Ist dies der Fall, ist anhand der Umstände im Einzelfall zu klären, in welchem Umfang das weitere Vorgehen dem jeweiligen Fall angemessen ist. Dabei berücksichtige ich auch die Schwere und Bedeutung des möglichen Verstoßes im Verhältnis zu anderen Beschwerden, bei denen möglicherweise eine große Zahl von Personen betroffen ist oder systematische Datenschutzverstöße durch Unternehmen oder staatliche Stellen im Raume stehen.

In manchen Fällen sind umfangreichere Maßnahmen gegenüber datenschutzrechtlich verantwortlichen Privatpersonen geboten und nötig, z. B. wenn unbelehrbare Personen in einer Vielzahl von Fällen die Persönlichkeitsrechte anderer bewusst immer wieder verletzen. Bei der Mehrzahl der Fälle aus den o. g. Fallgruppen handelt es sich jedoch eher um Einzelfälle, die vorwiegend private Streitigkeiten zwischen den jeweiligen Betroffenen und Verantwortlichen betreffen. In solchen Fällen ist regelmäßig ein Vorgehen angemessen und ausreichend, bei dem zum Beispiel die Verantwortlichen auf ihre Verstöße hingewiesen werden, Tipps zu rechtskonformem Verhalten erhalten und auf deutlich schwerwiegendere Folgen im Falle einer Wiederholung aufmerksam gemacht werden.

Neben der Beschwerde bei einer Aufsichtsbehörde steht Betroffenen in solchen Konstellationen natürlich immer auch die Möglichkeit offen, sich zivilrechtlich gegen Persönlichkeitsrechtsverletzungen durch Privatpersonen zur Wehr zu setzen. Auf diese Weise können Betroffene, nötigenfalls auch mit anwaltlicher Unterstützung oder auf gerichtlichem Wege, zudem auch Schadensersatz nach Art. 82 DS-GVO für durch eine Datenschutzverletzung erlittene Schäden geltend machen. Dies ist im aufsichtsbehördlichen Beschwerdeverfahren hingegen nicht möglich.

10.2
Prüfverfahren gegen DeepSeek

Im Jahr 2025 begann eine Prüfung des chinesischen Unternehmens DeepSeek durch mehrere Landesdatenschutzbeauftragte. DeepSeek bietet Anwendungen Künstlicher Intelligenz in Deutschland an und muss daher die DS-GVO einhalten.

Im Februar 2025 habe ich gemeinsam mit den Landesdatenschutzbeauftragten aus Baden-Württemberg, Berlin, Bremen, Rheinland-Pfalz, Sachsen-Anhalt und Thüringen ein Prüfverfahren gegen das chinesische Unternehmen Hangzhou DeepSeek Artificial Intelligence Co., Ltd. (DeepSeek) eingeleitet. Da das Unternehmen seine Anwendung der Künstlichen Intelligenz, DeepSeek, unter anderem in Deutschland etwa in Form einer Website sowie über Apps mit deutscher Beschreibung und in deutscher Sprache anbietet, unterliegt es den Regelungen der DS-GVO. Daher stimme ich mich mit meinen Kolleginnen und Kollegen auf nationaler sowie auf europäischer Ebene ab, um eine gemeinsame Vorgehensweise und damit eine kohärente Rechtsanwendung der DS-GVO in Deutschland und der EU zu erreichen.

Zunächst war zu klären, ob DeepSeek gemäß Art. 27 Abs. 1 DS-GVO überhaupt einen Vertreter in der EU benannt hat. Nach dieser Regelung besteht für Verantwortliche oder Auftragsverarbeiter, die nicht in der EU niedergelassen sind, aber dennoch dort ihre Dienstleistungen anbieten, die Pflicht, einen Vertreter in der EU zu benennen. Damit soll sichergestellt werden, dass auch Unternehmen aus dem nicht-europäischen Ausland die Pflichten der Datenschutzgrundverordnung beachten, indem deren benannter Vertreter als Ansprechpartner fungiert und die Einhaltung der Datenschutzvorschriften sicherstellt. Erst in Folge unserer koordinierten Prüfung hat DeepSeek tatsächlich einen solchen Vertreter in der EU benannt.

Datenschutzrechtlich bedenklich ist außerdem, dass – nach derzeitigem Kenntnisstand – bei der Nutzung von DeepSeek umfangreiche personenbezogene Daten der Nutzenden wie Texteingaben, Chatverläufe oder hochgeladene Dateien an chinesische Auftragsverarbeiter übermittelt und auf Servern in China gespeichert werden. Datenübermittlungen in Drittländer wie China sind nach Art. 46 Abs. 1 DS-GVO allerdings nur zulässig, wenn den betroffenen Personen garantierte durchsetzbare Rechte sowie wirksame Rechtsbehelfe zur Verfügung stehen.

Meine Kolleginnen, Kollegen und ich sind jedoch nicht davon überzeugt, dass die Daten deutscher Nutzender in China auf einem der EU gleichwertigen Niveau geschützt sind. Denn chinesische Behörden besitzen umfangreiche Zugriffsrechte auf personenbezogene Daten, die bei chinesischen Unterneh-

men verarbeitet werden. Außerdem haben Nutzer von DeepSeek in China keine durchsetzbaren Rechte oder wirksamen Rechtsbehelfe, wie sie durch die DS-GVO in der EU gewährleistet werden.

Daher haben wir das Unternehmen im Mai 2025 aufgefordert, seine Apps selbstständig aus den deutschen App Stores zu entfernen, die rechtswidrige Datenübermittlung nach China einzustellen oder die gesetzlichen Voraussetzungen für eine rechtmäßige Übermittlung in Drittstaaten zu erfüllen. Dem ist DeepSeek allerdings bisher nicht nachgekommen. Aus diesem Grund hat meine Berliner Kollegin im Rahmen unseres gemeinsam betriebenen Verfahrens im Juni 2025 die Applikation von DeepSeek gegenüber den Betreibern der Appstores von Apple und Google als rechtswidrigen Inhalt im Sinne des Digital Services Act gemeldet.

Internationale Reaktionen auf DeepSeek sind ebenfalls kritisch. In Italien wurde die App aufgrund von Datenschutzbedenken blockiert. Auch in Tschechien wurde die App wegen Sicherheitsbedenken verboten. In den Niederlanden kündigte die Datenschutzbehörde eine Untersuchung der Datenpraktiken von DeepSeek an. In Südkorea wurde die App vorübergehend aus den App-Stores entfernt, nachdem festgestellt wurde, dass Nutzerdaten ohne Zustimmung nach China übertragen wurden.

Um den hessischen Nutzenden vorübergehend Unterstützung bei der Auswahl des richtigen KI-Tools sowie bei dessen Verwendung zu bieten, habe ich Empfehlungen für den Umgang mit Anwendungen Künstlicher Intelligenz von Anbietern außerhalb der EU veröffentlicht. Dadurch sollen die mit dem Einsatz solcher Anwendungen verbundenen Risiken zumindest eingeschränkt werden können. Diese finden sich auf meiner Homepage unter der Rubrik „Künstliche Intelligenz“ (https://datenschutz.hessen.de/datenschutz/kuenstliche-intelligenz/empfehlungen-zum-einsatz-von-ki-anwendungen-von-anbietern-ausserhalb-der-eu).

11. Werbung und Adresshandel

Werbeunternehmen und Adresshändler verarbeiten gewerblich viele personenbezogene Daten und verursachen durch die Menge der personenbezogenen Daten und die Zielsetzung der Verarbeitung besondere datenschutzrechtliche Risiken. Diesen korrespondieren besondere Pflichten und ein hohes Maß an Verantwortung. Sie dürfen Zweckänderungen von Daten für Werbeaktionen nur unter sehr eingeschränkten Bedingungen vornehmen (Kap. 11.1). Um Werbewidersprüche automatisiert zu beachten, müssen sie verlässliche Systeme und geeignete technisch-organisatorische Maßnahmen einsetzen (Kap. 11.2). Daten, die sie rechtmäßig erhalten haben, dürfen sie für Werbezwecke nicht zeitlich unbegrenzt einsetzen. Auch Werbedaten haben ein Mindesthaltbarkeitsdatum (Kap. 11.3).

11.1
Werbeaktion mit Daten aus Corona-Tests

Ein Unternehmen, das während der Corona-Pandemie bundesweit Testcenter betrieben hatte, hat die Daten von Besuchern nach Ende der Pandemie dazu genutzt, um Werbung für eigene Dienste und Produkte zu machen, die in keinem Zusammenhang mit Corona-Tests standen. In dem aufgrund mehrerer Beschwerden geführten Verwaltungsverfahren war zu klären, ob die Verarbeitung von personenbezogenen Daten von ehemaligen Corona-Testcenterbesuchern zu Werbezwecken auf Grundlage eines berechtigten Interesses und ohne explizite Einwilligung zulässig war.

Eine umfangreiche Werbeaktion

Mich erreichten mehrere, voneinander unabhängige Beschwerden von Personen, die unerwünschte E-Mail-Werbung von einem Unternehmen erhielten, das während der Pandemie Corona-Testcenter betrieben hatte, die die betroffenen Personen besucht hatten. Zu keinem Zeitpunkt, weder bei der Onlinebuchung eines Termins zur Durchführung eines Corona-Tests noch vor Ort bei der faktischen Durchführung des Tests, hatten sie eine Einwilligung in die Verarbeitung ihrer personenbezogenen Daten zu werblichen Zwecken erteilt. Darüber hinaus wurden die Testcenterbesucher bei der Erhebung ihrer Daten auch nicht über die beabsichtigte spätere werbliche Verwendung ihrer personenbezogenen Daten durch das Unternehmen informiert.

Aufgrund der unerwarteten werblichen Verarbeitung ihrer Daten stellten einige betroffene Personen ein Auskunftsersuchen gemäß Art. 15 DS-GVO. Im Zuge der Auskunftserteilung erklärte das verantwortliche Unternehmen, die Verarbeitung basiere auf einem überwiegenden berechtigten Interesse

nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO in Verbindung mit § 7 Abs. 3 UWG. Dort ist die sogenannte Bestandskundenausnahme geregelt, die vorsieht, dass Unternehmen per Mail im Rahmen von bereits bestehenden Kundenverhältnissen in gewissem Umfang für eigene, ähnliche Produkte werben dürfen, auch wenn ihre Kunden keine ausdrückliche Werbeeinwilligung erteilt haben.

Bei der Aufklärung des Sachverhalts wurde festgestellt, dass die betreffende Werbekampagne den Versand von über 1.300.000 werblichen E-Mails an ehemalige Besucher von Corona-Testzentren umfasste, die in mehreren Tranchen verschickt wurden.

Notwendigkeit einer datenschutzrechtlichen Erlaubnis

Zur Beschränkung der E-Mail-Flut und zum Schutz des Persönlichkeitsrechts des Empfängers sind der Kontaktaufnahme mittels Werbe-E-Mails durch den Gesetzgeber enge Grenzen gesetzt. Datenschutzrechtlich bedeutet dies zunächst, dass eine Rechtsgrundlage dem Versender die Verarbeitung der personenbezogenen Daten erlauben muss. Der Versand von Werbe-E-Mails ist unter datenschutzrechtlichen Aspekten grundsätzlich 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. Eine solche Einwilligung der betroffenen Personen konnte der Verantwortliche jedoch nicht nachweisen.

Überwiegende berechtigte Interessen?

Daneben kann die Datenverarbeitung zu Werbezwecken auch auf die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO gestützt werden. Dabei gilt allerdings, dass die Interessen der betroffenen Personen immer dann diejenigen des Verantwortlichen überwiegen, wenn dessen Handeln nicht im Einklang mit der Rechtsordnung steht (vorliegend insb. mit dem Wettbewerbsrecht). Die wesentliche wettbewerbsrechtliche Regelung zur Zulässigkeit von E-Mail-Werbung findet sich in § 7 Abs. 2 Nr. 2 UWG. Danach ist E-Mail-Werbung ohne vorherige ausdrückliche Einwilligung grundsätzlich als unzumutbare Belästigung unzulässig.

Abweichend von 7 Abs. 2 Nr. 2 UWG ist keine unzumutbare Belästigung bei einer Werbung unter Verwendung elektronischer Post bei Bestandskunden anzunehmen, wenn die in § 7 Abs. 3 Nr. 1 – 4 UWG aufgeführten Voraussetzungen kumulativ erfüllt sind. Danach ist Werbung per elektronischer Post zulässig, wenn:

§ 7 Abs. 3 Nr. 1 – 4 UWG

1. *ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat,*
2. *der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet,*
3. *der Kunde der Verwendung nicht widersprochen hat und*
4. *der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.*

Im vorliegenden Fall fehlte es allerdings an der zweiten und an der letztgenannten Voraussetzung.

In Bezug auf die fragliche Werbekampagne konnte keine Ähnlichkeit von Waren und Dienstleistungen im Sinne von § 7 Abs. 3 Nr. 2 UWG festgestellt werden. Die Kampagne stellte den Empfängern die gesamte vom Unternehmen angebotene Produktpalette an Tests auf verschiedene Krankheiten vor und bewarb diese mit einem allgemeinen Gutscheincode.

Die Ähnlichkeit der beworbenen Waren und Dienstleistungen muss sich jedoch auf die bereits vom Kunden gekauften Produkte beziehen und denselben typischen Verwendungszweck oder Bedarf abdecken (s. OLG Jena, Urteil vom 21. April 2010 – Az. 2 U 88/10; LG Frankfurt am Main, Urteil vom 22. März 2018 – m Az. 2-03 O 372/17). Da die Werbe-E-Mail nicht ausschließlich auf einen spezifischen Produkttyp abzielte, wie beispielsweise Corona-Tests im Kontext der Pandemie, sondern ebenfalls das breite Angebot an Testkits für Geschlechtskrankheiten und allgemeine Gesundheitsauswertungen umfasste, war die Voraussetzung einer Ähnlichkeit nicht erfüllt. Dies bedeutet, dass es sich hierbei weder um einen identischen typischen Verwendungszweck noch um den gleichen Bedarf des Kunden handelte.

Das Gesetz schreibt vor, dass Kunden bei der Erhebung ihrer Adresse und bei jeder späteren Verwendung unmissverständlich darauf hingewiesen werden müssen, dass sie der Nutzung ihrer Daten jederzeit widersprechen können. Der Verantwortliche hatte bei seiner Interessenabwägung zur Direktwerbung auch diesen entscheidenden Aspekt nicht berücksichtigt. Insbesondere fehlte es an dem Hinweis auf das Widerspruchsrecht, der klar und deutlich zum Zeitpunkt der Erhebung der personenbezogenen Daten erfolgen muss. Der Datenschutzhinweis des Verantwortlichen enthielt zwar einen abstrakten Verweis auf ein Widerspruchsrecht. Dieser Hinweis war jedoch ohne eine konkrete Information über die beabsichtigte werbliche Verwendung der Daten weder transparent noch bestimmt genug. Er war zudem im Fließtext einer umfangreichen Datenschutzerklärung versteckt, eingebettet zwischen

vielen anderen Informationen. Eine derartige Vorgehensweise genügt nicht den Anforderungen an die erforderliche Transparenz (s. z. B. LG Paderborn, Urteil vom 12. März 2024 – m Az. 2 O 325/23).

Angesichts dieser Defizite habe ich den Verantwortlichen darauf hingewiesen, dass auch bei der Durchführung von Covid-Schnelltests zur Pandemiebekämpfung und bei der Speicherung der dazu erhobenen Daten die datenschutzrechtlichen Grundsätze, insbesondere der Grundsatz der Zweckbindung, zu beachten sind. Die Erhebung der personenbezogenen Daten der betroffenen Personen erfolgte ausschließlich zum Zweck der Testdurchführung, der Ergebnismitteilung sowie zu Abrechnungs- und Nachweiszwecken. Die anschließende Verarbeitung dieser Daten zu Werbezwecken ist mit dem ursprünglichen Erhebungszweck nicht vereinbar, für die Betroffenen nicht vorhersehbar und damit unzulässig.

Anordnung und Sanktion

Auf Grund der fehlenden Einsicht des Verantwortlichen untersagte ich dem Unternehmen, die im Rahmen der Nutzung von Corona-Testcentern erhobenen personenbezogenen Daten von getesteten Personen, insbesondere deren E-Mail-Adressen, zur werblichen Kommunikation per E-Mail zu nutzen, soweit keine Einwilligungen vorliegen.

Nach Abschluss des Verwaltungsverfahrens wurde ein Geldbußenverfahren eingeleitet, um die begangenen Verstöße zu sanktionieren.

11.2
Systemfehler führt zur Missachtung tausender Werbewidersprüche

Technische Fehler entbinden werbende Unternehmen nicht von der Pflicht, Werbewidersprüche zu beachten. Sie tragen die Verantwortung für ihre technischen Systeme.

Durch eine Beschwerde erfuhr ich, dass ein global tätiges Reiseunternehmen den vor Jahren eingelegten und bis dato umfassend berücksichtigten Werbewiderspruch eines Betroffenen plötzlich nicht mehr beachtete. Dessen Daten wurden stattdessen erneut zu werblichen Zwecken verarbeitet, um Briefwerbung zu versenden.

Nach Art. 21 Abs. 2 DS-GVO hat die betroffene Person das Recht, jederzeit ohne Angabe von Gründen Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke von Direktwerbung einzulegen. Sobald ein solcher Werbewiderspruch eingeht, ist der Verantwortliche verpflichtet, die Daten der betroffenen Person nicht mehr für diese Zwecke

zu verarbeiten. Um dies sicherzustellen, muss der Verantwortliche sowohl technische als auch organisatorische Maßnahmen ergreifen.

Im Rahmen des aufgrund der Beschwerde angestrengten Verwaltungsverfahrens stellte sich heraus, dass der Verantwortliche seine internen Prozesse neu gestaltet hatte, um die Effizienz der Kundensysteme zu steigern. Diese Prozessänderungen führten bei ihrer Implementierung jedoch zu einem technischen Fehler, durch den im Kundensystem ein zweiter Datensatz angelegt wurde.

Aufgrund eines Systemfehlers wurden ordnungsgemäß hinterlegte und berücksichtigte Werbewidersprüche allerdings nicht in den neuen Datensatz mit übernommen. Infolgedessen kam es trotz des ursprünglich bereits hinterlegten und auch beachteten Werbewiderspruchs zu einer erneuten Verarbeitung von personenbezogenen Daten zu werblichen Zwecken.

Die Analyse des Sachverhalts legte die Vermutung nahe, dass der Umfang des technischen Fehlers über den Einzelfall hinausgehen und potenziell auch weitere Personen betreffen könnte. Tatsächlich stellte sich heraus, dass auch für weitere Kunden ein fehlerhafter zweiter Datensatz erstellt worden war. Insgesamt waren knapp über 5.000 Kunden des Unternehmens in der Europäischen Union sowie in Liechtenstein, der Schweiz und Norwegen von diesem technischen Fehler betroffen – mit der Folge, dass sie alle Briefwerbung des Unternehmens erhielten, obwohl sie der Verarbeitung ihrer Daten zu werblichen Zwecken bereits ausdrücklich widersprochen hatten.

Der all diesen Fällen zugrundeliegende Fehler konnte im Rahmen des von mir geführten Verfahrens aufgedeckt werden und wurde vom Unternehmen umgehend behoben.

Auf Grund der festgestellten Datenschutzverstöße in mehreren Tausend Fällen wurde ein Geldbußenverfahren eingeleitet.

11.3
Auch Werbedaten haben ein Mindesthaltbarkeitsdatum

Eine Kundin, die vor mehreren Jahren zum ersten und gleichzeitig letzten Mal bei einem Versandhändler etwas bestellt hatte, erhielt plötzlich Werbung des Unternehmens und beschwerte sich daher über die werbliche Verarbeitung ihrer Kundendaten. Im Fokus des Falls stand die Frage, unter welchen rechtlichen Rahmenbedingungen und vor allem wie lange die Daten ehemaliger Kunden für Marketingmaßnahmen genutzt werden dürfen.

Während die Regeln für E-Mail-Marketing strikt sind und in der Regel eine vorherige Einwilligung der Empfänger verlangen, gelten für die persönlich

adressierte Postwerbung andere datenschutzrechtliche Maßstäbe. Die DS-GVO und das UWG bilden den rechtlichen Rahmen für den Versand von Postwerbung. Grundlage für die Beurteilung der Zulässigkeit einer Verarbeitung personenbezogener Daten für Zwecke der Direktwerbung ist in der DS-GVO, abgesehen von einer Einwilligung der betroffenen Person, eine Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO. Danach muss die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich sein und die Interessen der betroffenen Person dürfen nicht überwiegen. Dass bei Direktwerbung Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO grundsätzlich als Rechtsgrundlage in Frage kommt, ist dem ErwG 47 DS-GVO zu entnehmen, der u. a. ausführt: „Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden."

In der Orientierungshilfe der Datenschutzkonferenz zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der DS-GVO aus dem Jahr 2022 wird festgestellt, dass für zulässigerweise beim Betroffenen erhobene Kontaktdaten das geltende Recht keine explizite und abstrakte Befristung einer werblichen Nutzung nach dem letzten aktiven Geschäfts- oder Direktwerbekontakt vorsieht. Vielmehr bedarf es einer Betrachtung und Beurteilung des jeweiligen Einzelfalls um festzustellen, wie lange eine werbliche Nutzung von personenbezogenen Daten jeweils zulässig ist. Bei der Beurteilung, ab wann nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO überwiegende schutzwürdige Interessen der betroffenen Person einer länger währenden werblichen Nutzung entgegenstehen, sollten einerseits der Zeitablauf seit dem letzten aktiven Kontakt, andererseits die Art des Grundgeschäfts berücksichtigt werden.

Eine Kundin erhielt postalische Werbung von einem Versandhändler, obwohl ihr erster und einziger Einkauf bei dem Unternehmen bereits neun Jahre zurücklag. Im Rahmen des Beschwerdeverfahrens stellte sich heraus, dass der Verantwortliche die personenbezogenen Daten seiner Kundinnen und Kunden zunächst sowohl auf elektronischem als auch auf postalischem Wege in zulässiger Weise zu werblichen Zwecken verarbeitet.

Bei Kunden, die über einen längeren Zeitraum nicht mehr bei ihm bestellten, wurde die werbliche Ansprache nach einer gewissen Zeit auf den postalischen Weg beschränkt und in der Häufigkeit konsequent reduziert. Ein entscheidender Aspekt bei der vom Verantwortlichen getroffenen Abwägungsentscheidung hinsichtlich der Dauer von Werbesendungen war die hohe Qualität und Langlebigkeit der von ihm angebotenen Artikel. Nach seinen Erfahrungen würde dadurch eine Ersatzbeschaffung für die Kunden erst nach mehreren Jahren wieder erforderlich, so dass die Zusendung von Werbung auch nach

einem längeren Zeitraum noch oder gerade wirtschaftlich vorteilhaft für sein Unternehmen sei. Ein solches Argument kann im Rahmen der getroffenen Abwägung tatsächlich eine berechtigte Rolle spielen.

In diesem Fall kam jedoch hinzu, dass die Verarbeitung der personenbezogenen Daten zu werblichen Zwecken und damit der Versand von Werbematerial über einen Zeitraum von drei Jahren vollständig ausgesetzt und dann im neunten Jahr nach dem ursprünglichen Kauf wieder aufgenommen worden war. Dies erzeugte bei der betroffenen Kundin den Eindruck, dass ihre Daten vom Unternehmen nicht mehr genutzt oder möglicherweise sogar schon gelöscht worden seien, und verstärkte die Überraschung, als sie schließlich doch erneut Werbung erhielt.

Obwohl das Unternehmen auch nach neun Jahren weiterhin ein berechtigtes Interesse an Direktwerbung annahm, hält diese Einschätzung einer datenschutzrechtlichen Prüfung nicht stand. Insbesondere aufgrund der langjährigen Inaktivität der werblichen Datenverarbeitung ist deren Wiederaufnahme und weitere Speicherung und Verarbeitung der Daten der Kunden nach einem derart langen Zeitraum nicht vertretbar. Ein Betroffener, der nur einmalig Kunde war, muss vernünftigerweise nicht damit rechnen, dass seine Daten für diesen Zweck so lange gespeichert und wiederverwendet werden.

Die unternehmensinternen Richtlinien für werbliche Kontaktaufnahmen und zeitliche Begrenzungen bei der Speicherung und Verarbeitung von personenbezogenen Daten wurden letztlich durch das Unternehmen, das mit meiner Behörde insofern gut kooperierte, präzisiert und neu festgelegt.

12. Videoüberwachung

Zur Frage, welche private Videoüberwachung datenschutzrechtlich zulässig ist, besteht noch immer eine hohe Rechtsunsicherheit. Um für hessische Vereine in dieser Frage Rechtssicherheit zu bieten, habe ich Handlungsempfehlungen für die datenschutzkonforme Videoüberwachung in Vereinen erarbeitet (Kap. 12.1). Kommunen zeigen zunehmend Interesse, Videoüberwachung zur Verhinderung illegaler Müllablagerungen einzusetzen. Aus diesem Grund war zu klären, unter welchen Voraussetzungen dieses Mittel gegen dieses Übel eingesetzt werden darf (Kap. 12.2).

12.1 Datenschutzkonforme Videoüberwachung in hessischen Vereinen

Die neue Handlungsempfehlung bietet Vereinen eine kompakte, praxisnahe Orientierung zum sensiblen Thema Videoüberwachung. Er zeigt klar auf, wann Kameras zulässig sind und wann nicht und gibt wertvolle Hinweise zur rechtssicheren Umsetzung.

Grundsätzlich darf niemand ohne Anlass oder Zustimmung mit Kameras beobachtet werden. Die DS-GVO erlaubt Videoüberwachung nur dann, wenn ein berechtigtes Interesse vorliegt (Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO) und keine milderen Alternativen existieren. Vor jeder Installation müssen daher Zweck, Erforderlichkeit und Verhältnismäßigkeit sorgfältig geprüft und dokumentiert werden.

Besonders wichtig ist der Schutz von Kindern und Jugendlichen, die in Vereinen häufig aktiv sind. Auch kleine Vereine ohne formelle Datenschutzbeauftragte müssen die datenschutzrechtlichen Vorgaben erfüllen und sollten eine verantwortliche Person für Datenschutzfragen benennen.

Über die Einführung einer Videoüberwachung entscheidet in der Regel der Vorstand. Bei weitreichenden Maßnahmen, die Mitglieder regelmäßig betreffen, sollte die Mitgliederversammlung einbezogen werden. Offenheit schafft Vertrauen – Transparenz ist der beste Datenschutz.

Betroffene müssen durch Hinweisschilder und Informationen nach Art. 13 DS-GVO über die Überwachung, den Zweck und die Speicherfristen informiert werden. Ich stelle hierfür kostenlose Mustervorlagen zur Verfügung (https://datenschutz.hessen.de/datenschutz/videoueberwachung/videoueberwachung-durch-nicht-oeffentliche-stellen).

Zugriff auf gespeicherte Aufnahmen dürfen nur befugte Personen haben, idealerweise nach dem Vier-Augen-Prinzip. Die Daten müssen verschlüsselt

und nach spätestens 48 bis 72 Stunden gelöscht werden, sofern kein sicherheitsrelevanter Vorfall vorliegt. Eine dauerhafte oder heimliche Überwachung ist unzulässig.

Im Vereinsheim kann eine Kamera ausnahmsweise – außerhalb von Trainingszeiten – sinnvoll sein, etwa zum Schutz vor Einbruch oder Vandalismus. Bereiche wie Aufenthaltsräume, Umkleiden oder Toiletten bleiben jedoch tabu.

Eine Überwachung von Trainingsflächen oder Sporthallen ist in der Regel nicht erlaubt, da sie tief in die Privatsphäre eingreift. Auch in Schützen- oder Reitvereinen dürfen nur sicherheitsrelevante Bereiche überwacht werden – niemals der laufende Vereinsbetrieb.

Fazit: Datenschutz schafft Vertrauen

Videoüberwachung kann ein wirksames Mittel zur Sicherheit sein, aber nur wenn sie verantwortungsvoll, transparent und verhältnismäßig eingesetzt wird. Meine neue Handlungsempfehlung hilft Vereinen, rechtliche Risiken zu vermeiden, Mitglieder zu schützen und Datenschutz verständlich umzusetzen. Er liefert klare Prüfschritte und praktische Beispiele – ein sehr gutes Hilfsmittel für Vorstände, Datenschutzverantwortliche und Vereinsmitglieder.

Der vollständige Ratgeber steht kostenfrei auf meiner Webseite unter www.datenschutz.hessen.de zum Download bereit. Es wird Vereinen empfohlen, diesen im Sinne der Vereinsmitglieder und der Privatsphäre aller Beteiligten zu nutzen.

12.2
Videoüberwachung zur Verhinderung illegaler Müllablagerungen

Videoüberwachung wird von Kommunen zumeist als Mittel zur Verfolgung vielfältiger Zwecke gesehen – oft für gute Zwecke wie etwa die Verhinderung illegaler Müllablagerungen. Videoüberwachung greift jedoch in die Grundrechte betroffener Personen ein. Im Rahmen von Beratungen, Beschwerden und Hinweisen widme ich mich den Bedingungen für die Zulässigkeit von Videoüberwachungen.

Videoüberwachung als Hilfsmittel gegen illegale Müllablagerungen

Illegale Müllablagerungen müssen verhindert und saubere Gemeinflächen erhalten werden. Um dieses Ziel zu erreichen, wollen viele Kommunen eine Videoüberwachung öffentlicher Räume einführen. Dabei ist zu berücksichtigen, dass dies in die Rechte betroffener Personen eingreift.

Im Rahmen vermehrter Beratungsanfragen durch Kommunen habe ich mich diesem Spannungsfeld gestellt und datenschutzkonforme Bedingungen evaluiert. Neben dem Schutz der gemeinsamen Räume müssen bei der Erarbeitung eines Konzepts zur Videoüberwachung auch die betroffenen Menschen in diesen bedacht werden. Im Regelfall handelt es sich damit um eine Einzelfallbetrachtung, bei der einzelne Aspekte übertragbar sind.

Von den Kommunen, die mich um eine Beratung und rechtliche Einschätzung ersucht haben, wurden jeweils unterschiedliche Örtlichkeiten innerhalb der gemeindlichen Flächen benannt, an denen sich sogenannte Hot-Spots von Müllanhäufungen regelmäßig bilden. Das Anfrageaufkommen ist in diesem Berichtsjahr, nach kontinuierlichen Anstiegen bereits in den Vorjahren, nochmals massiv gewachsen. So wurde in diesem Jahr von unterschiedlichen Kommunen in Hessen unter anderem für die Möglichkeit einer kommunalen Videoüberwachung von Parkplätzen, Sportparks, von Glas-, Altkleider- und anderen Containern und öffentlichen Parks eine Beratung durch mich angefragt. Darüber hinaus spielten aber auch sogenannte Open Libraries, also jederzeit zugängliche kommunale Bibliotheken, in der Beratung zur Videoüberwachung in diesem Kontext eine Rolle, weil hier u. a. unliebsame Hinterlassenschaften (neben Befürchtungen von Vandalismus oder Diebstahl) befürchtet wurden.

Auch wenn in der medialen Berichterstattung eine angebliche Datenschutzkonformität behauptet und in der zu Wort kommenden Bevölkerung ein breites Verständnis für die Videoüberwachung zwecks Verhinderung illegaler Müllablagerungen suggeriert wurde, bedarf es für die Verarbeitung personenbezogener Daten einer Rechtsgrundlage und die Maßnahme muss sich als verhältnismäßig erweisen.

In allen Fällen muss die Videoüberwachung erforderlich sein. Um dies feststellen zu können, bedarf es präziser Angaben. Es ist nicht ausreichend, unbestimmte Begriffe wie „viel“ oder „hoch“ oder „intensiv“ zu nennen, vielmehr ist regelmäßig eine recht genaue und nachvollziehbare Bezifferung und Dokumentation von Nöten, um eine möglichst passgenaue Einschätzung zur Datenschutzkonformität des Vorhabens zu ermöglichen. Auch die Einstufung z. B. einer „erheblichen“ Belastung kann erst nach dem Tatsachenvortrag erfolgen und kann diesen nicht ersetzen.

Rechtsgrundlage für Videoüberwachungen durch Kommunen

Einschlägige gesetzliche Grundlagen für die Videoüberwachung im öffentlichen Bereich kann Art. 6 Abs. 1 UAbs. 1 Buchst. e DS-GVO i. V. m. § 4 HDSIG sein.

§ 4 HDSIG

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

1. zur Aufgabenerfüllung öffentlicher Stellen,

2. zur Wahrnehmung des Hausrechts

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

(2) Der Umstand der Beobachtung sowie der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) Die Speicherung oder Verwendung von nach Abs. 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten und nicht geringfügigen Ordnungswidrigkeiten erforderlich ist.

(4) Die Daten sind zu löschen, sobald sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder wenn schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Die Räume, um die es meist geht, sind nach ihrer Widmung dafür bestimmt, von einem unbestimmten Personenkreis genutzt zu werden, und sind damit öffentlich zugängliche Räume im Sinne der Vorschrift. Weiterhin ist sowohl die Abfallentsorgung wie auch die Bereitstellung sozialer und kultureller Räume eine im öffentlichen Interesse liegende Aufgabe, so dass es im Rahmen der Erforderlichkeit und der Abwägung schutzwürdiger Interessen der Betroffenen zu den folgenden Abwägungen kommt.

Notwendige Abwägungen

Eine Videoüberwachung öffentlicher Räume ist zunächst regelmäßig kritisch zu betrachten, da sie einen ungerechtfertigten Eingriff in das Recht auf informationelle Selbstbestimmung darstellen kann, sofern sie nicht über die genannte Rechtsgrundlage rechtmäßig ist.

Die in den Beratungsanfragen genannten Bereiche werden nahezu ausnahmslos von vielen unbeteiligten Personen besucht, die sich an diesen öffentlichen Orten ordnungsgemäß und anstandslos verhalten. Da diese

die jeweiligen Orte ganz überwiegend dem jeweiligen Zweck entsprechend berechtigt nutzen, handelt es sich bei der Videoüberwachung von öffentlichen Bereichen meist um verdachtslose Eingriffe mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Die Maßnahme weist grundsätzlich eine hohe Eingriffsintensität auf (s. BVerfG, Beschluss vom 23. Februar 2007 – 1 BvR 2368/06, Rn. 51). Eine Videoüberwachung des öffentlichen Raumes ist damit ein intensiver Eingriff in das allgemeine Persönlichkeitsrecht des Menschen, der den überwachten öffentlichen Raum betritt. Da lediglich von einer kleinen Minderheit der erfassten Personen Verstöße gegen rechtliche Vorgaben zu erwarten wären, würde möglicherweise der überwiegende Anteil der Personen ohne Anlass miterfasst werden (vgl. BVerfG, Beschluss vom 23. Februar 2007 – 1 BvR 2368/06, Rn. 52).

Es ist daher abzuwägen, ob die schutzwürdigen Interessen der Betroffenen, selbst wenn die Videoüberwachung zum Erreichen des verfolgten Zwecks grundsätzlich geeignet erscheint, überwiegen. Dabei ist insbesondere zu bedenken, ob die Videoüberwachung die Müllablagerungen tatsächlich verhindern würde. Es ist darauf hinzuweisen, dass es diesbezüglich nicht immer so erfolgversprechend ist, wie von der Berichterstattung suggeriert wird. Häufig führt die Videoüberwachung lediglich zu einer Verdrängung des bekämpften Geschehens und bewirkt weder den gewünschten Abschreckungseffekt noch eine geeignete Beweissicherung.

Auch kann die Videoüberwachung die Zweckbestimmung eines öffentlichen Raumes vollständig konterkarieren und muss deswegen als Mittel gegen illegale Müllablagerungen ausscheiden. Dies kann etwa bei einem öffentlichen Park der Fall sein, der dem dauerhaften Aufenthalt im Rahmen der Freizeitgestaltung gewidmet ist.

Grundsätzlich sollte eine Videoüberwachung immer das letzte Mittel sein, das zum Einsatz kommt. Ist die konkrete Einsatzform zwar grundsätzlich geeignet, den Zweck der Überwachung zu erreichen, kann es dennoch an der Erforderlichkeit fehlen, wenn mildere, aber gleich wirksame Mittel vorhanden sind. Als mildere Mittel sind z. B. Umzäunung, Beleuchtung, Bestreifung, Entsorgungshilfe, Überprüfung von Entsorgungskonzepten (z. B. Müllkapazitäten für die Anzahl der Bewohner in Mehrfamilienhäusern), Vor-Ort-Kontrollen und Öffentlichkeitskampagnen zu nennen.

Es dürfen zugunsten der Videoüberwachung gesundheitliche Gefährdungen, Auswirkungen auf die Umwelt und unhygienische Zustände gewichtet werden. Hierbei kommt es aber insbesondere darauf an, dass geeignete Maßnahmen spezifisch gegen die Gefährdung ergriffen werden. Das heißt,

in einem solchen Fall müsste auch detailliert dargelegt werden, um welche gesundheitsgefährdenden Aspekte es sich ausgehend von den illegalen Müllablagerungen handelt und welche Ausmaße diese angenommen haben. Darüber hinaus müsste nach einem geeigneten Zeitraum evaluiert werden, ob die Videoüberwachung zur Verringerung der gesundheitlichen Gefährdungen, die von den Müllablagerungen tatsächlich ausgehen, beigetragen hat.

In meinen Beratungen ergeht häufig der Hinweis an die potenziell Verantwortlichen einer Videoüberwachung, zweckentsprechende Überlegungen anzustellen, wie ein datenschutzkonformer Betrieb aussehen könnte. Hierzu sind zum einen die Zeiten einzugrenzen, in denen es zu Müllablagerungen kommt (z. B. während der Abend- und Nachtzeiten), es ist ein geeignetes Löschkonzept zu entwickeln (keine längere Speicherdauer als 72 Stunden), zudem hat die Videoüberwachung stets offen zu erfolgen (eine entsprechende Hinweisbeschilderung wäre somit notwendig), die Aufnahmen sollten verpixelt erfolgen (nur anlassbezogen wird die Verpixelung aufgehoben) und der Aufnahmebereich muss ausgewählt und eingegrenzt werden (z. B. Aussparung von Spielplätzen und öffentlichen Toiletten).

In der Regel muss damit ein Konzept erarbeitet werden, das technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten der Bürger enthält sowie darstellt, dass sämtliche milderen Mittel bereits ausgeschöpft wurden. Zur Akzeptanz und Vorhersehbarkeit der geplanten Videoüberwachung ist anzuraten, ein solches Konzept dann auch den Bürgerinnen und Bürgern zugänglich zu machen.

Da als weitere Rechtsgrundlage eine Anpassung der kommunalen Gefahrenabwehrverordnung in Erwägung gezogen wurde, ist zudem darauf hinzuweisen, dass eine solche immer an den insoweit vorrangigen Regelungen der DS-GVO und dem HDSIG zu messen ist. Es können in einer kommunalen Gefahrenabwehrverordnung keine weiterreichenden Regelungen getroffen werden, als die einschlägigen europarechtlichen und landesrechtlichen Vorschriften es zulassen. Daher kann auch eine kommunale Gefahrenabwehrverordnung keine über sie hinausgehende tragfähige Rechtsgrundlage darstellen.

Da die Kommunen den datenschutzkonformen Betrieb ihrer geplanten Videoüberwachung als Verantwortliche im Sinn von Art. 4 Nr. 7 DS-GVO selbst gestalten und verantworten, sieht weder die DS-GVO noch das HDSIG ein Genehmigungsverfahren durch die Aufsichtsbehörden vor.

Daher existieren auch keine spezifischen Listen mit Auflagen. Vielmehr hat die Kommune einzelfallbezogene geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten zu ergreifen, wobei die bisherigen Ausführungen zur Orientierung dienen können.

Zusammenfassung

Im Rahmen des Beratungsjahres 2025 kann ich festhalten, dass die Möglichkeit der datenschutzkonformen Ausgestaltung der Videoüberwachung im Kontext illegaler Müllablagerungen einzig im Rahmen eines öffentlichen Parks nicht gesehen werden konnte, da der dauerhafte Aufenthalt im Rahmen der Freizeitgestaltung im Fokus der öffentlichen Widmung eine Videoüberwachung ausschließt.

Zusammenfassend ist festzuhalten, dass die datenschutzrechtlichen Anforderungen der Videoüberwachung öffentlicher Räume sich gezielt daran orientieren sollten,

– den erfassten Raum anhand einer klaren Zweckbenennung zur Vermeidung illegaler Müllablagerungen abzugrenzen,
– die Datenerhebung auf das notwendige Minimum zu begrenzen,
– geeignete technisch-organisatorische Schutzmaßnahmen zu ergreifen und
– die Überwachung transparent für die betroffenen Personen mit Augenmaß zu gestalten,

um öffentliche Räume weiterhin weitestgehend frei von der Ausübung von Überwachungsdruck zu halten.

13. Wirtschaft

Im Bereich der Wirtschaft sind die Beschwerden, Hinweise und Beratungen ebenfalls überdurchschnittlich gestiegen. Dies erforderte vermehrte Aufsichtsverfahren und führte auch zu mehr Sanktionen gegen Unternehmen. Die hier für den Bericht ausgewählten Fälle betrafen die Schwierigkeiten, berechtigte Auskunftsersuchen gegen einen Verantwortlichen in einem anderen EU-Mitgliedstaat durchzusetzen (Kap. 13.2). Noch schwieriger wird eine Löschung von Daten bei einem deutschen Inkassounternehmen, das eine umstrittene Forderung eines Unternehmens in einem Drittland vollstrecken will (Kap. 13.3). Wer Waren auf Fake-Seiten im Internet bestellt, muss damit rechnen, keine Betroffenenrechte geltend machen zu können (Kap. 13.6). Auch eine Auskunft über die eigenen Daten zu erlangen, erweist sich als voraussetzungsvoll, wenn sie an einen Stellvertreter gesendet werden soll (Kap. 13.5). Verstöße gegen die DS-GVO mussten festgestellt und behoben werden – bei einem Kreditinstitut, das zu viele Daten an das Jobcenter geliefert hat (Kap. 13.4), bei einem Online-Bestelldienst, der die Bestelldaten unzureichend sicherte (Kap. 13.7) und bei einem Copy-Shop, der unzulässig kopierte Dokumente gespeichert hatte (Kap. 13.8).

13.1
Die Wirkung von Verhaltensregeln

Verhaltensregeln sind wichtige, in der DS-GVO vorgesehene Instrumente zur Reduzierung von Bürokratie (s. Kap. 1.3). Sie ermöglichen, die abstrakten und allgemeinen Vorgaben der DS-GVO an die spezifischen technischen, wirtschaftlichen und rechtlichen Bedingungen einer Branche anzupassen. Dieses nützliche Instrument ist aber sehr voraussetzungsvoll und der Aufwand wird nur übernommen, wenn Verhaltensregeln auch gewisse Rechtswirkungen haben.

Verhaltensregeln der deutschen Wirtschaftsauskunfteien

Durch Bescheid vom 24. Mai 2024 habe ich neue „Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien“ genehmigt (s. hierzu 53. Tätigkeitsbericht, Kap. 1.6, S. 14 ff.). Solche Verhaltensregeln sieht die DS-GVO in Art. 40 und 41 vor, damit Verbände oder andere Vereinigungen die abstrakten Anforderungen der Verordnung bereichsspezifisch präzisieren und konkretisieren und dadurch für mehr Rechtssicherheit sorgen können (s. Kap. 1.3).

Wirtschaftsauskunfteien sind private gewerbliche Unternehmen, die Informationen über die Identität, die wirtschaftliche Betätigung, die Kreditwürdigkeit,

die Zahlungswillig- und -fähigkeit von Unternehmen und Privatpersonen erheben. Diese Informationen werden gespeichert und an Dritte übermittelt, wenn die Wirtschaftsauskunftei und die Dritten ein berechtigtes Interesse am Erhalt einer solchen Information haben. Die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch eine Wirtschaftsauskunftei beruht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO und § 31 BDSG.

Neben der Verarbeitung von Identifikationsdaten (z. B. Name, Vorname, Adresse, Geburtsdatum und frühere Anschriften), Negativdaten zum Zahlungsverhalten und Daten zu offenen Forderungen darf die Wirtschaftsauskunftei darüber hinaus personenbezogene Daten zu ausgeglichenen Forderungen speichern. In den aktuellen Verhaltensregeln unter Punkt IV., Nr. 1, Buchst. b wurde dafür die folgende Regelung getroffen:

> *„Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien Punkt IV, Nr. 1, Buchst. b*
>
> *b) Ausgeglichene Forderungen*
>
> *Personenbezogene Daten über ausgeglichene Forderungen werden grundsätzlich für drei Jahre gespeichert. Die Speicherung endet abweichend davon bereits nach 18 Monaten, wenn der*
>
> *(1) Auskunftei bis zu diesem Zeitpunkt keine weiteren Negativdaten gemeldet worden sind,*
>
> *(2) keine Informationen aus dem Schuldnerverzeichnis oder aus Insolvenzbekanntmachungen vorliegen und*
>
> *(3) der Ausgleich der Forderung innerhalb von 100 Tagen nach Einmeldung erfolgte.“*

Das OLG Köln verurteilte am 10. April 2025 eine in Hessen ansässige Wirtschaftsauskunftei, trotz dieser in den Verhaltensregeln verankerten Regelung zur Zahlung eines Schadensersatzes nach Art. 82 Abs. 1 DS-GVO, da sie ein Negativmerkmal nach dem Nachweis des vollständigen Begleichens der Forderung nicht umgehend (vor Ablauf der in den Verhaltensregeln benannten Speicherfristen) gelöscht hat (OLG Köln, Az. 15 U 249/24). Sie habe damit gegen die gebotene Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO verstoßen. In der Urteilsbegründung ging das OLG Köln auf die Verhaltensregeln der Wirtschaftsauskunfteien nur wie folgt ein: Dass nach diesen Verhaltensregeln *„personenbezogene Daten über ausgeglichene Forderungen für bestimmte Zeiträume gespeichert werden dürfen,*

ist unerheblich. Denn Verhaltensregeln im Sinne des Art. 40 DS-GVO, die zu einer anderen Beurteilung führen würden als derjenigen, die sich nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO ergibt, können bei der Abwägung nach dieser Bestimmung nicht berücksichtigt werden" (OLG Köln, Az. 15 U 249/24, Rn. 33).

Nur einen Tag später entschied das OLG München mit Endurteil vom 11. April 2025 (Az. 14 U 3590/24e) konträr zur Entscheidung des OLG Köln. Es führte aus, dass die Verhaltensregeln weiterhin zu beachten seien und Informationen zu Zahlungsstörungen grundsätzlich durch Wirtschaftsauskunfteien bis zu 36 Monate gespeichert werden dürften. Dabei erläuterte es zu den Verhaltensregeln wie folgt: *„Diese Verhaltensregeln binden den Senat nicht. Bedenkt man aber, dass die Verhaltensregeln durch den hessischen Datenschutzbeauftragten (im Folgenden: HBDI) genehmigt wurden, dass der Neufassung der Verhaltensregeln eine Beanstandung seitens des HBDI vorausging und dass der Genehmigung wiederum eine Anhörung interessierter Kreise und eine Abstimmung mit weiteren Datenschutzbeauftragten vorausging, bieten die Verhaltensregeln zumindest einen gewissen Anhalt dafür, welche Speicherfristen von interessierten und mit der Materie beschäftigten Kreisen vorbehaltlich besonderer Umstände des jeweiligen Einzelfalles für notwendig und rechtmäßig erachtet werden"* (OLG München, Az. 14 U 3590/24e, Rn. 39). Im Folgenden prüfte und bejahte das OLG München, dass diese Wertung auch dem Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO entspreche (OLG München, 14 U 3590/24e, Rn. 29 ff).

Der BGH hob mit Urteil vom 18. Dezember 2025 (Az. I ZR 97/25) das Urteil des OLG Köln auf. Er führt in seiner Entscheidung aus, dass die in den aktuellen Verhaltensregeln geregelten Prüf- und Speicherfristen sachgerecht seien und demnach grundsätzlich einen angemessenen Interessenausgleich vornehmen würden. Er erklärte weiterhin, dass im Interesse der Rechtssicherheit und auch mit Blick auf das von Wirtschaftsauskunfteien betriebene Massengeschäft die Speicherfristen der aktuellen Verhaltensregeln als „Orientierung" für die nach Art. 6 Abs. 1 UAbs. 1 Buchstabe f DS-GVO vorzunehmende Interessenabwägung herangezogen werden könnten (BGH, Az. I ZR 97/25, Rn. 49 ff.).

Nur dann, wenn die betroffene Person besondere Umstände vorbringt, die einem Löschungsinteresse ein wesentlich überdurchschnittliches Gewicht verleihen, könne die Interessenabwägung ausnahmsweise dazu führen, dass in diesem Einzelfall eine kürzere Speicherdauer als angemessen anzusehen ist (BGH, Az. I ZR 97/25, Rn. 52).

Beschwerden nach Art. 77 DS-GVO

Das Urteil des OLG Köln führte bis zu dieser BGH-Entscheidung zu einer Vielzahl an Beschwerden gegen die in Hessen ansässige Wirtschaftsauskunftei. In diesen Beschwerden forderten die Beschwerdeführer auf Grundlage des Urteils des OLG Köln bei der in Hessen ansässigen Wirtschaftsauskunftei, das Negativmerkmal einer ausgeglichenen Forderung sofort nach Art. 17 DS-GVO zu löschen. Die in den Verhaltensregeln vorgesehenen Speicherfristen waren in diesen Fällen jeweils noch nicht abgelaufen. Aus diesem Grund lehnte die Wirtschaftsauskunftei die Löschung unter Berufung auf die Verhaltensregeln ab.

Ich habe diese Beschwerden dahingehend entschieden, dass in der Einhaltung der in den Verhaltensregeln beschriebenen Speicherfristen zu ausgeglichenen Forderungen durch die Wirtschaftsauskunftei kein datenschutzrechtlicher Verstoß besteht. Dies hat der BGH mit seiner Entscheidung vom 18. Dezember 2025 nun bestätigt. Meine Entscheidung habe ich auf die folgenden rechtlichen Erwägungen gestützt.

Einzelfallentscheidung des OLG Köln

Die Verhaltensregeln sind – entgegen der Auffassung des OLG Köln – grundsätzlich anwendbar und gültig. Denn bei dem Urteil des OLG Köln handelt es sich um eine Einzelfallentscheidung des Gerichts. Generell sind Gerichte nicht an Verhaltensregeln gebunden. Ob die Einhaltung der Verhaltensregeln auch die Vorgaben der DS-GVO erfüllt, haben die Gerichte eigenständig festzustellen. Darüber hinaus sind die Gerichte nicht an die Feststellungen der Aufsichtsbehörde gebunden, die besagen, dass die Verhaltensregeln der DS-GVO entsprechen. Das bedeutet, dass ein Gericht sowohl allgemein als auch im Einzelfall die Entscheidung treffen kann, dass eine Vorschrift der von der Aufsichtsbehörde genehmigten Verhaltensregeln nicht der DS-GVO entspricht.

Aus den Vorgaben der Art. 24 Abs. 3, 28 Abs. 5, 32 Abs. 3, 35 Abs. 8, 46 Abs. 3 Buchst. e und 83 Abs. 2 Satz 2 Buchst. j DS-GVO zu den Rechtswirkungen von genehmigten Verhaltensregeln ergibt sich jedoch eine Indizwirkung für die in den Verhaltensregeln getroffenen, präzisierenden Inhalte. Diese Indizwirkung gilt nicht nur für alle Aufsichtsbehörden, sondern auch für Gerichte, die den gleichen Sachverhalt bewerten. Sie müssen demnach in ihren Entscheidungen die genehmigten Verhaltensregeln berücksichtigen und sich mit ihnen auseinandersetzen (s. näher Roßnagel, Zeitschrift für Datenschutz 2025, 669, 672 ff.).

In seiner Entscheidung berücksichtigt das OLG Köln diese Indizwirkung der Verhaltensregeln nicht und lehnt die Anwendbarkeit der in ihnen enthaltenen Speicherfristen für ausgeglichene Forderungen ab. Ein pauschaler Anspruch auf Löschung von Negativeinträgen zu ausgeglichenen Forderungen nach Art. 17 DS-GVO war auch schon vor der Entscheidung des BGH aus der Entscheidung des OLG Köln nicht abzuleiten.

Dementsprechend erkannte auch die Mehrheit der gerichtlichen Entscheidungen die Verhaltensregeln und die darin enthaltenen Speicherfristen an (z. B. OLG München, Endurteil vom 11. April 2025 – 14 U 3590/24e; OLG Brandenburg, Urteil vom 3. Juli 2023 – 1 U 8/22; LG Rottweil (6. Zivilkammer), Urteil vom 20. Dezember 2023 – 6 O 65/23).

Sinn und Zweck des Art. 40 DS-GVO

Nach Art. 40 Abs. 2 DS-GVO dürfen Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln ausarbeiten. So können sehr abstrakte Regelungen der DS-GVO bereichsspezifisch präzisiert und konkretisiert werden und damit deren Anwendbarkeit gefördert werden. Zwar fehlt es Verhaltensregeln an der demokratischen Legitimation. Sie sind daher kein Ersatz für gesetzlichen Datenschutz. Jedoch ist die Praxis immer wieder mit unbestimmten Rechtsbegriffen, die die DS-GVO normiert hat, konfrontiert und in der rechtssicheren, bereichsspezifischen Anwendung herausgefordert (s. Kap. 1.3).

Insbesondere berechtigte Interessen nach Art. 6 Abs. 1 UAbs. 1 Buchst. f DS-GVO können sich von Branche zu Branche je nach Zielsetzung der Datenverarbeitung und den strukturellen Verhältnissen zwischen Verantwortlichen und betroffenen Personen enorm unterscheiden.

Aus diesen Gründen ist es sehr hilfreich, wenn Verhaltensregeln für den Regelfall festlegen, welche Zwecke der Datenverarbeitung berechtigten Interessen entsprechen, welche schutzwürdigen Interessen der betroffenen Person durch diese beeinträchtigt sein können und mit welchen Ergebnissen berechtigte und schutzwürdige Interessen im Konfliktfall branchentypisch abgewogen werden sollen (s. z. B. Roßnagel in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2. Aufl. 2025, Art. DS-GVO 40 Rn. 40).

So können Verhaltensregeln im Bereich der Wirtschaftsauskunftei etwa festlegen, welche Fristen für die weitere Erforderlichkeit einer Datenspeicherung notwendig sind, um einheitliche Speichermodalitäten zu gewährleisten. Diese Präzisierung führt zur rechtssicheren Datenverarbeitung in diesem Wirtschaftsbereich.

Selbstbindung der Verwaltung

Weiterhin begründet sich die Verbindlichkeit der Verhaltensregeln für mich aus meinem Genehmigungsbescheid vom 24. Mai 2024. Gemäß dem Grundsatz der Selbstbindung der Verwaltung bin ich an die Einhaltung dieses Bescheids gebunden. Der Grundsatz der Selbstbindung der Verwaltung leitet sich aus Art. 3 Abs. 1 GG in Verbindung mit der Verwaltungspraxis ab. Er verlangt eine ständig gleichmäßige Übung der Verwaltungspraxis und begründet somit für die Behörde, im Rahmen ihres Ermessens ähnlich gelagerte Fälle gleichartig zu entscheiden.

Beteiligung von Interessenträgern und Betroffenen bei der Erstellung

Die DS-GVO sieht in ErwG 99 vor, dass bei der Ausarbeitung, bei der Änderung oder Erweiterung von Verhaltensregeln die erstellenden Verbände maßgebliche Interessenträger, möglichst auch die betroffenen Personen, konsultieren und die Eingaben und Stellungnahmen, die sie dabei erhalten, berücksichtigen. Dies dient der Rationalität und Rechtssicherheit des Vollzugs der DS-GVO. Aus diesen Gründen wurden für die aktuellen Verhaltensregeln im Rahmen einer Verbändeanhörung der Bundesverband Deutscher Inkasso-Unternehmen, der Bundesverband E-Commerce und Versandhandel Deutschland e. V., der Verband „Die Deutsche Kreditwirtschaft“, die Verbraucherzentrale Bundesverband, die Bundesarbeitsgemeinschaft Schuldnerberatung e. V. sowie die Deutsche Industrie- und Handelskammer beteiligt. Sie wurden gebeten, zu dem Entwurf Stellung zu nehmen. Ein Großteil der beteiligten Interessenträger äußerte sich zu dem Entwurf befürwortend.

Zusätzlich hat die DSK den Entwurf der Genehmigung der aktuellen Verhaltensregeln zustimmend zur Kenntnis genommen.

Auch das OLG München sah in der Beteiligung interessierter Kreise und der weiteren Abstimmung mit den Datenschutzbeauftragten der Länder „zumindest einen gewissen Anhalt dafür, welche Speicherfristen von interessierten und mit der Materie beschäftigten Kreisen, vorbehaltlich besonderer Umstände des jeweiligen Einzelfalles, für notwendig und rechtmäßig erachtet werden“ sollten (OLG München, Urteil vom 11. April 2025, Az. 14 U 3590/24e, Rn. 39).

Kein allgemeiner Löschungsanspruch

In Einzelfällen kann eine Löschung aufgrund der Geltendmachung der „besonderen Situation“ des Art. 21 Abs. 1 DS-GVO indiziert sein (EuGH vom 7. Dezember 2023, Az. C-26/22 und C-26/24, Rn. 104 ff.). Hierzu müssen allerdings konkrete Gründe qualifiziert dargelegt werden, wieso eine solche

„besondere Situation“ vorliegt, welche die Datenverarbeitung in diesem Einzelfall nicht mehr zulässig erscheinen lässt (Kamann/Braun, in: Ehmann/Selmayr, Kommentar DS-GVO und BDSG, Art. 21 DS-GVO, Rn. 35). Allein die fehlende Möglichkeit, trotz eingeschränkter Bonität am Wirtschaftsleben weiterhin ungehindert teilnehmen zu können, rechtfertigt einen Widerspruch im Sinne des Art. 21 Abs. 1 DS-GVO nicht.

Fazit

Die Entscheidung des BGH vom 18. Dezember 2025 bestätigt meine Auffassung, dass die Prüf- und Speicherfristen der aktuellen Verhaltensregeln zu berücksichtigen sind. Folglich ist die Speicherung einer ausgeglichenen Forderung grundsätzlich für drei Jahre ab Erledigung der Forderung zulässig. Eine frühere Löschung kann sich bereits nach 18 Monaten nach Erledigung der Forderung ergeben, wenn die in Punkt IV Nr. 1 Buchst. b der Verhaltensregeln genannten Voraussetzungen vorliegen.

Denn die Verhaltensregeln erfüllen die vom Gesetzgeber in Art. 40 Abs. 2 und 5 DS-GVO normierten Anforderungen. Sinn und Zweck des Art. 40 DS-GVO würden bei einer Nichtberücksichtigung der Verhaltensregeln unterlaufen. Der BGH sieht die darin geregelten Prüf- und Speicherfristen als sachgerecht und als angemessene Interessenabwägung an. An ihr haben sich auch andere Gerichte zu orientieren.

13.2
Auskunftsersuchen gegen Online-Wettanbieter in Malta

Mehr als 100 Beschwerden wurden im Berichtsjahr gegen ein Unternehmen erhoben, das Internetplattformen für Glücksspiele, in der Regel Sportwetten, betreibt – mit steigender Tendenz. Auch gegen andere Anbieter solcher Internetplattformen richteten sich vereinzelt Beschwerden.

Das Unternehmen mit den meisten Beschwerden verarbeitet personenbezogene Daten und ist daher Verantwortlicher im Sinn von Art. 4 Nr. 7 DS-GVO. Der Sitz des Unternehmens ist jedoch in Malta und somit außerhalb meiner Zuständigkeit.

Sämtliche Beschwerden richten sich vor allem dagegen, dass der Verantwortliche beantragte Auskünfte nach Art. 15 DS-GVO nicht oder aus Sicht der Beschwerdeführenden nur unzureichend erteilt. In sämtlichen Fällen geht es darum, dass eine Aufstellung über Ein- und Auszahlungen sowie Spielverluste gefordert wird, die der Verantwortliche unter Berufung auf maltesisches Recht verweigert.

Hintergrund der Beschwerden ist, dass der Verantwortliche bis zum Inkrafttreten des Glücksspielstaatsvertrags 2021, in Hessen ratifiziert durch das Gesetz zu dem Glücksspielstaatsvertrag 2021 vom 5. Februar 2021 (GVBl. S. 86; 2025 Nr. 4), am 1. Juli 2021 keine Lizenz zum Wettbetrieb in der Bundesrepublik Deutschland hatte. Nach vielfacher obergerichtlicher Rechtsprechung sind die Spielverträge, die vor diesem Zeitpunkt geschlossen worden waren, nichtig und sämtliche Verluste zurückzuerstatten. Einige Rechtsanwaltskanzleien werben im Internet damit, diese Ansprüche (teils finanziert durch Investoren) zu erstreiten, verlangen dafür jedoch zunächst eine Übersicht über die Verluste, die, sollte sie den Beschwerdeführenden nicht vorliegen, durch eine Auskunft nach Art. 15 DS-GVO bei dem Verantwortlichen eingeholt werden könnte. Nach den Beschwerden werden entsprechende Anträge vom Verantwortlichen meist nur zögerlich bearbeitet und, falls überhaupt, schlussendlich nur dergestalt beantwortet, dass eine Übersicht über Transaktionen nicht enthalten ist.

In allen Fällen binde ich die zuständige maltesische Datenschutzaufsichtsbehörde, den Information and Data Protection Commissioner (IDPC), nach Art. 56 und 60 ff. DS-GVO ein. Er hat inzwischen zurückgemeldet, dass er die von dem Verantwortlichen vertretene Rechtsauffassung zur Verweigerung der Auskünfte nicht teilt.

Der Verantwortliche beruft sich bei der Auskunftsverweigerung auf die maltesische „Regulation 4(e) der Subsidiary Legislation 586.09“, aus der er ableitet, dass Auskünfte verweigert werden können, wenn diese „zum Zwecke der Einleitung“ eines Gerichtsverfahrens beantragt werden. Nach Auffassung des IDPC kann sich die Verantwortliche jedoch nur auf die vorgenannte Regelung berufen, wenn die Beschwerdeführenden „bereits eine Klage erhoben haben“. Der IDPC hat auch längst Bescheide erlassen, die den Verantwortlichen zur Auskunftserteilung verpflichten, gegen die der Verantwortliche wiederum Rechtsbehelfe eingelegt hat. Der IDPC wartet nun zunächst den Ausgang dieser Rechtsbehelfsverfahren ab, bevor er weitere Maßnahmen ergreift.

Ich leite weiterhin jedes Verfahren an den IDPC weiter, der dieses auch bearbeitet. Wann in den dort anhängigen Rechtsbehelfsverfahren eine endgültige Entscheidung vorliegen wird, kann ich nicht abschätzen. Es könnte jedoch durchaus noch einige Monate bis sogar Jahre dauern.

Anzumerken ist in diesem Zusammenhang, dass es inzwischen (zivilgerichtliche) Rechtsprechung, z. B. des LG Dortmund (Urteil vom 8. April 2025, Az. 5 O 162/24), gibt, nach der Anträge auf Auskünfte nach Art. 15 DS-GVO mit dem Zweck, eine Übersicht über Wetttransaktionen und insbesondere Verluste zu erlangen, rechtsmissbräuchlich sind und den Verantwortlichen

in diesen Fällen ein Auskunftsverweigerungsrecht nach Art. 12 Abs. 5 Satz 2 DS-GVO zusteht. Auch unter Beachtung der geltenden EuGH-Rechtsprechung (s. EuGH, Urteil vom 26. Oktober 2023 – Rs. C-307/22) sollen Auskunftsersuchen in den Fällen, in denen es um solche Transaktionshistorien geht, rechtsmissbräuchlich sein. Es fehle den betroffenen Personen im Gegensatz zu dem genannten EuGH-Urteil an einem Rechtsschutzbedürfnis. Sie begehrten mit ihren Auskunftsersuchen Daten, die ebenso ihrer eigenen Kenntnissphäre unterliegen würden. Es gehe ihnen in erster Linie nur darum, Beweise für die von ihnen behaupteten Rückzahlungsansprüche zu erlangen. Über sämtliche Informationen zu Geldflüssen müssten die Betroffenen jedoch auch selbst verfügen und diese im Zivilprozess insbesondere selbst vortragen und beweisen. Letztlich würde mit dem Auskunftsanspruch versucht, über dieses Instrument einen Ausforschungsbeweis zu konstruieren, der im Widerspruch zu den zivilprozessualen Grundsätzen stehe – vor allem zum Beibringungsgrundsatz.

Ich bemühe mich, mit den anderen deutschen Aufsichtsbehörden um eine einheitliche Rechtsauffassung zu diesen Fragen und Interpretationen, die durchaus einer näheren, kritischen Betrachtung und Bewertung wert zu sein scheinen.

13.3
Löschung von Daten zu dubiosen Forderungen bei Inkassounternehmen?

Soweit die Möglichkeit existiert, dass eine von einem deutschen Inkassounternehmen gegenüber einem in Deutschland wohnhaften (vermeintlichen) Schuldner geltend gemachte Forderung tatsächlich besteht, ist die Datenverarbeitung des Inkassounternehmens zu diesem Forderungssachverhalt aus datenschutzrechtlicher Sicht grundsätzlich nicht zu beanstanden. Die abschließende Klärung der Frage, ob eine zivilrechtliche Forderung materiell-rechtlich besteht, fällt nicht in die Zuständigkeit der Datenschutzaufsichtsbehörde, sondern obliegt vielmehr der Zivilgerichtsbarkeit. Eine datenschutzrechtliche Löschungsanordnung gegenüber dem Inkassounternehmen bezüglich der entsprechenden Forderungsdaten kommt in derartigen Fallkonstellationen nicht in Betracht.

Viele Beschwerden richteten sich gegen ein Inkassounternehmen, das durch Webseiten-Betreiber mit der Beitreibung von Forderungen mandatiert wurde. Die Beschwerdeführenden bestreiten u. a. das materiell-rechtliche Bestehen der Forderung und halten die Datenverarbeitung des Inkassounternehmens in diesem Forderungszusammenhang für unzulässig.

Dubiose Forderung

Der Beitragsservice für ARD, ZDF und Deutschlandradio ist insbesondere für die Realisierung von Rundfunkgebühren gegenüber beitragspflichtigen Personen zuständig. Der Homepage des Beitragsservice https://www.rundfunkbeitrag.de/ sind diesbezüglich u. a. folgende Erläuterungen zu entnehmen:

„(…) Der Beitragsservice ist eine Gemeinschaftseinrichtung von ARD, ZDF und Deutschlandradio mit Sitz in Köln. (…)

Die Hauptaufgaben des Beitragsservice sind der Einzug des Rundfunkbeitrags und die Verwaltung der rund 47 Millionen Beitragskonten. (…)

Als zentrale Ansprechpersonen für Bürgerinnen und Bürger wie auch Unternehmen, Institutionen und Einrichtungen des Gemeinwohls kümmern sich die Mitarbeitenden des Beitragsservice um die Bearbeitung von Anliegen und Fragen rund um den Rundfunkbeitrag. Sie erfassen und bearbeiten beispielsweise Anmeldungen, die Änderung von Daten sowie Anträge auf Ermäßigung und Befreiung. (…)

Grundlage für die Erhebung des Rundfunkbeitrags und die Arbeit des Beitragsservice von ARD, ZDF und Deutschlandradio ist der von allen 16 Landesparlamenten ratifizierte Rundfunkbeitragsstaatsvertrag (RBStV). Er legt fest, wie der Rundfunkbeitrag berechnet wird, wer ihn zu zahlen hat und für wen besondere Regelungen gelten.

Zusätzlich hat jede Landesrundfunkanstalt eine Beitragssatzung erlassen. Die Satzungen sind im Wesentlichen wortgleich. Sie wurden durch die zuständigen Behörden in jedem Bundesland genehmigt. (…)“

Neben Informationen zum Rundfunkbeitrag stellt der Beitragsservice auf seiner Website u. a. den Bürgerinnen und Bürgern Formulare zur Verfügung, mit denen sie ihre Anliegen geltend machen können, wie etwa die Ummeldung eines Wohnsitzes, die Änderung des Namens oder der Kontoverbindung. Diese Formulare können auf der Website entweder unmittelbar online ausgefüllt oder als PDF-Dokumente zum Ausfüllen heruntergeladen werden. Für die Bearbeitung dieser Anliegen wie z. B. die Ummeldung eines Wohnsitzes fallen für die betroffenen Bürgerinnen und Bürger keine Gebühren oder Kosten an.

Im Gegensatz zu dem öffentlich-rechtlichen Beitragsservice betreibt der privatrechtliche Anbieter „Rundfunkbeitragshilfe L.L.C“ unter der URL https://rundfunkbeitrag-service.de/ eine Webseite, auf der ein verwechslungsfähiger „Online-Service Rundfunkbeitrag“ kostenpflichtig wie folgt angeboten wird:

„(…) Sie sind umgezogen und möchten der Rundfunkanstalt Ihre neue Adresse nennen oder Ihre geänderte Bankverbindung mitteilen? Diese und viele weitere Anliegen können Sie jetzt einfach über unser Online-Formular absenden.(…)

Online-Service für den Rundfunkbeitrag

(…)

1. Online-Formular

Wählen Sie einfach das gewünschte Online-Formular, welches Sie übermitteln möchten. Sie werden Schritt für Schritt durch das Online-Formular geleitet. (…)

2. Antrag erstellen

Anhand der von Ihnen gemachten Angaben erstellen wir die benötigten Formulare. Alle Formulare werden automatisch erstellt. (…)

3. Antrag Versand

Wir überprüfen Ihre Angaben und senden die Formulare an die Rundfunkanstalt. (…)

Hilfreiche Links

– Abmelden einer Wohnung

– Änderung zum Beitragskonto mitteilen

– Erstanmeldung einer Wohnung

– Anmeldung einer weiteren Wohnung (…)“

Neben diesen Links, über die man ausschließlich zu den jeweiligen Online-Formularen gelangt, ist – neben weiteren Links, wie etwa Impressum oder Datenschutz, – auf der rechten unteren Seite dieser Homepage folgender weiterer Hinweis zu finden:

„(…) Hinweis zum Service

Wir sind ein unabhängiger Online-Service, wir stehen in keiner Verbindung zu den öffentlich-rechtlichen Rundfunkanstalten. (…)“

Bei Nutzung des Formulars „Abmelden einer Wohnung“ ist im abschließenden Informationstext bei genauerer Betrachtung am Ende des ersten Absatzes des Hinweistextes folgender Hinweis zu den Kosten für die Nutzung dieses „Services“ zu finden:

„(…) Kosten für die Abmeldung Ihres Beitragskontos gesamt 39,99 €. Sie erhalten dann eine Bestätigung. (…)“

Zusammenfassend kann daher zum Sachverhalt festgestellt werden, dass der privatrechtliche Anbieter „Rundfunkbeitragshilfe L.L.C“ gegenüber dem Beitragspflichtigen Kosten in Höhe von 39,99 € für einen Service generiert, den der Bürger bei Nutzung der Formulare der Website des öffentlich-rechtlichen Beitragsservice völlig kostenfrei selbst erledigen könnte.

Gemäß der Anbieterkennzeichnung sitzt dieser privatrechtliche Anbieter „Rundfunkbeitragshilfe L.L.C“ in Dubai, Vereinigte Arabische Emirate.

Nachdem der Beschwerdeführer zunächst Zahlungsaufforderungen dieses Dienstleisters über die vorgenannten Kosten in Höhe von 39,99 € erhalten hat, erfolgt sodann die Mandatierung eines in Hessen ansässigen Inkassounternehmens.

Verpflichtung zur Löschung?

Die hier eingehenden Beschwerden richten sich sowohl gegen den Anbieter „Rundfunkbeitragshilfe L.L.C“ (mit Sitz in Dubai) als auch gegen das mandatierte hessische Inkassounternehmen.

Ein Beschwerdeführer trägt z. B. vor:

Er habe die Dienstleistung des privatrechtlichen Anbieters „Rundfunkbeitragshilfe L.L.C“ versehentlich in Anspruch genommen, da diese durch deren Website vorgebe, offizieller Teil des öffentlich-rechtlichen ARD ZDF Beitragsservices zu sein. Er habe den gegenständlichen Vertragsschluss fristgerecht nach § 355 BGB widerrufen und Löschung seiner personenbezogenen Daten gemäß Art. 17 DS-GVO gefordert. Gleichwohl seien seine Daten ohne rechtmäßige Grundlage an das Inkassounternehmen weitergeleitet worden. Weder auf seinen Widerruf noch auf dessen Aufforderung zur Datenlöschung sei reagiert worden. In seinen an die „Rundfunkbeitragshilfe L.L.C“ sowie das Inkassounternehmen gerichteten Schreiben vertritt der Beschwerdeführer weiterhin die Ansicht, ein wirksamer Vertrag sei nicht zustande gekommen. Vielmehr lägen eine arglistige Täuschung nach § 123 BGB sowie „irreführende Geschäftspraktiken nach § 5 UWG vor: Die Website des Unternehmens erwecke bewusst den Eindruck, es handele sich um den öffentlich-rechtlichen Beitragsservice, was wettbewerbswidrig und vertragsschädlich sei. Die geltend gemachte Forderung sei mithin nicht durchsetzbar. Die Daten seien daher jeweils zu löschen.

Der Beschwerdeführer bittet meine Behörde um Prüfung der Frage, ob ein Verstoß u. a. gegen Art. 17 DS-GVO vorliegt. Art. 17 DS-GVO lautet wie folgt (Zitat):

Art. 17 DS-GVO

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

a) Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.

b) Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.

c) Die betroffene Person legt gemäß Artikel 21 Absatz 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt gemäß Artikel 21 Absatz 2 Widerspruch gegen die Verarbeitung ein.

d) Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

e) Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.

f) Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft gemäß Artikel 8 Absatz 1 erhoben. (…)

(3) Die Absätze 1 und 2 gelten nicht, soweit die Verarbeitung erforderlich ist (…)

e) zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Die hier zugrundeliegende Fragestellung nach dem wirksamen Zustandekommen des Dienstleistungsvertrages und damit des Bestehens der Forderung in Höhe von 39,99 € ist zivil- bzw. wettbewerbsrechtlicher Natur und entzieht sich damit meiner Beurteilung als Datenschutzaufsichtsbehörde. Dies ist vielmehr durch die Zivilgerichtsbarkeit zu klären. Eine offenkundige Sittenwidrigkeit (und damit Nichtigkeit des Rechtsgeschäfts von Anfang an), die ich hier eventuell berücksichtigen könnte, ist für mich schwer zu begründen. Vielmehr besteht die Möglichkeit, dass die geltend gemachte Forderung ggf. doch besteht. Dann greift die Ausnahme nach Art. 17 Abs. 3 Buchst. e DS-GVO. Damit ist die Datenverarbeitung des Inkassounternehmens aus datenschutzrechtlicher Sicht zunächst nicht zu beanstanden. Eine Löschungsanordnung gegenüber dem Inkassounternehmen kommt somit nicht in Betracht.

Hinsichtlich der Zulässigkeit der Datenverarbeitung durch Inkassounternehmen verweise ich auf meinen 49. Tätigkeitsbericht (Ziffer 12.3, Seiten 115 ff.).

Hinsichtlich einer etwaigen datenschutzrechtlichen Prüfung eines Unternehmens mit Sitz in Dubai ist ergänzend Folgendes auszuführen: Ein solches unterfällt mangels Zuständigkeit nicht der hessischen Datenschutzaufsicht. Ich bin örtlich nur zuständig für datenverarbeitende Stellen mit Sitz in Hessen. Die nach Art. 50 Buchst. a, b DS-GVO vorgesehenen Maßnahmen zur wirksamen Durchsetzung von Rechtsvorschriften zum Schutz personenbezogener Daten in Ländern außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums wurden bisher nicht getroffen.

13.4
Auskünfte von Kreditinstituten an Jobcenter

Bei Anfragen von Jobcentern nach § 60 Abs. 2 SGB II haben Kreditinstitute den Umfang der zu übermittelnden Daten zu prüfen und zu begrenzen.

Kreditinstitute, die Konten für ihre Kundinnen und Kunden führen, sind gemäß § 60 Abs. 2 SGB II dazu verpflichtet, bei Auskunftsersuchen durch Jobcenter bestimmte Informationen an diese zu übermitteln. Im Rahmen einer Beschwerde habe ich den Umfang der erteilten Auskünfte überprüft. Hierbei stellte sich heraus, dass die überprüfte Bank den Umfang aus dem Auskunftsersuchen des Jobcenters vollumfänglich erfüllt hatte, ohne zu überprüfen, ob dieses vom Gesetzeswortlaut gedeckt war. Sie wurde im Rahmen des Auskunftsbegehrens vom Jobcenter um die Zusendung von Kontoauszügen ersucht.

Anforderungen an die Rechtmäßigkeit

Nach Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO ist eine Datenverarbeitung, hier Datenübermittlung, rechtmäßig, sofern diese zur Erfüllung einer rechtlichen Verpflichtung erfolgt.

> *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; (…)*

Im Rahmen von Auskunftsersuchen nach § 60 Abs. 2 SGB II ist die Herausgabe von Kontoauszügen an das anfragende Jobcenter hingegen datenschutzrechtlich nicht rechtmäßig, da vom Wortlaut der Norm nicht gedeckt.

§ 60 Abs. 2 SGB II

(2) Wer jemandem, der eine Leistung nach diesem Buch beantragt hat oder bezieht, zu Leistungen verpflichtet ist, die geeignet sind, Leistungen nach diesem Buch auszuschließen oder zu mindern, oder wer für ihn Guthaben führt oder Vermögensgegenstände verwahrt, hat der Agentur für Arbeit auf Verlangen hierüber sowie über damit im Zusammenhang stehendes Einkommen oder Vermögen Auskunft zu erteilen, soweit es zur Durchführung der Aufgaben nach diesem Buch erforderlich ist. § 21 Absatz 3 Satz 4 des Zehnten Buches gilt entsprechend. Für die Feststellung einer Unterhaltsverpflichtung ist § 1605 Absatz 1 des Bürgerlichen Gesetzbuchs anzuwenden.

Bei Auskunftsersuchen nach § 60 Abs. 2 SGB II darf die Bank daher darauf vertrauen, dass das Auskunftsersuchen dem Grunde nach rechtmäßig ist und sich der Vorgang so darstellt, wie von der Behörde dargelegt, also dass eine derartige Prüfung im Rahmen des Leistungsbezugs oder Leistungsantrags erforderlich ist. Die Behörde führt hoheitliche Aufgaben aus, so dass die Anfrage bezüglich dieser Grundvoraussetzungen nicht in Zweifel zu ziehen ist.

Prüfpflicht zum Umfang der Auskunft

Anders gestaltet es sich beim Umfang der Anfrage bezogen auf die Daten, die zu beauskunften sind. § 60 Abs. 2 SGB II legitimiert die Preisgabe von Informationen über das Vermögen (Kontostände) und das Einkommen. Daher darf die Bank in diesem Rahmen auch entsprechend Auskunft erteilen und die Übermittlung auf Art. 6 Abs. 1 UAbs. 1 Buchst. c DS-GVO i. V. m. § 60 Abs. 2 SGB II stützen. Da allerdings der Umfang durch den Wortlaut der Norm klar definiert ist, muss die Bank das Auskunftsersuchen dahingehend auch überprüfen. Sollte diese Prüfung ergeben, dass der Umfang des Ersuchens über den in der Norm definierten Umfang hinausgeht, wie es z. B. bei der Anforderung von Kontoauszügen, also Kontoumsatzdaten, der Fall ist, wäre die zu erteilende Auskunft auf das Maß der Regelungen des Art. 60 Abs. 2 SGB II (Auskunft über Einkommen und Vermögen) zu beschränken.

Es besteht daher zwar keine Pflicht, das Auskunftsersuchen bezüglich des Vorliegens der Voraussetzungen zu prüfen, bezüglich des gemäß § 60 Abs. 2 SGB II definierten Umfangs der zu erteilenden Auskunft besteht hingegen eine Prüfpflicht.

13.5
Selbstauskunft an Stellvertreter

Die Geltendmachung des Auskunftsanspruchs nach Art. 15 DS-GVO wirft in der Praxis die Frage auf, ob und in welchem Umfang dieser Anspruch durch einen Vertreter ausgeübt werden kann.

Art. 15 DS-GVO gewährt betroffenen Personen ein zentrales Grundrecht: das Recht auf Auskunft über die Datenverarbeitung ihrer personenbezogenen Daten. Dieses Grundrecht ist Ausdruck des Transparenzgrundsatzes nach Art. 5 Abs. 1 Buchst. a DS-GVO und bildet eine Grundlage für die Geltendmachung von weiteren Betroffenenrechten wie etwa Berichtigung, Löschung oder Einschränkung der Verarbeitung.

Mich erreichte eine Beschwerde gegen eine in Hessen ansässige Auskunftei. Der Beschwerdeführer wohnt im außereuropäischen Ausland und bat die Auskunftei um die Übermittlung einer Datenauskunft gemäß Art. 15 DS-GVO an eine von ihm bevollmächtigte Person. Eine entsprechende Vollmachtsurkunde einschließlich Einwilligungserklärung zur Datenübermittlung wurde beigefügt.

Die verantwortliche Stelle verweigerte die Zustellung der Auskunft an den Bevollmächtigten mit der Begründung, dass nur so sichergestellt werden könne, dass die angeforderte Auskunft auch tatsächlich den Empfänger erreiche. In der Praxis stellt sich häufig die Frage, ob und inwieweit Dritte das Auskunftsrecht des Betroffenen nach Art. 15 DS-GVO wirksam in dessen Namen geltend machen können. Dabei kommt den zivilrechtlichen Regelungen über die Stellvertretung nach §§ 164 ff. BGB eine maßgebliche Bedeutung zu.

Nach Art. 15 DS-GVO hat die betroffene Person das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Sollte dies der Fall sein, so besteht ein Anspruch auf Auskunft über weitere Informationen zur Verarbeitung von Daten des Anspruchstellers.

Stellvertretung nach § 164 ff. BGB

Gemäß § 164 Abs. 1 Satz 1 BGB wirkt eine Willenserklärung, die ein Vertreter innerhalb der ihm zustehenden Vertretungsmacht im Namen des Vertretenen abgibt, unmittelbar für und gegen den Vertretenen.

Eine wirksame Stellvertretung setzt voraus:

1. Abgabe einer Erklärung im Namen des Vertretenen („Offenkundigkeit“),
2. Vertretungsmacht (gesetzlich, behördlich oder durch Vollmacht),

3. keine höchstpersönliche Handlung, die nur der Betroffene selbst vornehmen kann.

Art. 15 Abs. 1 DS-GVO bestimmt, dass der Auskunftsanspruch der betroffenen Person zusteht. Hieraus wird überwiegend abgeleitet, es handle sich bei dem Auskunftsrecht nach Art. 15 DS-GVO um ein höchstpersönliches Recht (s. z. B. Paal/Kritzer, NJW 2022, 2437). Hieraus folge, dass eine Abtretung des Anspruchs oder sonstige Übertragung auf Dritte nicht erfolgen könne (Schmidt-Wudy, in: BeckOK Datenschutzrecht, 42. Ed. 1.11.2022, DS-GVO Art. 15 Rn. 35). Allerdings bestehe die Möglichkeit, die Geltendmachung durch Dritte im Wege der rechtsgeschäftlichen Bevollmächtigung zu erreichen. Eine mittelbare Indizwirkung für die Anwendbarkeit der Betroffenenrechte durch bevollmächtigte Personen stellt zudem Art. 80 DS-GVO dar, der ein Verbandsklagerecht für gemeinnützige Verbände vorsieht.

Die Leitlinien des EDSA bejahen die Möglichkeit des Handelns eines Dritten im Namen der betroffenen Person im Rahmen der Auskunftserteilung nach Art. 15 DS-GVO (EDSA- Leitlinien 01/2022, Version 2.0, Rn. 80).Hierbei sollen die einzelstaatlichen Rechtsvorschriften über die rechtmäßige Vertretung (z. B. Vollmacht) angewendet werden. Folglich sind die Regeln der rechtsgeschäftlichen Stellvertretung nach §§ 164 ff. BGB maßgeblich.

Demnach kann die bevollmächtigte Person sowohl den Antrag auf Erteilung einer Auskunft gemäß Art. 15 DS-GVO stellen als auch die Datenauskunft entgegennehmen.

Die Vollmacht ist gegenüber der verantwortlichen Stelle nachzuweisen (s. näher OLG Stuttgart (9. Zivilsenat), Urteil vom 31. März 2021 – 9 U 34/21 BeckRS 2021, 6282 Rn. 33). Sie muss sich ausdrücklich sowohl auf die Geltendmachung des Anspruchs gemäß Art. 15 DS-GVO als auch auf den Empfang der zu beauskunftenden personenbezogenen Daten beziehen und somit inhaltlich klar und bestimmt sein.

Gemäß Art. 12 Abs. 3 DS-GVO hat die verantwortliche Stelle einen Monat Zeit, auf die Geltendmachung von Betroffenenrechten im Sinne der Art. 15-22 DS-GVO zu reagieren. Bei der Bevollmächtigung beginnt die Frist erst dann, wenn eine hinreichende Legitimation des Vertreters gegenüber der verantwortlichen Stelle vorliegt (AG Berlin-Mitte: Frist für Auskunftsanspruch nach Art. 15 DS-GVO bei Verlangen einer Vollmachtsvorlage, ZD 2020, 647 Rn. 16).

Aufgrund der Tatsache, dass die zuvor aufgezählten Voraussetzungen vorlagen, wies ich die Auskunftei an, die Auskunft gemäß Art. 15 DS-GVO an den Vertreter zu versenden.

13.6
Ware bestellt – Probleme mit Daten geliefert

Das Internet kennt keine Staatsgrenzen. Mühelos lässt sich das Pendant großer europäischer Tauschbörsen, virtueller Marktplätze, Informations- oder Dienstleistungsseiten in jedem beliebigen Land der Welt aufrufen, erkunden und auch nutzen.

Man spart sich den kostspieligen Umweg über ein Reisebüro, wenn man das Urlaubsdomizil direkt auf der Internetseite des Betreibers bucht. Und welcher Sammler von Raritäten freut sich nicht, wenn ein lang gesuchtes Sammlerstück irgendwo auf dem Erdenrund endlich zum Kauf angeboten wird. Wer zudem nach Schnäppchen bei Elektronik- und Technikartikeln oder Fashion und Accessoires sucht, stößt häufig auf Onlineshops aus Asien. Auch auf Social Media-Plattformen tauchen immer wieder Anzeigen von Shops aus aller Welt auf, die Produkte zu besonders günstigen Preisen anbieten.

Viele Websites und die dort angepriesenen Angebote erwecken mit scheinbar seriöser Gestaltung und in fehlerfreier deutscher Sprache den Eindruck eines inländischen Händlers. Verstärkt wird dieser Eindruck zumeist noch durch die Verwendung einer .de-Domain. Die „Story“ auf der Website suggeriert häufig, dass der Shop-Inhaber die gleichen Interessen mit derselben Leidenschaft wie die potenziellen Käufer teilt und mit seinem Herzensprojekt nun Waren für ein gemeinsames Hobby offeriert.

Der Blick in die Allgemeinen Geschäftsbedingungen oder das Impressum kann – sofern vorhanden – den tatsächlichen Firmensitz aufzeigen. Hier endet die authentische Story der Website und der leidenschaftliche Anbieter für alpines Wanderzubehör hat seinen Sitz nicht in einem Dorf mit Bergpanorama, sondern zumeist in einem Industrie- oder Businessdistrikt außerhalb der EU.

Die Meldungen und Hinweise von Beschwerdeführern häufen sich, die Onlinedienstleistungen nutzen oder bei vermeintlich lokalen Onlineshops einkaufen. Die Gründe für Beschwerden sind sehr vielfältig: nicht oder falsch gelieferte Ware, Probleme bei der Reklamation oder Vertragsabwicklung. Eine Beschwerdeführerin hatte die Sorge, dass die im Ausland betriebene Website für eine Onlinepartnervermittlung die von ihr übersandte Ausweiskopie zum Identitätsdiebstahl missbrauchen könnte. Da für diese Fälle die Datenschutzbehörden nicht zuständig sind, bleibt hier häufig nur der Verweis bei Verdacht auf Straftaten an die jeweiligen Strafverfolgungsbehörden oder bei Streitigkeiten mit dem Unternehmen an die Zivilgerichte.

Doch auch Beschwerden mit datenschutzrechtlichen Belangen werden regelmäßig an mich herangetragen. Dabei geht es meist um die Durchsetzung von Betroffenenrechten. Die DS-GVO sieht u. a. das Recht auf Auskunft über

die gespeicherten Daten (Art. 15 DS-GVO), das Recht auf Berichtigung oder Löschung der gespeicherten Daten (Art. 16 und 17 DS-GVO) und das Recht auf Widerspruch gegen die Datenverarbeitung (Art. 21 DS-GVO) vor. Die Unternehmen müssen auf entsprechende Ersuchen der betroffenen Person nach Art. 12 Abs. 3 DS-GVO binnen eines Monats reagieren.

Nicht selten erhalten die Beschwerdeführer durch das Unternehmen, auch bei mehrfacher Nachfrage, keine oder nur eine sehr unbefriedigende Antwort. Hier bleibt die betroffene Person oft im Unklaren, welche ihrer personenbezogenen Daten zu welchem Zweck und über welchen Zeitraum durch das Unternehmen verarbeitet werden. Dabei sind auch Unternehmen, die über keine Niederlassung in der EU verfügen, dennoch nach Art. 3 Abs. 2 DS-GVO zur Einhaltung der DS-GVO verpflichtet, wenn sich ihr Produktangebot an europäische Kunden richtet. Allerdings wird der europäische Standard beim Datenschutz in Unternehmen mit Sitz außerhalb der EU nicht immer umgesetzt, auch wenn hier auf den Websites explizit damit geworben wird und die Einhaltung von Betroffenenrechten als Selbstverständlichkeit aufgeführt ist.

Die Durchsetzung der Betroffenenrechte außerhalb der EU und dem EWR ist schwierig. Dies gilt auch für die Durchsetzung einer Anweisung zu datenschutzgerechter Datenverarbeitung oder zu datenschutzkonformem Verhalten durch die Aufsichtsbehörden in der EU. Sie haben im außereuropäischen Ausland keine Weisungsbefugnis. Eine Abhilfe oder die Ahndung von datenschutzrechtlichen Verstößen ist nicht in jedem Fall möglich. Zu den Ländern außerhalb des Geltungsbereiches der DS-GVO zählen im Übrigen auch die Schweiz und das Vereinigte Königreich.

Zwar sind Verantwortliche nach § 40 Abs. 4 Satz 1 BDSG verpflichtet, mir entsprechende Auskünfte zu Sachverhalten zu erteilen. Hierzu kann ich sie auch nach Art. 58 Abs. 1 Buchst. a DS-GVO anweisen. Meine Möglichkeiten, diese Anordnung außerhalb der EU durchzusetzen, sind jedoch äußerst beschränkt. Existiert eine Niederlassung innerhalb der EU, kann ich die dort zuständige Aufsichtsbehörde nach Art. 56 DS-GVO um Amtshilfe oder nach Art. 60 DS-GVO um Fallübernahme als federführende Aufsichtsbehörde bitten. In vielen Fällen konnte so dem Datenschutz dank der europäischen Zusammenarbeit Rechnung getragen werden.

Nach Art. 77 DS-GVO und 57 Abs. 1 Buchst. f DS-GVO bin ich angehalten, Beschwerden in einem „angemessenen Umfang“ zu bearbeiten (ErwG 141 DS-GVO). Ein nicht wirksam durchführbares Verwaltungsverfahren gegen einen außereuropäischen Verantwortlichen widerspricht jedoch in vielen Fällen einem angemessenen Umfang. Oftmals lässt sich mangels korrekten Impressums nebst fehlenden oder widersprüchlichen Angaben mit den mir zur Verfügung stehenden Ermittlungswerkzeugen kein Verantwortlicher

feststellen. Auch aus den durch die Beschwerdeführer vorgelegten Unterlagen wie Kaufvertrag oder Schriftverkehr geht nicht immer eindeutig hervor, mit welchem Unternehmen hier nun Handel betrieben wurde. Die Suche nach dem Verantwortlichen über die registrierte Website ist nicht in jedem Fall zielführend. Auch Anfragen über die zentrale Registrierungsstelle der .de-Domains führen immer wieder zu falschen Daten. So gab es z. B. in einem Fall zwar den inländischen Ort, jedoch war die angegebene Straße auch auf Nachfrage bei der zuständigen Gemeindeverwaltung nicht zu finden. Mangels Erfolgsaussichten ist somit eine Verfolgung von Datenschutzverstößen nicht immer möglich und eine Abhilfe der Beschwerde kann nicht erfolgen.

In meiner täglichen Arbeit weise ich präventiv darauf hin, dass ein seriöser Anbieter, der zumeist auch eine rechtskonforme Datenverarbeitung gewährleistet, oftmals daran zu erkennen ist, ob Gütesiegel oder authentische Bewertungen auf entsprechenden Portalen vorliegen. Auch lohnt der Blick in das Impressum. Sind hier nachvollziehbare Daten vorhanden, existiert zumindest eine Niederlassung innerhalb der EU? Mit wenigen Klicks kann man selbst prüfen, ob eine datenschutzkonforme Bearbeitung durch ein Onlineangebot erfolgt und ob im Problemfall eine Abhilfe mit Hilfe einer europäischen Aufsichtsbehörde möglich ist.

13.7
Einsichtnahme in personenbezogene Daten bei Online-Bestelldiensten

Auch Online-Bestelldienste für Restaurants müssen die Gewährleistungsziele Vertraulichkeit und Integrität der Datenverarbeitung erfüllen. Gleichwohl zeigen aktuelle Beschwerden, dass bei zahlreichen Anbietern dies nicht der Fall ist. Insbesondere mangelt es häufig an angemessenen technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO zur wirksamen Zugriffssicherung personenbezogener Bestelldaten vor der Einsicht durch unbefugte Dritte.

Online-Bestellungen von Mahlzeiten und Getränken gehören mittlerweile zum festen Bestandteil des Alltags. Marktforschungsdaten belegen, dass der Umsatz im Bereich der Online-Bestelldienste für Restaurants (sog. Online-Food-Delivery) in Deutschland kontinuierlich steigt und auch in den kommenden Jahren weiteres Wachstum zu erwarten ist (https://de.statista.com/themen/3440/food-delivery-lieferdienste-lieferservice-portale).

Zugriffsmöglichkeiten

Mit dieser zunehmenden Digitalisierung des Bestell- und Lieferprozesses gehen jedoch erhebliche Herausforderungen im Bereich des Datenschutzes einher. Online-Bestelldienste verarbeiten im Rahmen ihrer Geschäftsprozesse regelmäßig eine Vielzahl personenbezogener Daten ihrer Kundschaft, darunter Kontaktdaten, Zahlungsinformationen sowie Bestellhistorien. Der Schutz dieser sensiblen Informationen ist nicht nur aus Gründen des Verbrauchervertrauens, sondern auch im Hinblick auf die Einhaltung der gesetzlichen Verpflichtungen gemäß der DS-GVO von zentraler Bedeutung. Insbesondere sind die Anbieter solcher Dienste gemäß Art. 32 DS-GVO verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um diese personenbezogenen Daten vor einer Einsicht durch unberechtigte Dritte zu schützen.

Eine Zunahme von Beschwerden zu Online-Bestelldiensten bei Restaurants zeigt jedoch, dass mehrere Anbieter die datenschutzrechtlichen Vorgaben nur unzureichend umgesetzt und keine geeigneten Maßnahmen zum Zugriffsschutz implementiert haben. Alle diese Beschwerden hatten als gemeinsamen Sachverhalt, dass der jeweilige Online-Bestelldienst eine Detailansicht für Bestellungen in seiner Bestellübersicht im Internet bereitstellte und der Zugriff auf die jeweilige Bestellübersicht allein die Eingabe der korrekten nummerischen Bestellnummer voraussetzte. Diese Ansichten dienten dazu, bestellenden Personen eine Ansicht ihrer Bestellung zur Kontrolle und Statusverfolgung zu ermöglichen. Da diese Bestellnummern von den jeweiligen Dienstleistern häufig einfach in hochzählender Weise vergeben wurden, war es ein Leichtes, korrekte Bestellnummern zu erraten. Besonders kritisch machte diesen Umstand, dass zur Prüfung, ob eine erratene Bestellnummer valide ist, keine Nutzung einer Eingabemaske notwendig war. Mehrere Bestelldienste ermöglichten durch Manipulation der Internetadresse zur Bestellübersicht, erratene Bestellnummern auf Korrektheit zu überprüfen. Als Beispiel für einen solchen Fall sei hier die fiktive Internetadresse www.bestelldienst-xyz.de/Bestellung/12345 genannt. Durch Abänderung dieser Internetadresse mittels einer validen Bestellnummer – also das Austauschen der Nummer „12345“ durch z. B. „98765“ – und den anschließenden Aufruf im Browser-Fenster, wird die Bestellübersicht einsehbar und somit ein unberechtigter Zugriff auf die dahinterliegenden personenbezogenen Daten möglich. Da das Erraten von Bestellnummern und die manuelle Prüfung auf Korrektheit zeitaufwendig sein kann, waren hier Hilfsmittel wie kleine Programme denkbar. Mit wenigen Zeilen Programm-Code konnte es möglich sein, solche Angriffe vollautomatisiert durchzuführen und im Erfolgsfall die jeweilige Bestellübersicht in geeigneter Form für eine weitere Verarbeitung abzuspeichern. Da die Prüfung mittels eines solchen Programms dann im Sekundenbereich und ohne manuelle Eingriffe möglich war, konnten unberechtigte Dritte bereits nach kurzem

Zeitraum auf eine Vielzahl von Bestellübersichten Zugriff nehmen. Auch meine Mitarbeiter haben im Rahmen der Bearbeitung der Beschwerden und hier insbesondere zur Beweissicherung diesen Ansatz erfolgreich verfolgt.

Die Tatsache, dass der Zugriff auf die personenbezogenen Daten einer Bestellübersicht allein mittels Bestellnummer möglich ist und geeignete technische und organisatorische Maßnahmen zum Zugriffsschutz fehlen, kann eine Verletzung der Vertraulichkeit und einen Verstoß gegen Art. 32 Abs. 1 Buchst. b DS-GVO darstellen. Üblicherweise wären hier zumindest Maßnahmen zur Authentisierung (Nachweis der Identität des zugreifenden Benutzers) und zur Autorisierung (Überprüfung der Zugriffsbefugnis dieses Benutzers auf einen bestimmten Datensatz) zu erwarten. Personenbezogene Daten, die durch Ausnutzen einer solchen Schwachstelle durch unberechtigte Dritte erbeutet werden, können beispielsweise für Identitätsmissbrauch und Betrugsvergehen und somit zum Nachteil der Betroffenen genutzt werden.

Bezeichnend ist in diesem Kontext auch, dass das Phänomen des fehlerhaften Zugriffsschutzes die Liste der von der US-amerikanischen Sicherheitsstiftung Open Web Application Security Project (OWASP) herausgegebenen „OWASP Top 10“ der am häufigsten beobachteten Klassen von Schwachstellen regelmäßig anführt. Es handelt sich somit um eine Form von Schwachstellen, die Software-Entwicklern im Allgemeinen und Anbietern von Bestelldiensten im Speziellen unbedingt bekannt sein sollte und die sie in geeigneter Weise angemessen adressieren müssen.

Unzureichende Abhilfemaßnahmen

Bei der Bearbeitung von hierauf bezogenen Beschwerden haben Dienstleister mir teilweise Abhilfemaßnahmen präsentiert, die für sich genommen zur Sicherstellung eines angemessenen Zugriffsschutzes unwirksam waren. Hierzu gehörte beispielsweise die Deaktivierung der Bestellübersichten nach einem bestimmten Zeitraum. Gemäß Art. 5 Abs. 1 Buchst. e DS-GVO dürfen personenbezogene Daten nur so lange gespeichert werden, wie es der Zweck, zu dem sie verarbeitet werden, erfordert. Dieser Grundsatz der Speicherbegrenzung gilt generell bei der Verarbeitung von personenbezogenen Daten und muss daher auch von den Anbietern der Bestelldienste beachtet werden. Die Speicherbegrenzung kann jedoch nicht verhindern, dass zu dem Zeitpunkt, an dem die jeweilige Bestellübersicht im Internet verfügbar ist, auf diese zugegriffen wird. Eine weitere Maßnahme, die für sich allein unwirksam ist, stellte die zufällige Vergabe von Bestellnummern anstelle eines einfachen Hochzählens dar. Zwar ist denkbar, dass hierdurch die manuelle Prüfung nach validen Bestellnummern erschwert wird, durch den automatisierten Ansatz mittels eines Programmes kann diese Erschwernis

allerdings recht einfach umgangen werden – insbesondere da sich der Bereich gültiger Bestellnummern in einem automatisiert leicht zu handhabenden Größenfenster bewegt.

Notwendige Schutzmaßnahmen

Eine geeignete Maßnahme kann hingegen eine wirksamere Authentisierung/Autorisierung mittels weiterer, für den Zugriff erforderlicher Informationen neben der Bestellnummer darstellen. Versanddienstleister nutzen bei der Bereitstellung von Sendungsverfolgungsfunktionen im Internet häufig die Postleitzahl des Kunden als weitere Zugangskennung, diese Lösung ist auch für Online-Bestelldienste von Restaurants denkbar. Zu beachten ist hierbei jedoch, dass auch hier wieder automatisierte Angriffe denkbar sind. Zwar bedeutet die zweite Zugangskennung eine höhere Komplexität bei der Entwicklung eines hierfür zum Einsatz geeigneten Algorithmus und sie verzögert auch die Durchführung dieser automatisierten Prüfungen, die zweite Zugangskennung alleine verhindert diesen Ansatz jedoch nicht. Bestelldienstleister müssen daher weitere geeignete Maßnahmen implementieren, um zu verhindern, dass solche automatisierten Angriffe erfolgreich sind. Eine geeignete Maßnahme kann hierbei etwa die Vorgabe eines Limits an möglichen Abfragen von einer bestimmten IP-Adresse in einem bestimmten Zeitraum darstellen. Eine weitere denkbare Maßnahme kann in Verbindung damit auch das Implementieren einer Verzögerung zwischen zwei Aufrufen von der gleichen IP-Adresse darstellen.

Insgesamt lässt sich festhalten, dass Online-Bestelldienste von Restaurants durch das Fehlen einer wirksamen Zugriffskontrolle und die unzureichende Sicherung von Bestellinformationen gegen grundlegende datenschutzrechtliche Anforderungen verstoßen können. Dass ein solcher Verstoß auch zu der Verhängung einer Geldbuße führen kann, zeigt der in Kap. 3.2 dargestellte Bericht.

13.8
Copy-Shop: Verantwortlicher oder Auftragsverarbeiter?

Ein Copy-Shop ist ein Dienstleistungsbetrieb, der sich auf das Verarbeiten von Dokumenten spezialisiert hat. Zum Tagesgeschäft eines solchen Betriebs gehören beispielsweise das Scannen, Drucken und Vervielfältigen diverser Arten von Schriftstücken. In aller Regel werden im Rahmen dieser Dienstleistungen auch personenbezogene Daten verarbeitet. Für die datenschutzrechtlichen Pflichten ist entscheidend, ob der Copy-Shop hierbei als Verantwortlicher oder als Auftragsverarbeiter im Sinne der DS-GVO tätig ist.

Hinweis auf unzulässige Datenverarbeitung

Im Rahmen eines Hinweises wurde mir folgender Sachverhalt zur Kenntnis gebracht: Die Kundin eines Copy-Shops bemerkte bei der Benutzung eines dort bereitgestellten PC-Systems, dass über das eingesetzte Betrachtungsprogramm für Dokumente Schriftstücke vorheriger Kunden aufgelistet wurden. Eine Vielzahl solcher Schriftstücke war über die Funktion „Zuletzt genutzte Dokumente“ auffindbar. Bei genauerer Betrachtung der Bezeichnungen dieser Schriftstücke erkannte die Kundin, dass es sich hierbei augenscheinlich u. a. um Mietverträge, Kündigungsschreiben und medizinische Dokumente handelte. Die Kundin vermutete, dass zuvor im Rahmen der Verarbeitung dieser Dokumente lokale Kopien angefertigt worden waren und diese nach Beendigung der Interaktion des vorherigen Kunden weiterhin im System verblieben waren. Die Kundin war der Überzeugung, dass eine endgültige Entfernung dieser Dokumente nur durch eine manuelle Löschung durch die Kunden des Copy-Shops in Verbindung mit der anschließenden Leerung des Papierkorbs erreicht werden könne. Sie vermutete hier einen Verstoß gegen datenschutzrechtliche Bestimmungen, denn dieser Sachverhalt sei ihr als Kundin nicht bewusst gewesen und die Mitarbeiter der Copy-Shops hätten es unterlassen, sie darüber in Kenntnis zu setzen.

Verantwortlicher oder Auftragsverarbeiter

Vor der weiteren Bearbeitung des Hinweises war zu klären, ob ein Copy-Shop im Rahmen seiner Diensterbringung datenschutzrechtlich als Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO oder als Auftragsverarbeiter gemäß Art. 4 Nr. 8 DS-GVO einzuordnen ist. Ein Copy-Shop in der Rolle des Verantwortlichen unterliegt anderen datenschutzrechtlichen Pflichten als in der Rolle des Auftragsverarbeiters. Als Auftragsverarbeiter würde der Copy-Shop personenbezogene Daten nur im Auftrag und nach Weisung eines Verantwortlichen verarbeiten. Als Verantwortlicher würde ein Copy-Shop hingegen über den Zweck und die Mittel der Verarbeitung entscheiden.

Um diese Fragestellung zu beantworten, betrachtete ich das folgende Szenario: Wenn die Kundin in einen Copy-Shop geht, um dort die gängigen Dienstleistungen in Anspruch zu nehmen (Erstellung von Kopien, Binden lassen von Kopien, Bedrucken von Tassen/T-Shirts) ist die Verarbeitung der personenbezogenen Daten, die auf diesen Dokumenten/Gegenständen ersichtlich sind, grundsätzlich „unvermeidliches Beiwerk“ bei der Ausführung der Dienstleistung. Möchte die Kundin etwa ein Zeugnis im Copy-Shop kopieren, geht es dem Copy-Shop in erster Linie darum, die Dienstleistung der Vervielfältigung dieses Zeugnisses für die Kundin anzubieten. Dem Copy-Shop geht es im Kern nicht darum, die darin enthaltenen personenbezogenen Daten zu

verarbeiten. Dass diese Daten dennoch durch den Copy-Shop im Rahmen des Vervielfältigungsprozesses oder im Rahmen der Kopieerstellung verarbeitet werden, erfolgt bei diesem Prozess nur zufällig (s. EDSA, Leitlinien 07/2020 zu den Begriffen ‚Verantwortlicher' und ‚Auftragsverarbeiter' in der DS-GVO, Rn. 73 ff.).

Gemäß Sinn des Art. 4 Nr. 8 DS-GVO i. V. m. Art. 28 Abs. 1 DS-GVO kann in den Fällen, in denen die Datenverarbeitung lediglich im Zusammenhang mit der Erbringung einer (Haupt-)Dienstleistung für einen anderen erfolgt, eine Auftragsverarbeitung abgelehnt werden. Gemäß Erwägungsgrund 81 DS-GVO muss der Verantwortliche den Auftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten „betrauen wollen". Dies kann im Einzelfall verneint werden, wenn die Datenverarbeitung nicht speziell beabsichtigt ist, beziehungsweise nicht den Schwerpunkt oder einen wichtigen (Kern-)Bestandteil der Leistung darstellt. Die Datenverarbeitung ist sodann als „unvermeidliches Beiwerk" bei der Erfüllung der eigentlichen Dienstleistungspflicht zu betrachten. Es kann somit festgehalten werden, dass ein Copy-Shop datenschutzrechtlich grundsätzlich als eigenständiger Verantwortlicher einzuordnen ist.

Rechtsgrundlage der Datenverarbeitung

Ein Copy-Shop braucht als Verantwortlicher aber eine Rechtsgrundlage, um diese personenbezogenen Daten, wenn auch nur als „Beiwerk", verarbeiten zu dürfen. Grundsätzlich wird sich ein Copy-Shop dabei auf Art. 6 Abs. 1 UAbs. 1 Buchst. a, b oder f DS-GVO stützen können. Art. 6 Abs. 1 UAbs. 1 Buchst. a DS-GVO ist dann einschlägig, wenn die betroffene Person in die Verarbeitung gemäß den Anforderungen nach Art. 7 DS-GVO eingewilligt hat. Darüber hinaus geht die betroffene Person bei Inanspruchnahme der Dienstleistungen des Copy-Shops einen Vertrag mit diesem ein, so dass die Verarbeitung ihrer personenbezogenen Daten grundsätzlich entsprechend Art. 6 Abs. 1 UAbs. 1 Buchst. b DS-GVO zur Erfüllung dieses Vertrags oder zur Erfüllung vorvertraglicher Maßnahmen erforderlich sein wird. Weiterhin wird der Copy-Shop grundsätzlich ein berechtigtes Interesse an der Zurverfügungstellung seiner Dienstleistungen (z. B. „Vervielfältigung/Kopie") haben und die Interessen der betroffenen Person werden diesem Interesse des Copy-Shops grundsätzlich nicht entgegenstehen. Zu beachten ist auch, dass es, wenn es um die Verarbeitung von Daten nach Art. 9 Abs. 1 DS-GVO geht (z. B. Taufurkunde, ärztliche Gutachten), die Anforderungen nach Art. 9 Abs. 2 DS-GVO durch den Copy-Shop zu berücksichtigen sind.

Verarbeitet ein Copy-Shop personenbezogene Daten der Kundin zur Abwicklung seiner Dienstleistung, z. B. im Rahmen einer Rechnungsstellung,

so ist unzweifelhaft auch in diesem Fall eine Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO gegeben. Denn in diesem Fall bestimmt der Copy-Shop selbst über den Zweck und die Mittel der Datenverarbeitung.

Ungeachtet dessen, ob die Verarbeitung personenbezogener Daten nun ein „unvermeidliches Beiwerk“ einer (Haupt-)Dienstleistung darstellt oder der Copy-Shop selbst über den Zweck und die Mittel der Datenverarbeitung entscheidet, ist er gemäß Art. 32 Abs. 1 DS-GVO verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und die verarbeiteten Daten vor einer Einsichtnahme durch unberechtigte Dritte zu schützen. Als Verantwortlicher muss er ferner auch den Grundsatz der Vertraulichkeit bei der Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 Buchst. f DS-GVO gemäß Art. 25 Abs. 1 und Art. 32 Abs. 1 DS-GVO durch technische und organisatorische Maßnahmen wirksam umsetzen.

Technischer Fehler?

Der Copy-Shop hat auf Rückfragen dargestellt, dass entsprechende Maßnahmen zum Schutz der verarbeiteten Daten implementiert seien. Er habe aber in der Vergangenheit bereits sporadisch festgestellt, dass Dokumente nach dem Kopieren noch aufgelistet waren. Als Grund hierfür habe man festgestellt, dass die Funktion „Zuletzt genutzte Dokumente“ zwar durch eine entsprechende Konfigurationsänderung regelmäßig deaktiviert sei, gelegentlich würde jedoch beim Einspielen von Updates für das Betrachtungsprogramm, die Funktion durch das Update wieder reaktiviert. In jedem Fall sei aber kein Zugriff auf die in dieser Funktion aufgelisteten Dokumente möglich; diese Dokumente seien nur auf den externen Datenträgern der Kunden gespeichert und würden nicht auf die eigenen PC-Systeme kopiert. Ein Zugriff auf diese Daten durch unberechtigte Dritte sei somit ausgeschlossen.

Der Copy-Shop sagte mir zu, meine Kontaktaufnahme zum Anlass zu nehmen, zukünftig die Prüfintervalle für die Deaktivierung der Funktion zu erhöhen und das Personal entsprechend zu schulen, damit etwaige Konfigurationsänderungen durch Softwareupdates am Betrachtungsprogramm zeitnah erkannt und, wenn nötig, behandelt werden.

Aus diesen Gründen konnte ich bei dieser Verarbeitungstätigkeit keinen Datenschutzverstoß feststellen und informierte die Hinweisgeberin abschließend über dieses Ergebnis.

14. Gesundheitsvorsorge

Gesundheitsdaten sind besonders schützenswert, weil sie intensiv das Persönlichkeitsrecht betreffen und ein hohes Diskriminierungspotenzial aufweisen. Für sie ist die informationelle Selbstbestimmung mit besonderer Sorgfalt zu wahren. Gesundheitsdaten sind aber auch von besonderer Bedeutung, um für die Gesundheit von Menschen vorzusorgen, sie zu erhalten oder wiederherzustellen. Es geht also bei Gesundheitsdaten immer um einen Ausgleich zwischen dem Ermöglichen hilfreicher Datenverarbeitung und dem Schutz vor ungewollter oder unzulässiger Datenverarbeitung. Für die mehrfache Nutzung von Gesundheitsdaten durch verschiedene Stellen kann eine Treuhandstelle von besonderer Bedeutung sein. Ich konnte den Aufbau einer solchen Treuhandstelle beratend unterstützen (Kap. 14.1). Auch beriet ich Ärzte, die aus einer Gemeinschaftspraxis ausscheiden wollten, wie sie dabei verfahren müssen, um die Patientenakten ausreichend zu schützen (Kap. 14.2). Das ungenehmigte Streaming von Ärzten und Patienten aus dem Gesundheitsbereich verstößt gegen Datenschutzrecht und ist eine strafbare Handlung (Kap. 14.3). Um das Patientengeheimnis zu wahren und die notwendige Vertraulichkeit sicherzustellen, sind im Anmeldebereich von Arztpraxen und Notaufnahmen geeignete bauliche und organisatorische Maßnahmen notwendig (Kap. 14.4). In Dialysegeräten, die nach der Nutzung an den Hersteller zurückgegeben und nach Überarbeitung wieder an neue Patienten ausgegeben werden, dürfen keine Daten der Patienten mehr gespeichert sein (Kap. 14.5).

14.1
Beratung beim Aufbau einer Treuhandstelle

Im Berichtszeitraum habe ich erstmals auch beim Aufbau einer Treuhandstelle beraten. Die Datentreuhandstelle sollte eine umfangreichere Datenverarbeitung und eine Verknüpfung von Daten im Forschungsbereich ermöglichen. Bei ihrem Aufbau war insbesondere die Verantwortlichkeit der Treuhandstelle im Hinblick auf ihre Unabhängigkeit zu klären. Auch die datenschutzrechtlichen Anforderungen, wie technische und organisatorische Maßnahmen, und die Prozesse zur Erfüllung der Betroffenenrechte sind von Beginn an zu betrachten.

Die Begriffe „Treuhandstelle“ und „Datentreuhänder“ sind nicht eindeutig gesetzlich definiert und werden mit unterschiedlicher Bedeutung verwendet. Treuhandstellen können sich anhand unterschiedlicher Aufgaben und Funktionen erheblich voneinander unterscheiden. Zu den Treuhändern kann man neben den Forschungsdatentreuhändern auch Personal Information

Management Systeme (PIMS) nach § 26 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) und Datenvermittlungsdienste nach Art. 2 Nr. 11 EU-Verordnung 2022/868 Data Governance Act (DGA) zählen.

Das Kompetenzzentrum für Telemedizin & E-Health (KTE) Hessen plante den Aufbau einer medizinischen Datentreuhandstelle (im Folgenden: MDTS). Es handelt sich hierbei um ein Pilotprojekt in Zusammenarbeit der Justus-Liebig-Universität Gießen (JLU) und der Technischen Hochschule Mittelhessen. Die MDTS soll zunächst verschiedene Aufgaben für das Datenintegrationszentrum der JLU wahrnehmen (Identitäts-, Pseudonym- und Einwilligungsmanagement), dabei aber keine medizinischen Daten verarbeiten. Sie soll hierbei auch als Treuhandstelle im Rahmen der Medizininformatik-Initiative handeln und die Einwilligungen der Patientinnen und Patienten (Broad Consent) zur Nutzung ihrer Daten zu Forschungszwecken verwalten.

Um die datenschutzrechtlichen Belange schon in der Planung angemessen zu berücksichtigen, hat mich das KTE Hessen um eine datenschutzrechtliche Beratung gebeten. Gerne habe ich den Aufbau der Treuhandstelle durch eine ausführliche Beratung unterstützt. Hierzu hat auch ein Gesprächstermin am KTE Hessen in Gießen stattgefunden.

Verantwortlichkeit

Zunächst musste geklärt werden, ob die MDTS als Auftragsverarbeiter der JLU oder als eigene Verantwortliche agiert.

Im Kontext einer Treuhandstelle ist eine Auftragsverarbeitung je nach konkreter Ausgestaltung grundsätzlich denkbar. Auftragsverarbeiter sind an Weisungen des Auftraggebers gebunden (Art. 28 Abs. 3 Satz 2 Buchst. a DS-GVO) und können daher nicht völlig unabhängig vom Auftraggeber sein. Gegen eine Auftragsverarbeitung im Sinne des Art. 28 DS-GVO spricht daher die erforderliche Unabhängigkeit einer Treuhandstelle. Eine Auftragsverarbeitung durch eine Treuhandstelle kommt daher nur in Betracht, wenn diese nicht unabhängig ist. Die Unabhängigkeit von Treuhandstellen hat rechtliche, finanzielle, personelle und räumliche Aspekte. Der Grad an Unabhängigkeit der Treuhandstelle sollte sich grundsätzlich nach deren Aufgabengebieten richten. Manche Aufgaben einer Treuhandstelle, wie das Identitätsmanagement, die Verwaltung von Einwilligungserklärungen und die Generierung von Pseudonymen könnten theoretisch auch im Rahmen einer weisungsgebundenen Auftragsverarbeitung erfüllt werden. Soll eine Treuhandstelle bewusst einen hohen Grad an Unabhängigkeit erhalten, steht dies jedoch im Widerspruch zu einer weisungsgebundenen Auftragsverarbeitung.

Maßgeblich ist letztlich, ob die Treuhandstelle über die Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DS-GVO) und daher datenschutzrechtlich Verantwortlicher ist. Eine Treuhandstelle kann auch trotz fehlender Rechtspersönlichkeit als Verantwortliche im Sinne der DS-GVO betrachtet werden. Eine eigene Rechtspersönlichkeit ist keine zwingende Voraussetzung für die Einordnung als Verantwortlicher (EuGH, Urteil vom 11. Januar 2024, Az. C-231/22, Rn. 36, Petri/Stief, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DS-GVO Art. 4 Nr. 7 Rn. 14). Wenn es sich bei einer Treuhandstelle jedoch nur um eine unselbstständige Abteilung einer Organisation handelt, spricht dies gegen eine eigene Verantwortlichkeit.

Eine Treuhandstelle, die selbst datenschutzrechtlich verantwortlich ist, bedarf einer eigenen Rechtsgrundlage für die Datenverarbeitungen. Hierfür kommen z. B. der Broad Consent nach dem Konzept der Medizin-Informatikinitiative oder eine projektspezifische Einwilligungserklärung mit einer Information über die Einbeziehung der Treuhandstelle in Betracht.

Technische und organisatorische Maßnahmen

Um eine datenschutzrechtskonforme Verarbeitung sicherzustellen, sind datenschutzrechtlich Verantwortliche gemäß Art. 24 Abs. 1 DS-GVO verpflichtet, technische und organisatorische Maßnahmen (TOM) zu ergreifen. Auch müssen sie nach Art. 25 Abs. 1 DS-GVO ihr System so gestalten, dass sie, insbesondere mit Hilfe ihrer TOMs, die Datenschutzgrundsätze des Art. 5 Abs. 1 DS-GVO umsetzen. Die Wirksamkeit der eingesetzten Maßnahmen hinsichtlich geeigneter TOMs müssen Verantwortliche gemäß Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO nachweisen. Schließlich müssen sie gemäß Art. 32 Abs. 1 DS-GVO mittels geeigneter TOMs die Sicherheit der Verarbeitung personenbezogener Daten gewährleisten. Als Werkzeug zur Festlegung der von der DS-GVO geforderten TOMs auf Basis eines risikobasierten Ansatzes habe ich dem MDTS das Standard-Datenschutzmodell (SDM) empfohlen.

Die Anwendung des SDM und allgemein die Umsetzung der datenschutzrechtlichen Anforderungen sollte insbesondere auch in enger wechselseitiger Abstimmung mit dem Bereich der IT-Sicherheit erfolgen. Dies gilt nicht zuletzt auch in Bezug auf die jeweils erforderlichen und ggf. voneinander abweichenden Risikobetrachtungen aus den beiden unterschiedlichen Perspektiven sowie hinsichtlich der TOMs. In jedem Fall sollte bei solchen Vorhaben sowohl Expertise aus dem Bereich des Datenschutzes als auch aus dem Bereich der IT-Sicherheit zur Umsetzung im Projekt hinzugezogen werden.

Operativer Datenschutz

Die MDTS habe ich auch auf die unterschiedlichen Prozesse des operativen Datenschutzes hingewiesen, etwa im Zusammenhang mit den Rechten der betroffenen Personen gemäß Kap. III DS-GVO wie dem Auskunftsrecht nach Art. 15 DS-GVO oder dem Widerruf einer Einwilligung.

Zur Gewährleistung der Betroffenenrechte müssen im Vorhinein Prozesse definiert und umgesetzt werden, damit entsprechende Anträge reibungslos bearbeitet werden können. Hier ist insbesondere zu klären, wer für die Bearbeitung dieser Anträge zuständig ist.

Da eine Aufgabe der MDTS auch die Verwaltung von Einwilligungen umfasst, müssen Widerrufe von betroffenen Personen nach Art. 7 Abs. 3 DS-GVO besonders betrachtet werden und Prozesse hierzu vorgesehen sein. In diesem Zusammenhang muss auch betrachtet werden, dass der Widerruf einer Einwilligung über alle Ebenen und auch im Rahmen der Backup-Strategie berücksichtigt wird.

Zusätzlich wurde auf erforderliche Prozesse zur Überprüfung und etwaigen Aktualisierung von Maßnahmen zur rechtskonformen Verarbeitung gemäß Art. 24 Abs. 1 DS-GVO sowie zur regelmäßigen Überprüfung, Bewertung und Evaluierung von Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gemäß Art. 32 Abs. 1 Buchst. d DS-GVO hingewiesen.

Fazit

Beim Aufbau einer Treuhandstelle ergaben sich einige besondere datenschutzrechtliche Fragestellungen, die im Dialog mit der KTE Hessen beantwortet werden konnten.

Den Aufbau von Treuhandstellen werde ich auch zukünftig gerne unterstützen, da diese ein wertvoller Baustein dafür sind, dass die Nutzung von Daten mit den Rechten der betroffenen Personen in Einklang gebracht wird. Auch eine Verknüpfung von Daten kann häufig erst durch den Einsatz einer Treuhandstelle auf eine sichere datenschutzrechtliche Grundlage gestellt werden. Gerade im Bereich der Forschung sollte dieses Instrument vermehrt eingesetzt werden.

14.2
Patientenakten beim Ausscheiden eines Arztes aus einer Gemeinschaftspraxis

In der Vergangenheit wurde bei mir schon häufiger angefragt, wie bestimmte Kooperationsformen im Gesundheitsbereich nach dem Ausscheiden eines Behandlers korrekt aufzulösen sind. So erhielt ich auch eine Anfrage zu Gemeinschaftspraxen, die nach dem Ausscheiden eines oder mehrerer Ärzte die Aufteilung der Patientendokumentation korrekt abwickeln wollten. Die ausscheidenden Ärzte hatten weiterhin Interesse an der Patientendokumentation, da sie eigene Arztpraxen gründen wollten. Ich habe für diese Fälle eine Handlungsempfehlung erarbeitet.

Grundsätze

In einer Gemeinschaftspraxis werden die Patientendokumentationen in der Regel gemeinschaftlich aufbewahrt. Eine Zuordnung der einzelnen Patientenakten zu einem konkreten Arzt ist nicht möglich, da die Ärzte die jeweiligen Patienten gemeinsam behandeln.

Aus dem Behandlungsvertrag nach § 630f Abs. 3 BGB ergibt sich grundsätzlich eine zehnjährige Aufbewahrungspflicht der Patientendokumentation. Diese Verpflichtung bleibt auch nach einer Praxisaufgabe bestehen. Zudem steht den Patienten innerhalb dieser Aufbewahrungsfrist ein Einsichtsrecht nach § 630g Abs. 1 BGB zu. Nach § 10 Abs. 4 Satz 1 der Berufsordnung für die Ärztinnen und Ärzte in Hessen (BO) haben Ärzte auch nach der Aufgabe der Praxis ihre ärztlichen Aufzeichnungen und Untersuchungsbefunde aufzubewahren oder dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden.

§ 630f BGB

(1) Der Behandelnde ist verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichen Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. (…)

(3) Der Behandelnde hat die Patientenakte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen.

§ 10 Abs. 4 BO

(4) Nach Aufgabe der Praxis haben Ärztinnen und Ärzte ihre ärztlichen Aufzeichnungen und Untersuchungsbefunde gemäß Absatz 3 aufzubewahren oder dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden. Ärztinnen und Ärzte, denen bei einer Praxisaufgabe oder Praxisübergabe ärztliche Aufzeichnungen über Patientinnen und Patienten in Obhut gegeben werden, müssen diese Aufzeichnungen unter Verschluss halten und dürfen sie nur mit Einwilligung der Patientin oder des Patienten einsehen oder weitergeben.

Lösungsmöglichkeiten und ihre Bewertung

Fraglich ist daher, wie mit der Patientendokumentation umgegangen werden sollte, so dass auch die austretenden Ärzte gegebenenfalls Zugriff auf diese haben könnten. Als Lösung kommen die Duplizierung der Akten und Verwahrung nach dem „Zwei-Schrank-Modell“ oder eine vertragliche Regelung in Betracht.

„Zwei-Schrank-Modell“

Aus einer Praxis kam der Vorschlag, die Patientenakten zu duplizieren. Die „gespiegelten“ Patientenakten sollten dabei von den ausgeschiedenen Ärzten in ihrer neuen Praxis lediglich ein bis zwei Jahre nach dem Zwei-Schrank-Model aufbewahrt und dann gelöscht werden, sofern sie nicht in das aktuelle Praxisverwaltungssystem überführt werden.

Das Zwei-Schrank-Modell ist datenschutzrechtlich anerkannt. Hierbei übergibt ein Arzt, der seine Praxis auflöst, die Patientendokumentation in die Obhut eines anderen Arztes. Der übernehmende Arzt verwahrt die übergebene Patientendokumentation unter Verschluss separat von seiner eigenen Dokumentation. Er darf sie nur mit Einwilligung des jeweiligen Patienten einsehen oder weitergeben. Er verpflichtet sich vertraglich, die Akten nur dann zu seiner eigenen Aktensammlung zu nehmen, wenn die jeweiligen Patienten ihr Einverständnis hierzu erteilen. Auch normiert § 10 Abs. 4 Satz 2 BO die Möglichkeit des Zwei-Schrank-Modells, so dass der aufbewahrende Arzt lediglich bei Einwilligung des Patienten die Patientendokumentation einsehen oder weitergeben darf.

Problematisch ist die Anwendbarkeit auf den vorliegenden Fall, da keine Praxis aufgelöst wird, sondern aus einer Gemeinschaftspraxis lediglich ein oder mehrere Ärzte austreten und eine eigene Praxis gründen. Die Patientendokumentation soll dabei nicht nur als Ganzes übergeben, sondern dupliziert werden. Aufgrund der vergleichbaren Interessenlage im Falle einer Praxisübernahme oder -auflösung liegt ein Rückgriff auf dieses Modell jedoch nahe.

Aufbewahrung in der neuen Praxis für einen kürzeren Zeitraum

Die Lösung der kürzeren Aufbewahrung der gespiegelten Dokumentation war aus meiner Sicht abzulehnen, da Sinn und Zweck des Zwei-Schrank-Modells auch gerade darin bestehen, dass die Patientendokumentation ordnungsgemäß aufbewahrt wird. Es gehört zur ärztlichen Nebenpflicht, die Akten grundsätzlich zehn Jahre lang aufzubewahren. Durch die Duplizierung wird eine Sorgfaltspflicht über die Patientenakten für die verlassenden Ärzte begründet. Sie sind zu einem rechtmäßigen Umgang verpflichtet. Zu diesem gehört es auch, die gesetzlich geregelte Aufbewahrungsfrist zu wahren.

Die Duplizierung der Akten verstößt meiner Auffassung nach zudem gegen den Grundsatz der Datenminimierung aus Art. 5 Abs. 1 Buchst. c DS-GVO. Hiernach müssen personenbezogene Daten dem Zweck angemessen und auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Die ausscheidenden Ärzte haben jedoch grundsätzlich nur Anspruch auf diejenigen Akten von Patienten, die dem verlassenden Arzt aus der Gemeinschaftspraxis in die neue Praxis folgen (Datenschutz in der Arzt-/Psychotherapeutenpraxis, Hinweise und Antworten der Kassenärztlichen Vereinigung Bayerns zum Umgang mit Patientendaten im Praxisalltag, 2015, S. 32).

Duplizierung von Stammdaten

Der vorzugswürdige Lösungsansatz ist aus meiner Sicht, lediglich die „Stammdaten“ (Name, Anschrift, Telefonnummer) von Patienten zu duplizieren. Hierbei habe ich mich der Auffassung des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) angeschlossen (Auflösung einer Gemeinschaftspraxis – Wie ist mit den Patientendaten zu verfahren?, 2021, https://www.datenschutzzentrum.de/artikel/38-Aufloesung-einer-Gemeinschaftspraxis-Wie-ist-mit-den-Patientendaten-zu-verfahren.html). So kann sichergestellt werden, dass die Patienten zumindest kontaktiert und leichter zugeordnet werden können, wenn sie in die neue Praxis kommen.

Die Aufbewahrung dieser Stammdaten nach dem Zwei-Schrank-Modell ist nur innerhalb einer bestimmten Übergangsphase zulässig. Diese sollte vertraglich geregelt werden und könnte zum Beispiel ein bis zwei Jahre betragen. Nach Ablauf dieser Übergangsphase sind die Stammdaten der nicht gewechselten Patienten zu löschen.

Zu beachten bei dieser Lösung ist die Pflicht nach Art. 13 DS-GVO, die Patienten darüber zu informieren. Dies könnte über die Internetseite der bisherigen Gemeinschaftspraxis und/oder über ein schriftliches Dokument bekannt gegeben werden.

Anspruch auf Herausgabe der Dokumentation

Um bei Bedarf den Zugriff der verlassenden Ärzte auf die Patientenakten sicherzustellen, kann zwischen der Gemeinschaftspraxis und den verlassenden Ärzten ein entsprechender Vertrag geschlossen werden. In diesem Vertrag könnten die Parteien die Zusicherung der Gemeinschaftspraxis regeln, bei Anforderung die Patientenakten unverzüglich an die verlassenden Ärzte herauszugeben.

Handlungsempfehlung

Bei der Auflösung einer Gemeinschaftspraxis erscheint die Anwendung des Zwei-Schrank-Modells im Hinblick auf den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchst. c DS-GVO aus datenschutzrechtlicher Sicht problematisch, da die Patientendokumentation dupliziert wird. Zum anderen erscheint die frühzeitige Löschung der duplizierten Daten nicht unzweifelhaft möglich, da aufgrund der Duplikation eine Sorgfaltspflicht über den rechtmäßigen Umgang begründet wird, zu dem auch die fristgemäße Aufbewahrung von zehn Jahren nach Abschluss der Behandlung gehört.

Bei der Auflösung einer Gemeinschaftspraxis empfiehlt sich der Ansatz, nur die Stammdaten der Patienten zu duplizieren. Hierdurch kann eine Zuordnung der gewechselten Patienten erleichtert werden. Nach Ablauf einer vereinbarten Übergangszeit müssen die nicht in das Praxisverwaltungssystem überführten Stammdaten gelöscht werden.

14.3
Streaming im Gesundheitsbereich

Immer wieder werde ich mit Fällen konfrontiert, in denen Mitarbeiter von Gesundheitseinrichtungen live von ihrem Arbeitsplatz aus Videos streamen, was mit der Gefahr einhergeht, dabei auch sensible Patientendaten zu veröffentlichen.

Streaming-Vorfälle

Solche Streaming-Vorfälle spielten sich nahezu in allen Kategorien von Gesundheitseinrichtungen ab, betroffen waren u. a. Pflegeeinrichtungen, Krankenhäuser, Arztpraxen und Apotheken. Die Aufnahmen erfolgten am Arbeitsplatz, wozu neben Patientenzimmern, Behandlungsräumen oder Wartebereichen auch sonstige Aufenthaltsräume zählen. Dabei kam es gelegentlich dazu, dass auch sensible Daten der Patienten mit gestreamt wurden.

Datenschutzrechtliche Bewertung

Gesundheitsdaten sind gemäß Art. 9 DS-GVO eine besondere Kategorie personenbezogener Daten, die eines besonderen Schutzes bedürfen. Jegliche Verarbeitung (inklusive Aufnehmen und Streamen) ist grundsätzlich verboten. Ausnahmen erfordern eine gesetzliche Grundlage oder die informierte, freiwillige Einwilligung der abgebildeten Personen. Eine solche Einwilligung ist im Gesundheitsbereich, insbesondere bei unbeteiligten Dritten im Hintergrund, kaum praktikabel oder rechtssicher einzuholen.

Kommt es zu einer Verletzung des Schutzes personenbezogener Daten durch unerlaubtes Streamen von personenbezogenen Daten, ist gemäß Art. 33 Abs. 1 Satz 1 DS-GVO die verantwortliche Stelle verpflichtet, unverzüglich und möglichst binnen 72 Stunden, nachdem ihr die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde zu melden. Je nach Risiko einer Rechtsverletzung müssen nach Art. 34 DS-GVO auch die Betroffenen informiert werden.

Die Aufsichtsbehörde hat nach Art. 58 Abs. 2 DS-GVO mehrere Instrumente, um auf Datenschutzverstöße im Einzelfall angemessen reagieren zu können. Dabei kommt es für die Beurteilung des Gewichts des Verstoßes auch darauf an, inwieweit der Verantwortliche selbst ausreichende Maßnahmen getroffen hat, um Fehlverhalten der beschriebenen Art durch die beschäftigten Personen zu verhindern. Zu beurteilen ist etwa, welche Vorgaben er den Beschäftigten hierzu macht, in welcher Weise und wie effektiv er die Beschäftigten über ihre Pflichten unterrichtet, wie er die Einhaltung der Vorgaben ansonsten überprüft und wie er auf etwaige Vorfälle in der Vergangenheit reagiert hat.

Der Verantwortliche muss nach 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 geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (…)“.

Mitarbeiterexzess

Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO ist in der Regel die Gesundheitseinrichtung selbst. Im Falle eines sogenannten „Mitarbeiterexzesses“ kann aber auch die beschäftigte Person als Verantwortlicher angesehen werden; die beschäftigte Person wird insoweit selbst zum Verantwortlichen. Ein solcher Mitarbeiterexzess liegt vor, wenn eine beschäftigte Person zu nicht-dienstlichen Zwecken eine rechtswidrige Verarbeitung von personenbe-

zogenen Daten vornimmt, zu denen sie kraft ihres Beschäftigtenverhältnisses die Möglichkeit des Zugangs hat. Die beschäftigte Person hält sich also in diesem Fall nicht an die intern festgelegten Regelungen und Verfahren des Verantwortlichen und verarbeitet auf eigene Initiative personenbezogene Daten.

Bei der Veröffentlichung von Gesundheitsdaten in sozialen Medien im Wege des Mitarbeiterexzesses ist regelmäßig eine Geldbuße in Betracht zu ziehen. Hierbei sind neben den Auswirkungen, die die Handlung für die betroffenen Personen hatte oder haben könnte, auch die Motive der handelnden Person und die Maßnahmen und Sanktionen, die die verantwortliche Stelle bereits gegenüber der handelnden Person vorgenommen hat, zu berücksichtigen.

Zusätzlich zu den datenschutzrechtlichen Aspekten ergeben sich noch die nachfolgenden, weiteren Problemfelder.

Recht am eigenen Bild

Das Filmen anderer Personen ist grundsätzlich nur mit der Einwilligung des Abgebildeten erlaubt. Jeder Mensch darf selbst darüber bestimmen, ob und wo von ihm Aufnahmen wie Fotos oder Videos gemacht und veröffentlicht werden dürfen. Dieses sogenannte Recht am eigenen Bild ergibt sich aus den vom Grundgesetz garantierten Persönlichkeitsrechten und wird durch §§ 22-24 KUG konkretisiert.

Betroffene haben zahlreiche Rechte, um sich gegen ein unerlaubt veröffentlichtes Foto oder Videoaufnahme im Internet zu wehren. Neben einem Anspruch auf Löschung der unerlaubt veröffentlichten Aufnahme nach § 37 KUG und einem Herausgabeanspruch nach § 38 KUG können sie Unterlassungsansprüche gegen den Verantwortlichen sowie Schadenersatz geltend machen. Bei einer schwerwiegenden Persönlichkeitsrechtsverletzung können sie neben dem Anspruch auf Schadensersatz auch eine Geldentschädigung für immaterielle Schäden in Form eines Schmerzensgeldes fordern.

Strafrechtliche Konsequenzen

Die Verletzung der ärztlichen Schweigepflicht ist eine Straftat gemäß § 203 StGB, der die „Verletzung von Privatgeheimnissen“ unter Strafe stellt. Eine Verletzung kann erhebliche Konsequenzen sowohl für die handelnde Person als auch für die Einrichtung nach sich ziehen. Diese Folgen reichen von strafrechtlichen Sanktionen über berufsrechtliche Maßnahmen bis hin zu zivilrechtlichen Schadensersatzforderungen – etwa nach Art. 82 DS-GVO.

Wird durch den Stream außerdem unbefugt ein anderes zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsge-

heimnis offenbart, können gemäß § 203 StGB Freiheitsstrafen bis zu einem Jahr oder Geldstrafen drohen. Da man diese nach § 203 StGB anvertrauten Geheimnisse für seinen Stream und somit seinen persönlichen Nutzen missbraucht, ist auch eine Strafbarkeit gemäß § 204 StGB (Verwertung fremder Geheimnisse) denkbar.

Bei der Aufnahme von vertraulichen Patientengesprächen kann überdies gemäß § 201 StGB die „Vertraulichkeit des Wortes" verletzt sein. Es drohen Strafen mit bis zu drei Jahren Haft oder Geldstrafe. Durch die Filmaufnahmen kommt auch gemäß § 201a StGB eine Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen in Betracht. Werden in diesem Zusammenhang absichtlich oder wissentlich Genitalien, das Gesäß, die weibliche Brust oder diese Körperteile bedeckende Unterwäsche gefilmt, liegt außerdem eine Verletzung des Intimbereichs durch Bildaufnahmen gemäß § 184k StGB vor.

Die betroffene Person kann schließlich eine Strafanzeige wegen einer unerlaubten Veröffentlichung der Aufnahme stellen. Auch hierfür drohen dem Täter gemäß § 33 KUG strafrechtliche Konsequenzen.

Verantwortung der Verantwortlichen

Die Entwicklung in den letzten Jahren unterstreicht die Dringlichkeit, das Bewusstsein für Datenschutzrisiken in medizinischen Einrichtungen zu schärfen. Gesundheitseinrichtungen sollten daher klare Social Media Guidelines und Hausordnungen implementieren sowie Mitarbeitende und Besucher aktiv über die strikten Regeln bezüglich Film- und Fotoaufnahmen informieren, um solche Vorfälle zu verhindern. Die Nutzung privater Smartphones oder Kameras in sensiblen Bereichen (OP, Patientenzimmer) muss klar geregelt oder vollständig untersagt werden, um das Risiko unbefugter Aufnahmen zu minimieren. Regelmäßige Schulungen zum Datenschutz und zur ärztlichen Schweigepflicht sind für das Personal unerlässlich. Der Datenschutzbeauftragte des Krankenhauses muss in die Erstellung der Richtlinien und die Überwachung der Einhaltung eingebunden sein.

Auch Kammern und Verbände sollten ihre Mitglieder weiter zu dem Thema sensibilisieren, so wie dies jüngst die Hessische Krankenhausgesellschaft mit einem internen Papier getan hat.

14.4
Vertraulichkeit im Anmeldebereich einer Notaufnahme

Gerade im medizinischen Bereich ist es besonders wichtig, dass Gesundheitsdaten nur mit ausreichender Diskretion erhoben werden. Die Vertraulichkeit der von den Patientinnen und Patienten preisgegebenen personenbezogenen Daten muss daher sichergestellt werden. Hierzu kann es auch nötig sein, dass die jeweilige Gesundheitseinrichtung bauliche Maßnahmen treffen muss, um einen datenschutzkonformen Zustand herbeizuführen.

Bauliche Situation

In einer Beschwerde wurde ich darauf hingewiesen, dass es datenschutzrechtliche Probleme bei der Aufnahme einer Zentralen Notaufnahme eines Krankenhauses in Hessen gebe. Die Anmeldung der Zentralen Notaufnahme befinde sich in einem hellhörigen Warteraum. Die von den Patientinnen und Patienten bei der Aufnahme gemachten Angaben könnten von den wartenden Personen dadurch deutlich mitgehört werden. Dies gelte auch für die Antworten der Patientinnen und Patienten zu Rückfragen des Aufnahmepersonals. Ein kleiner Raumteiler, der am Anmeldeschalter aufgestellt worden sei, sei mangels ausreichenden Schallschutzes nicht ausreichend, um das Problem zu beheben.

Datenschutzrechtliche Anforderungen

Im Aufnahmeprozess in der Zentralen Notaufnahme erhebt das Krankenhaus von den Patientinnen und Patienten besonders sensible Gesundheitsdaten.

Nach Art. 5 Abs. 1 Buchst. f DS-GVO ist das Krankenhaus gesetzlich dazu verpflichtet, personenbezogene Daten in einer Weise zu verarbeiten, die eine angemessene Sicherheit dieser personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung („Integrität und Vertraulichkeit“). Das Krankenhaus muss nach Art. 32 Abs. 1 DS-GVO geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Bei einer unzureichenden baulichen Gestaltung der Notaufnahme droht im Aufnahmeprozess die Offenbarung von sensiblen Gesundheitsdaten gegenüber unbefugten Dritten. Es ist aufgrund der besonderen Schutzbedürftigkeit von Gesundheitsdaten in dieser Situation von einem hohen Risiko für die betroffenen Personen auszugehen. Das Krankenhaus muss als Verantwortlicher für eine Umgebung sorgen, in der dieses Risiko durch angemessene Maßnahmen auf ein vertretbares Maß reduziert wird. In der

Aufnahme der zentralen Notaufnahme fehlten aber entsprechende wirksame Schutzmaßnahmen.

Verbesserung der Zentralen Aufnahme

Ich habe das Krankenhaus auf die Rechtslage und meine Bewertung hingewiesen. Das Krankenhaus hat sich kooperativ gezeigt und sich dafür entschieden, eine Schallschutzkabine in der Zentralen Notaufnahme einzubauen. Hierdurch konnte sichergestellt werden, dass im Aufnahmeprozess ein angemessenes Schutzniveau vorliegt und die Diskretion und die Vertraulichkeit gewahrt werden.

In meinem 50. Tätigkeitsbericht 2021 (Kap. 17.3) habe ich bereits in einem Beitrag dargestellt, wie in einem vergleichbaren Fall durch eine räumliche Trennung von Wartezimmer und Empfangsbereich die Diskretion in einer Arztpraxis hergestellt werden konnte. Viele medizinische Einrichtungen in Hessen haben bereits wirksame Maßnahmen getroffen, um den Schutz personenbezogener Daten bei der Erhebung von Daten der Patientinnen und Patienten sicherzustellen, z. B. durch Aufnahmegespräche in abgetrennten Kabinen. Ich gehe davon aus, dass sich dieses Vorgehen überall durchsetzt und viele Nachahmer findet.

14.5
Datenspeicherung in Dialysegeräten

Auch für Medizinprodukte, wie beispielsweise Dialysegeräte, gelten die allgemeinen datenschutzrechtlichen Anforderungen. Die Verantwortlichen müssen sich einen Überblick darüber verschaffen, welche Datenverarbeitungen erfolgen, und sicherstellen, dass hierbei alle datenschutzrechtlichen Anforderungen erfüllt werden. Dies schließt insbesondere die Erfüllung der Informationspflichten, die Verschlüsselung und die Löschung personenbezogener Daten mit ein. Bevor ein Medizinprodukt wieder an den Hersteller zurückgeschickt wird, müssen die Verantwortlichen auch sorgfältig prüfen, ob sich noch personenbezogene Daten auf dem Gerät befinden.

Datenverarbeitung im Dialysegerät

Aufgrund einer Beschwerde habe ich die Datenspeicherung auf den Dialysegeräten eines Herstellers aus Hessen untersucht. Nach den Angaben in der Beschwerde seien die auf den Dialysegeräten gespeicherten personenbezogenen Daten nicht verschlüsselt und es gebe keine Möglichkeit, die Daten vor der Rücksendung an den Hersteller zu löschen. Dadurch erhielten sowohl der Hersteller als auch andere Patientinnen und Patienten – da die Geräte

nach einer Wartung ggf. wieder ausgegeben würden – Zugriff auf sensible personenbezogene Daten zu den Behandlungen. Außerdem informiere der Hersteller die Nutzerinnen und Nutzer der Dialysegeräte nicht ausreichend über diese Datenspeicherung.

Der Hersteller der Dialysegeräte hat mir die Funktionsweise und den Prozess bei der Rückgabe von Dialysegeräten erläutert. Die entsprechenden Dialysegeräte werden sowohl in Krankenhäusern und Arztpraxen als auch bei den Patientinnen und Patienten zuhause eingesetzt. Nach Ablauf der Nutzungsdauer oder im Falle eines Defekts werden die Dialysegeräte an den Hersteller zurückgeschickt. Die Dialysegeräte verfügen über einen internen Speicher mit technischen Logfiles und Behandlungsdatensätzen, die jeweils personenbezogene Gesundheitsdaten der Patientinnen und Patienten enthalten. Eine Auswertung der Daten von den Dialysegeräten erfolge durch den Hersteller zu Zwecken der Qualitätssicherung und zur Erfüllung gesetzlicher Anforderungen für Medizinprodukte.

Verantwortlichkeit und Rechtsgrundlagen

Datenschutzrechtlich ist zunächst im Hinblick auf die Verantwortlichkeit wie folgt zu differenzieren: Im Rahmen der Wartung von Dialysegeräten ist der Hersteller hier gemäß Art. 28 DS-GVO Auftragsverarbeiter der jeweiligen medizinischen Einrichtung, die für die Patientendaten verantwortlich ist. Für die Aufklärung möglicher Vorfälle in Zusammenhang mit der Nutzung der Dialysegeräte ist er hingegen datenschutzrechtlich Verantwortlicher, da er die Mittel und Zwecke hierfür selbst bestimmt und, aufgrund ihn betreffender gesetzlicher Pflichten, auch bestimmen muss.

Er kann sich für die Verarbeitung der auf den Dialysegeräten gespeicherten Daten auf Art. 6 Abs. 1 UAbs. 1 Buchst. c und f, Art. 9 Abs. 2 Buchst. i DS-GVO sowie § 22 Abs. 1 Nr. 1 Buchst. c BDSG in Verbindung mit Art. 83 und 88 EU-Verordnung 2017/745 (Medical Device Regulation – MDR) berufen (s. DSK, Positionspapier digitale Gesundheitsanwendungen vom 6. November 2023, S. 4, https://www.datenschutzkonferenz-online.de/media/dskb/2023_11_06_Beschluss_cloudbasierte_digitale_Gesundheitsanwendungen.pdf).

Als Rechtsgrundlage käme hier gegebenenfalls auch Art. 9 Abs. 2 Buchst. f DS-GVO in Betracht. Danach ist eine Verarbeitung von Gesundheitsdaten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen zulässig. Im vorliegenden Kontext könnte diese Norm aber nur dann das Vorhalten der Logfiles legitimieren, wenn bereits ein konkreter Rechtsstreit absehbar wäre. Sie könnte jedoch nicht bei der abstrakten Möglichkeit eines Rechtsstreits eine weitere Aufbewahrung „auf Vorrat“ legitimieren (s. zu

Art. 17 Abs. 3 Buchst. e DS-GVO Simitis/Hornung/Spiecker gen. Döhmann/Dix, Datenschutzrecht, DSGVO Art. 17 Rn. 38 und Kühling/Buchner/Herbst, 4. Aufl. 2024, DS-GVO Art. 17 Rn. 83).

Informationspflichten

Der Hersteller hat als Verantwortlicher für die Aufklärung möglicher Vorfälle die betroffenen Personen nach Art. 14 DS-GVO zu informieren.

Nach Art. 28 Abs. 3 Satz 2 Buchst. f DS-GVO ist er als Auftragsverarbeiter außerdem dazu verpflichtet, unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen die Verantwortlichen (hier Krankenhäuser und Arztpraxen) bei der Einhaltung der in den Art. 32 bis 36 DS-GVO genannten Pflichten zu unterstützen.

Aus diesen Normen kann daher bei einem entsprechenden „Wissensgefälle" eine Pflicht des Herstellers hergeleitet werden, die Verantwortlichen über die Datenspeicherungen zu informieren.

Verschlüsselung

Nach Art. 32 Abs. 1 DS-GVO trifft der Auftragsverarbeiter unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Hierzu gehört gemäß Art. 32 Abs. 1 Buchst. a DS-GVO eine Verschlüsselung personenbezogener Daten. Der Hersteller ist hierzu auch in seiner Rolle als Auftragsverarbeiter verpflichtet, denn Art. 32 Abs. 1 DS-GVO ist gemäß Art. 28 Abs. 3 Satz 2 Buchst. c DS-GVO ausdrücklich auch auf Auftragsverarbeiter anwendbar.

Löschung

Nach den Grundsätzen der Datenminimierung gemäß Art. 5 Abs. 1 Buchst. c DS-GVO und der Speicherbegrenzung nach Art. 5 Abs. 1 Buchst. e DS-GVO in Verbindung mit dem Recht auf Löschung gemäß Art. 17 DS-GVO sind personenbezogene Daten grundsätzlich zu löschen, wenn die weitere Aufbewahrung nicht mehr erforderlich ist. Daher ist auch bei der Speicherung von personenbezogenen Daten auf Medizinprodukten eine Löschmöglichkeit vorzusehen.

Ergebnis meiner Überprüfung

Vor dem Hintergrund der genannten gesetzlichen Pflichten des Auftragsverarbeiters und Verantwortlichen und dessen Einlassungen zu den Verarbeitungstätigkeiten im Zusammenhang mit den Dialysegeräten in ihrer bisherigen Form bin ich zu dem Ergebnis gekommen, dass dabei noch kein angemessenes Datenschutzniveau gewährleistet war. Die lückenhafte Informationsbereitstellung in Verbindung mit noch nicht ausreichenden Möglichkeiten zur Löschung personenbezogener Daten durch die betroffenen Personen hatte zur Folge, dass diese ihre Betroffenenrechte nicht wirksam und in informierter Weise durchsetzen konnten. Eine zu schwach ausgeprägte Zugangs- und Zugriffssicherung bezogen auf die auf den Geräten gespeicherten Daten begünstigte außerdem unbefugte Zugriffe.

Umgesetzte Verbesserungen

Nach der Klärung des komplexen Sachverhalts und der datenschutzrechtlichen Einordnung habe ich den Hersteller auf die oben genannten Anforderungen und meine dahingehende Bewertung hingewiesen. Er hat diese Kritik aufgegriffen und umfassende Änderungen am Rückgabeprozess und der Gerätesoftware vorgenommen. So hat er bei der Speicherung von Daten auf den Geräten klarer zwischen den verschiedenen Zwecken getrennt. Die technischen Logfiles dienen nun ausschließlich der Qualitätssicherung und Erfüllung der MDR. Sie werden für die jeweils zurückliegenden vier Monate auf dem Gerät gespeichert. Die Logfiles werden nun, mit einem dem aktuellen Stand der Technik entsprechenden Verfahren, verschlüsselt. Mit einem auf dem Gerät angebrachten Sicherheitssiegel soll außerdem ein unberechtigtes Öffnen des Geräts erkannt werden können.

Die Behandlungsdatensätze können von den Patientinnen und Patienten für einen Zeitraum bis zu einem Jahr eigenständig gespeichert werden und dienen der Behandlungshistorie und der Benutzerfreundlichkeit. Sie werden mit einem von der Patientin oder dem Patienten selbst gewählten Passwort verschlüsselt. Außerdem können die Patientinnen und Patienten durch eine neue Funktion selbstständig die Behandlungsdatensätze löschen, z. B. vor der Rücksendung des Geräts. Daneben können die internen Speichermedien auch vor Rücksendung der Geräte von den lokalen Technikern der Gesundheitseinrichtung entnommen werden.

Zur Erfüllung der Informationspflichten als Verantwortlicher stellt der Hersteller auf seiner Website eine entsprechende Datenschutzerklärung bereit, auf die auch die jeweiligen Krankenhäuser und Arztpraxen hinweisen.

Zudem hat er eine Handreichung erstellt, in der die Nutzerinnen und Nutzer des Dialysegeräts auf den Schutz personenbezogener Daten und den richtigen Umgang bei der Rücksendung von Geräten hingewiesen werden.

Fazit

Durch diese Maßnahmen konnte ein zufriedenstellendes Datenschutzniveau der Dialysegeräte hergestellt werden. Die Kooperation des Herstellers mit meiner Behörde ermöglichte es, diese Verbesserungen auch ohne förmliche Maßnahmen gegen ihn zu erreichen.

Im Bereich der Medizinprodukte sind viele gesetzliche Vorgaben von den Herstellern zu berücksichtigen, insbesondere im Hinblick auf die Sicherheit der Produkte. Die Hersteller von Medizinprodukten sollten aber auch bereits in der Entwicklungsphase datenschutzrechtliche Belange ausreichend berücksichtigen, damit aufwendige Nachbesserungen nach dem Inverkehrbringen vermieden werden.

15. Wissenschaft und Forschung

Forschung, die auf datenschutzkonforme Weise neue Erkenntnisse gewinnt, ist mir ein besonderes Anliegen. Daher habe ich mich auch in diesem Berichtsjahr intensiv mit dem Datenschutz im Forschungsbereich beschäftigt. Durch von mir (mit-)initiierte Abstimmungen in Gremien der Datenschutzaufsichtsbehörden konnten einige wichtige Festlegungen getroffen werden, die mehr Rechtssicherheit für die Forschenden bringen und ihnen Unterstützung bei der Erfüllung ihrer datenschutzrechtlichen Pflichten bieten. Dies wird ermöglicht durch Anwendungshinweise der DSK zum Drittstaatentransfer in der medizinischen Forschung (Kap. 15.1), durch Erleichterungen für die gemeinsame Verarbeitung von Gesundheitsdaten durch Forschungseinrichtungen (Kap. 15.2) und durch den datenschutzgerechten Zugang zu Daten sehr großer Online-Plattformen und Suchmaschinen (Kap. 15.3). Zusammen mit der Deutschen Gesellschaft für Innere Medizin (DGMI) habe ich einen Leitfaden für Datenschutz in der medizinischen Forschung erarbeitet, der für medizinische Forschungsprojekte mehr Rechtssicherheit gewährleisten kann (Kap. 15.4).

15.1 Anwendungshinweise zum Drittstaatentransfer in der medizinischen Forschung

Die Taskforce Forschungsdaten der DSK hat zusammen mit dem DSK-Arbeitskreis Internationaler Datenverkehr einen Dialog mit der Technologie- und Methodenplattform für die vernetzte medizinische Forschung e. V. (TMF) zu einem neuen Modul der bereits mit der DSK abgestimmten Broad Consent-Mustereinwilligungserklärung geführt. Dieses Modul behandelt die Übermittlung von personenbezogenen Gesundheitsdaten an Drittstaaten zu Zwecken der medizinischen Forschung.

Aufbauend auf den Erkenntnissen aus diesem Stakeholder-Dialog haben die beiden Gremien der DSK eine Veröffentlichung erstellt, die über den Anwendungsfall des Broad Consent hinaus wichtige Informationen zum Drittstaatentransfer in der medizinischen Forschung gibt.

Diese „Anwendungshinweise zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken“ (https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen.pdf) erläutern zunächst die zweistufige Prüfung bei solchen Datenübermittlungen und stellen dann dar, welche Übermittlungsinstrumente nach dem Kapitel V der DS-GVO hier in Betracht kommen. Dazu zählen neben einem Angemessenheitsbeschluss

nach Art. 45 DS-GVO und geeigneten Garantien nach Art. 46 Abs. 2 DS-GVO auch die Ausnahmebestimmungen für bestimmte Fälle nach Art. 49 DS-GVO.

Zur informierten Einwilligung nach Art. 49 Abs. 1 Buchst. a DS-GVO ist besonders hervorzuheben, dass die betroffenen Personen über das konkrete Drittland und über die spezifischen Risiken aus der Übermittlung informiert werden müssen.

Um den Verantwortlichen eine Unterstützung bereitzustellen, hat die DSK in einer Anlage zu den Anwendungshinweisen konkrete Empfehlungen für die Erfüllung der Informationspflichten bei solchen Datenübermittlungen gegeben (https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen_Anlage.pdf).

15.2
Antragsformular für die gemeinsame Verarbeitung von Gesundheitsdaten

Das im März 2024 in Kraft getretene Gesundheitsdatennutzungsgesetz (GDNG) enthält in § 6 Abs. 3 Satz 4 eine neue datenschutzrechtliche Rechtsgrundlage für die gemeinsame Verarbeitung von Gesundheitsdaten durch „öffentlich geförderte Zusammenschlüsse von datenverarbeitenden Gesundheitseinrichtungen“.

Diese Regelung ist nur für bestimmte gesetzlich genannte Zwecke anwendbar. Hierzu gehören insbesondere die Qualitätssicherung und die medizinische Forschung. Die gemeinsame Datenverarbeitung darf auch nur dann erfolgen, wenn eine Abwägung zwischen den Interessen des Verantwortlichen und den Interessen der betroffenen Personen zu dem Ergebnis kommt, dass die Interessen des Verantwortlichen erheblich überwiegen.

Außerdem muss nach § 6 Abs. 3 Satz 4 Nr. 4 GDNG die zuständige Datenschutzaufsichtsbehörde der gemeinsamen Nutzung und Verarbeitung zugestimmt haben. Um diesen neuen behördlichen Zustimmungsprozess effektiv zu gestalten, habe ich zusammen mit den anderen Datenschutzaufsichtsbehörden in der Taskforce Forschungsdaten ein einheitliches Antragsformular entwickelt (https://datenschutz.hessen.de/service/antrag-auf-zustimmung-nach-ss-6-abs-3-s-4-nr-4-gdng).

Mit diesem Antragsformular erhalten die Forschenden einen Überblick darüber, welche Informationen und Dokumente für die Prüfung der Zustimmung benötigt werden. Es kann zeitraubende Rückfragen im Zustimmungsverfahren vermeiden und so das Verfahren beschleunigen.

Das Formular soll deutschlandweit eingesetzt werden, so dass auch bei länderübergreifenden Forschungsprojekten einheitliche Antragsunterlagen verwendet werden können.

Außerdem hat die Taskforce Forschungsdaten der DSK in diesem Zusammenhang auch einen einheitlichen Musterbescheid für die Zustimmung nach § 6 Abs. 3 Satz 4 Nr. 4 GDNG abgestimmt.

15.3
Zugang zu Daten sehr großer Online-Plattformen und Suchmaschinen

Eine weitere neue Rechtsgrundlage für die Forschung mit personenbezogenen Daten hat der EU-Gesetzgeber mit Art. 40 des Digital Services Act (EU VO 2022/2065 – DSA) geschaffen. Danach sind sehr große Online-Plattformen und Suchmaschinen wie Meta (Facebook und Instagram), Google (YouTube und Search) sowie Tiktok und X nun dazu verpflichtet, Nutzerdaten für bestimmte Forschungsvorhaben zur Verfügung zu stellen.

Berechtigt sind nur Forschungsvorhaben, die zur Aufspürung, zur Ermittlung und zum Verständnis systemischer Risiken solcher großen Online-Plattformen und Suchmaschinen in der EU beitragen. Hierzu gehören etwa die Verbreitung rechtswidriger Inhalte, nachteilige Auswirkungen auf die Ausübung von Grundrechten wie die Menschenwürde, der Schutz personenbezogener Daten, die Meinungs- und Informationsfreiheit sowie nachteilige Auswirkungen auf Wahlprozesse und die öffentliche Sicherheit.

Die Forschenden müssen für den Datenzugang einen Antrag bei dem Koordinator für digitale Dienste des zuständigen Mitgliedstaats stellen. In Deutschland ist die Koordinierungsstelle für digitale Dienste (DSC) der Bundesnetzagentur zuständig. Diese trifft nach § 19 Abs. 1 Digitale-Dienste-Gesetz Entscheidungen im Hinblick auf die DS-GVO im Benehmen mit der zuständigen Datenschutzaufsichtsbehörde.

Bei der Beantragung des Datenzugangs muss auch die Erfüllung der datenschutzrechtlichen Anforderungen dargelegt werden. Damit die Forschenden wissen, welche Themen und Inhalte hierbei relevant sind, haben die Datenschutzaufsichtsbehörden unter Koordination des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit eine Datenschutz-Checkliste erstellt (https://datenschutz.hessen.de/presse/digital-services-act-forschende-erhalten-zugang-zu-nicht-oeffentlichen-plattformdaten).

In meiner Funktion als Co-Vorsitz der Taskforce Forschungsdaten habe ich bei der Erstellung der Checkliste mitgewirkt. In guter Zusammenarbeit mit

der Bundesnetzagentur konnte die Checkliste zügig erstellt werden und stand für die Forschenden mit dem Start der einheitlichen Antragsplattform bereit.

15.4
Leitfaden für Datenschutz in der medizinischen Forschung

In der medizinischen Forschung hat der Datenschutz eine besondere Bedeutung. In der Regel stehen sensible Gesundheitsdaten und damit besonders schützenswerte Daten im Fokus. Für die Forschenden ist es aber nicht immer leicht, die datenschutzrechtlichen Anforderungen vollständig zu durchdringen. Um hier eine praxisnahe Unterstützung zu geben, haben die Deutsche Gesellschaft für Innere Medizin e. V. (DGIM) und ich einen Leitfaden zum Datenschutz in der medizinischen Forschung veröffentlicht.

Seit Jahren betreiben die DGIM und ich einen intensiven Dialog zum Datenschutz in der medizinischen Forschung, der sehr zum gegenseitigen Verständnis der unterschiedlichen Sichtweisen auf die zu lösenden Probleme geführt hat. Aus ihm entstand der beiderseitige Wunsch, die Umsetzung von Datenschutz in der medizinischen Forschung in der Praxis zu unterstützen. Daher haben Vertreter der DGIM und meiner Behörde gemeinsam an der Konzeption und Erstellung eines Leitfadens zum Datenschutz in der medizinischen Forschung gearbeitet. Die erste Fassung des Leitfadens konnte Ende 2025 veröffentlicht werden (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2025-12/20251028_dgim_hbdi_leifaden_datenschutz_1.01.pdf).

In dem Leitfaden werden vier konkrete Fallbeispiele (use cases) aus der Praxis der medizinischen Forschung dargestellt und datenschutzrechtlich eingeordnet. In jedem dieser Fallbeispiele haben DGIM und HBDI die Probleme beschrieben und im Dialog gelöst und dabei datenschutzkonforme Lösungswege aufgezeigt. Die Fallbeispiele behandeln Themen wie den Einsatz von Künstlicher Intelligenz in verschiedenen medizinischen Bereichen (Darmkrebsvorsorge, Pathologie, Intensivmedizin) und die Abgrenzung von Qualitätssicherung und wissenschaftlicher Forschung.

Besondere Aufmerksamkeit widmet der Leitfaden der Frage, unter welchen Umständen Daten als anonym betrachtet werden können. Die Nutzung von anonymen Daten ist für die medizinische Forschung und das Training von KI-Modellen von besonderer Relevanz. Für Forschungsvorhaben, bei denen eine Anonymisierung nicht sinnvoll ist, stellt der Leitfaden die alternativen datenschutzrechtlichen Rechtsgrundlagen dar.

Die Autoren verstehen den Leitfaden als ein „lebendes Dokument“. Sie wollen zukünftig weitere Fallbeispiele in den Leitfaden aufnehmen. Dazu soll die Zusammenarbeit zwischen der DGIM und mir fortgesetzt werden. Beide Seiten sehen die Zusammenarbeit an dem Leitfaden als ein gelungenes Beispiel für einen Datenschutz an, der im Austausch mit der Praxis gelebt wird.

16. Technik und Organisation

In meiner Abteilung für technischen und organisatorischen Datenschutz sorgt eine gelungene Schwerpunktsetzung für eine arbeitsteilige, aber zugleich enge, effektive und effiziente Zusammenarbeit (Kap. 16.1). Die Zielsetzung ist, vor allem durch Beratung und Unterstützung datenschutzkonforme Datenverarbeitungen zu erreichen. Dies ist im Berichtsjahr in Bezug auf den Einsatz von Microsoft 365 (Kap. 16.2), zur Einführung der Bezahlkarte für Asylsuchende (Kap. 16.3), durch die Entwicklung eines Werkzeugs zur Analyse von Datenveröffentlichungen im Darknet (Kap. 16.4) und durch einen Webseiten-Check für Vereine (Kap. 16.5) gelungen. Wir waren Gastgeber für den Dritten Informationsaustausch der IT-Labore der Datenschutzbehörden (Kap. 16.6) und konnten das erste Akkreditierungsverfahren für eine Zertifizierungsstelle nach Art. 43 DS-GVO abschließen (Kap. 16.7). Datenschutzverletzungen müssen nach Art. 33 DS-GVO an mich gemeldet werden. Ihre Bearbeitung beansprucht einen großen Teil der Arbeitskraft in meiner Behörde (Kap. 16.8). Solche Datenschutzverletzungen betrafen z. B. Ransomware-Angriffe auf Pflegeeinrichtungen (Kap. 16.9), Datenpreisgaben bei einem Luftfahrtkonzern (Kap. 16.10) und Datenschutzvorfälle durch Phishing (Kap. 16.11).

16.1 Arbeitspraxis der Abteilung für technischen und organisatorischen Datenschutz

In meiner Abteilung für technischen und organisatorischen Datenschutz erfolgte in der Vergangenheit eine Schwerpunktsetzung, um eine effektivere, effizientere und einheitlichere Bearbeitung von Vorgängen zu erreichen. Anhand eines konkreten Vorfalls wird nun dargestellt, wie eine zielführende Zusammenarbeit an Berührungspunkten erfolgt und wie sich die Schwerpunkte der Referate ergänzen.

In meinem 52. Tätigkeitsbericht habe ich die Schwerpunktsetzung der Referate in der Abteilung für technischen und organisatorischen Datenschutz meiner Behörde vorgestellt (52. Tätigkeitsbericht zum Datenschutz, Kap. 14.1). Hierbei habe ich separat Beispiele der Tätigkeiten der Referate vorgestellt. Nach mehr als zwei Jahren kann ich mit einem positiven Resümee auf die zielorientierte Arbeitsteilung zwischen den Referaten für technischen und organisatorischen Datenschutz blicken, die den aktuellen Herausforderungen gerecht wird.

Im Rahmen der Tätigkeiten der einzelnen Referate kommt es jedoch auch immer wieder zu Berührungspunkten. In solchen Fällen zeigen sich die Vorteile einer kollegialen, effektiven und effizienten Zusammenarbeit. Diese werden im Folgenden anhand eines Vorfalls dargestellt, der sich Ende März 2025 bei einem Auftragsverarbeiter eines in Hessen ansässigen Elektronikherstellers zugetragen hat. Dabei wurden durch Angreifer Kundendaten des Verantwortlichen aus einer IT-Umgebung eines Auftragsverarbeiters kopiert und im sogenannten Darknet veröffentlicht.

Meldung von Verletzungen des Schutzes personenbezogener Daten

Wird einem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, so muss er diese dem Verantwortlichen gemäß Art. 33 Abs. 2 DS-GVO unverzüglich melden. Der Verantwortliche muss daraufhin prüfen, ob der Vorfall voraussichtlich zu einem Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen führt. Im Falle eines voraussichtlichen Risikos muss er mir gemäß Art. 33 Abs. 1 DS-GVO die Verletzung des Schutzes personenbezogener Daten unverzüglich (möglichst binnen 72 Stunden) melden. Hat die Verletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen natürlichen Personen zur Folge, muss der Verantwortliche diese gemäß Art. 34 Abs. 1 DS-GVO zusätzlich unverzüglich benachrichtigen.

Der Auftragsverarbeiter meldete dem Verantwortlichen den Vorfall noch am Tag der Entdeckung. Daraufhin untersuchte dieser den Sachverhalt und kam zu dem ersten Ergebnis, dass voraussichtlich ein Risiko für Rechte und Freiheiten der betroffenen Personen bestand. Aus diesem Grund meldete er mir die Datenschutzverletzung fristgerecht gemäß Art. 33 Abs. 1 DS-GVO innerhalb von 72 Stunden. Da seine Untersuchung zu diesem Zeitpunkt noch nicht abgeschlossen war, hatte diese erste Meldung den Charakter einer ersten, schrittweisen Bereitstellung von Informationen im Sinne des Art. 33 Abs. 4 DS-GVO über die bis zu diesem Zeitpunkt vorliegenden Erkenntnisse.

Nach dieser ersten Meldung setzte der Verantwortliche die Untersuchung und Behandlung des Vorfalls fort. Durch die fortgeführte Risikobewertung kam er anschließend zu dem Ergebnis, dass insbesondere die Verletzung der Vertraulichkeit ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen natürlichen Personen zur Folge hatte, da u. a. Namen und E-Mail-Adressen betroffen waren. Über diesen neuen Sachverhalt und die geplante Benachrichtigung der betroffenen Personen gemäß Art. 34 Abs. 1 DS-GVO informierte mich der Verantwortliche wieder gemäß Art. 33 Abs. 4 DS-GVO. Etwa eine Woche nachdem ihm der Vorfall bekannt geworden war, begann der Verantwortliche, ca. 270.000 Personen gemäß Art. 34 Abs. 1

DS-GVO zu benachrichtigen. Aufgrund der großen Anzahl betroffener Personen dauerte dies mehrere Tage.

Der Verantwortliche analysierte den Vorfall und die betroffenen Daten nach der Benachrichtigung der betroffenen Personen weiter und detaillierter. Nach drei Monaten erkannte er, dass für eine Teilmenge von weniger als 1 % der betroffenen Personen weitere Kategorien von personenbezogenen Daten betroffen waren. Diese umfassten u. a. IBANs und Bankinformationen, für eine einstellige Anzahl an Personen auch Kreditkarteninformationen. Der Verantwortliche benachrichtigte die hiervon betroffene Personengruppe daher erneut unter Berücksichtigung der neuen Erkenntnisse und der möglichen resultierenden Folgen der Verletzung.

Im Laufe der Vorgangsbearbeitung der Art. 33-Meldung holte ich beim Verantwortlichen verschiedene Auskünfte ein. So ist es bei einer Datenschutzverletzung bei einem Auftragsverarbeiter z. B. relevant zu prüfen, welche technischen und organisatorischen Maßnahmen zwischen den beiden Stellen vereinbart worden sind, um diese Art von Vorfällen zu verhindern. In diesem Fall war es auch von Interesse nachzuvollziehen, wie der Verantwortliche die von der Datenschutzverletzung betroffenen personenbezogenen Daten und die Personen identifiziert hatte. Die Prüfung der bereitgestellten Informationen ergab keine Anzeichen für mögliche Beanstandungen. Der Verantwortliche hatte unverzüglich und angemessen auf den erkannten Vorfall beim Auftragsverarbeiter reagiert. Da dieser seinen Sitz in einem anderen Bundesland hat, ist die dortige Datenschutzaufsichtsbehörde für ihn örtlich zuständig.

Beratung betroffener Personen

Als Teil der Erfüllung der Benachrichtigungspflicht gemäß Art. 34 Abs. 1 DS-GVO informierte der Verantwortliche die Betroffenen gemäß Art. 34 Abs. 2 DS-GVO u. a. über die wahrscheinlichen Folgen des Vorfalls. Je nach Umständen des Vorfalls sowie Art und Umfang der betroffenen Daten können die betrachteten Folgen verschiedene Schwerpunkte haben. In Fällen wie dem vorliegenden schloss dies insbesondere Folgendes mit ein:

– Unbefugte Nutzung betroffener Daten für Phishing-Versuche,
– Identitätsdiebstahl etwa für Online-Einkäufe oder Abschluss von Verträgen sowie
– Bloßstellungen und Erpressungsversuche.

Die Möglichkeit solcher Folgen schürt nachvollziehbare Ängste bei den betroffenen Personen. Dies führte zu Nachfragen bei meiner Behörde hinsichtlich des Umgangs mit den möglichen Folgen des Vorfalls.

Gerade das Thema Identitätsdiebstahl ist im Zusammenhang mit Verletzungen des Schutzes personenbezogener Daten für Betroffene von besonderer Bedeutung. Aus diesem Grund habe ich im Rahmen meiner Beratung auch einen auf dieses Thema gerichteten Beitrag auf meiner Website veröffentlicht. Der Beitrag mit dem Titel „Umgang mit Identitätsdiebstahl – Erkennen, Reagieren, Vorbeugen“ (https://datenschutz.hessen.de/datenschutz/internet-und-medien/umgang-mit-identitaetsdiebstahl) soll Personen, die hiervon betroffen sind oder sich für einen solchen Fall vorbeugend informieren möchten, die wichtigsten Informationen zentral und öffentlich abrufbar bereitstellen. Neben allgemeinen Informationen für Betroffene von Identitätsdiebstahl enthält der Artikel vor allem auch Hinweise zum Verhalten bei kompromittierten E-Mail-Konten und Hilfestellungen in diesem Zusammenhang. Gerade E-Mail-Konten sind in der digitalen Welt häufig ein zentraler Schlüssel zur digitalen Identität einer Person und dementsprechend häufig das Ziel von Angriffen. So dienen E-Mail-Konten etwa häufig als Schnittstelle zu anderen Online-Konten und können in diesem Zusammenhang auch zu deren Übernahme missbraucht werden, etwa mittels einer „Passwort vergessen“-Funktion. Auch können in einem E-Mail-Konto gespeicherte E-Mails vielfältige Informationen enthalten, die Kriminelle für ihre Aktivitäten ausnutzen können, etwa Kontaktdaten, Kontoauszüge, Bestellinformationen oder Bankdaten. Die möglichen Folgen können vielfältiger Art sein und nicht nur die ursprünglich betroffenen Personen selbst, sondern auch deren Kommunikationspartner betreffen.

Dabei ist jedoch auch zu berücksichtigen, dass die Benachrichtigung durch einen Verantwortlichen nicht automatisch bedeutet, dass eine betroffene Person auch schon konkret Opfer eines Identitätsdiebstahls geworden ist. Meist liegt lediglich eine latente Gefahr vor, die sich unter Umständen auch erst nach Jahren verwirklichen kann. Um diese zu minimieren, sollten Betroffene daher im digitalen Raum Sicherheitsvorkehrungen zum Schutz ihrer Daten treffen und diese regelmäßig prüfen und an die aktuellen technischen Gegebenheiten anpassen. Dies schließt etwa auch die Beobachtung von Kontobewegungen mit ein. Kommt es tatsächlich zu einem Identitätsdiebstahl oder einem Erpressungsversuch, sollten Opfer unverzüglich Kontakt mit der zuständigen Strafverfolgungsbehörde aufnehmen und eine Strafanzeige erstatten. Ich habe die betroffenen Personen entsprechend beraten und ihnen angeboten, sich bei weiterführenden Fragen erneut an mich zu wenden.

Hinweise auf Datenschutzverletzungen und Beschwerden

Zu dem Vorfall gingen bei meiner Behörde nicht zuletzt aufgrund der gesetzesgemäßen Benachrichtigung gemäß Art. 34 Abs. 1 DS-GVO durch den Verantwortlichen 30 Beschwerden ein. Diese waren schwerpunktmäßig

technischer Natur. Ausgehend von dem jeweiligen Anliegen der Petentinnen und Petenten ließen sich diese 30 Vorgänge wie folgt klassifizieren:

1. In acht Fällen war die Geltendmachung etwaiger Schadenersatzansprüche das zentrale Anliegen der Eingebenden.
2. In neun Fällen beschränkte sich die Eingabe auf einen Hinweis darauf, dass es zu einem solchen Vorfall gekommen war.
3. In 13 Fällen hatte die Beschwerde die Informationsbereitstellung durch den Verantwortlichen zum Gegenstand, im Kern also die Erfüllung seiner Pflichten aus Art. 34 Abs. 2 DS-GVO.

Das Anliegen der Beschwerdeführer entscheidet dabei maßgeblich über die Art der Vorgangsbearbeitung mit. Für die Durchsetzung etwaiger Schadenersatzansprüche sind die Datenschutzbehörden nicht zuständig. Sofern eine betroffene Person einen solchen Anspruch gemäß Art. 82 DS-GVO geltend machen möchte, handelt es sich dabei um einen zivilrechtlichen Anspruch, den sie im Wege der ordentlichen Gerichtsbarkeit durchsetzen kann. Dazu kann ich sie jedoch ebenso wenig beraten, wie ich ihren Anspruch unmittelbar gegenüber dem Verantwortlichen durchsetzen könnte. Aus diesem Grund bleibt mir bei dieser Art von Eingaben lediglich der Verweis an die Mitglieder der rechtsberatenden Berufe.

Ein Hinweis auf einen vermeintlichen Datenschutzverstoß ist gegenüber meiner Behörde immer möglich. Der Umfang der Bearbeitung solcher Hinweise kommt unter anderem auch auf die zeitliche Abfolge der Ereignisse an. Beim Vorliegen der entsprechenden Voraussetzungen ist ein Verantwortlicher zur unverzüglichen Meldung einer Verletzung des Schutzes personenbezogener Daten an meine Behörde gemäß Art. 33 Abs. 1 DS-GVO verpflichtet. Liegt mir eine solche Meldung bereits vor, wenn mich Beschwerden zu demselben Vorfall erreichen, bearbeite ich die Meldung gemäß Art. 33 Abs. 1 DS-GVO vorrangig. Dies liegt zum einen darin begründet, dass die Bearbeitung der Meldung zu diesem Zeitpunkt ohnehin bereits begonnen hat und eine Unterbrechung nicht zweckmäßig wäre. Zum anderen steht die Meldepflicht für Verantwortliche aber auch in einem Spannungsverhältnis mit dem im deutschen Rechtswesen etablierten Grundsatz der Freiheit vor einer Selbstbezichtigung („Nemo-tenetur“-Grundsatz). Diesem Grundsatz folgend dürfen Verantwortliche nicht dazu gezwungen werden, sich selbst zu belasten. Eine pflichtgemäße Meldung ohne die Bekanntgabe belastender Informationen ist in vielen Fällen aber nicht möglich. Daher ist in den §§ 42 Abs. 4 und 43 Abs. 4 BDSG geregelt, dass Meldungen gemäß Art. 33 Abs. 1 DS-GVO nicht ohne die Zustimmung der Verantwortlichen in Straf- oder Ordnungswidrigkeitenverfahren gegen diese verwendet werden können. Dies schränkt das Spektrum möglicher Sanktionen gegenüber den Verantwortlichen ohnehin

ein. Eine pflichtgemäße Abgabe von Meldungen gemäß Art. 33 Abs. 1 DS-GVO gegenüber meiner Behörde ist zudem wünschenswert. Daher erfolgt bei einer nachgelagerten Beschwerde gegenüber dem Beschwerdeführer nur der Hinweis darauf, dass eine entsprechende Meldung des Verantwortlichen bei mir vorliegt. Da die Beschwerdeführer nicht Beteiligte des Verfahrens zu dieser Meldung sind, stehen ihnen weitergehende Informationen auch nicht zu. Anders verhält es sich, wenn mich eine Beschwerde zuerst erreicht und die Meldung gemäß Art. 33 DS-GVO nicht unverzüglich abgegeben worden ist. In diesem Fall betreibe ich vorrangig das Beschwerdeverfahren, da ein Meldeverstoß durch den Verantwortlichen im Raum steht und er dementsprechend auch nicht privilegiert ist.

Auch wenn der Gegenstand der Beschwerde über das reine Vorliegen eines Vorfalls hinausgeht – z. B. weil sich der Beschwerdeführer auf eine unzureichende Benachrichtigung gemäß Art. 34 Abs. 1 DS-GVO bezieht –, prüfe ich das Vorliegen von Verstößen. Bei dem Vorfall habe ich so etwa die Praxis des Verantwortlichen überprüft und darauf hingewiesen, betroffenen Personen ihre Auskünfte, verteilt auf mehrere einzelne Dateien – einen pro Dienst des Verantwortlichen –, mitzuteilen.

Einige dieser Eingaben an meine Behörde wurden offenbar mit Unterstützung von KI-Werkzeugen formuliert. Dies zeigt sich etwa anhand des Aufbaus der Texte (z. B. eine zuvor eher selten beobachtete strukturierte Gliederung) als auch an ihren Inhalten (häufiger Bezug auf rechtliche Regelungen, der zuvor von Privatpersonen selten gewählt wurde, sowie immer wiederkehrende Formulierungen). Während solche Werkzeuge Beschwerdeführer etwa im Sinne einer Rechtschreibkorrektur bei der Formulierung von Eingaben durchaus sinnvoll unterstützen können, waren die Grenzen der eingesetzten KI-Systeme immer wieder klar ersichtlich. So wurden etwa die Aufgaben der Datenschutzaufsichtsbehörde falsch dargestellt und darauf aufbauend Beschwerdeführer zu einem nicht zielführenden und damit für sie letztlich leider frustrierenden Vorgehen bewegt. Dies zeigt, dass die Verwendung von KI-Systemen eine angemessene Auseinandersetzung mit anderen, faktischen Informationsquellen hier nicht ersetzen kann.

Zusammenarbeit

Den Ausgangspunkt der Befassung meiner Behörde mit dem Vorfall bildete die Meldung des Verantwortlichen gemäß Art. 33 Abs. 1 DS-GVO. Die in der Folge durchgeführten Aktivitäten des zuständigen Referats führten auch dazu, dass mir umfangreiche Informationen zum Vorfall vorlagen und ich über die Hintergründe des Vorfalls informiert war. Hierauf konnte das zuständige Referat aufbauen, als besorgte Beratungsanfragen betroffener Personen

eingingen. Eine erneute Sachverhaltsermittlung konnte unterbleiben und es konnte direkt eine für den konkreten Fall angemessene und zielführende Beratung erfolgen. Dasselbe galt auch für von betroffenen Personen eingereichte Beschwerden. Insgesamt tauschten sich die drei beteiligten Referate zum Sachstand und zu Einzelfragen aus, um die einzelnen Vorgänge effizient und gemäß der jeweiligen Schwerpunktsetzung effektiv zu bearbeiten.

16.2
Mehr Rechtssicherheit beim Einsatz von Microsoft 365

Der Einsatz cloudbasierter Standardsoftware, insbesondere von Microsoft 365 (M365), stellt öffentliche und nicht-öffentliche Stellen seit Jahren vor erhebliche datenschutzrechtliche Herausforderungen. Zuletzt hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) 2022 festgestellt, dass Verantwortliche den Nachweis eines datenschutzrechtskonformen Betriebs von M365 auf Grundlage des damals vorliegenden Datenschutznachtrags von Microsoft nicht führen konnten.

Diese Feststellung war die Grundlage von etlichen Informationsveranstaltungen, die ich im Jahr 2023 veranstaltete, und führte zu mehreren Aufsichtsverfahren gegen Verantwortliche in Hessen (s. 52 Tätigkeitsbericht zum Datenschutz, Kap. 1.2). Sie verursachte in der Praxis erhebliche Rechtsunsicherheit, sowohl im öffentlichen Bereich als auch in der Privatwirtschaft. Vor diesem Hintergrund habe ich Gespräche mit Microsoft aufgenommen, um zu prüfen, ob – unter Berücksichtigung zwischenzeitlicher rechtlicher, vertraglicher und technischer Entwicklungen – mittlerweile ein datenschutzkonformer Einsatz von M365 möglich ist. Ziel war es, öffentlichen und nicht-öffentlichen Stellen mit Sitz in Hessen grundlegende Handlungs- und Rechtssicherheit zu verschaffen. Die Ergebnisse dieser Gespräche habe ich in einem ausführlichen Bericht zum Einsatz von M365 zusammengefasst, der auf meiner Webseite unter https://datenschutz.hessen.de/presse/hbdi-microsoft-365-kann-datenschutzkonform-genutzt-werden veröffentlicht ist (s. auch Kap. I 1.5).

Bezogen auf die sieben von der DSK benannten Kritikpunkte komme ich zu dem Ergebnis, dass ein datenschutzkonformer Betrieb von M365 hinsichtlich des Datenschutznachtrags von Microsoft grundsätzlich möglich ist. Diese Schlussfolgerung beruht insbesondere auf:

– der Fortentwicklung des Datenschutznachtrags (Data Protection Addendum – DPA) durch Microsoft, einschließlich spezifischer Anpassungen für öffentliche Stellen,

– zusätzlichen transparenzfördernden Begleitdokumenten, etwa einer Interpretationshilfe zum DPA und dem „M365-Kit“,
– einer von meiner Behörde erstellten Taxonomie der verarbeiteten Datenkategorien sowie
– veränderten rechtlichen Rahmenbedingungen, insbesondere dem Angemessenheitsbeschluss der Europäischen Kommission zum EU-U.S. Data Privacy Framework.

In Gesprächen mit Microsoft konnte ich klären, dass Microsoft personenbezogene Daten nicht für eigene Geschäftszwecke inhaltlich auswertet, sondern lediglich bestimmte generierte, abgeleitete oder gesammelte Daten in aggregierter Form verarbeitet. Diese aggregierten Daten weisen keinen Personenbezug mehr auf.

Im Folgenden werden die sieben Kritikpunkte der DSK am DPA vom 15. September 2022 genannt und die Gründe für eine neue Bewertung durch den HBDI erläutert:

1. Kritikpunkt: Im DPA fehlten klare Angaben zu Art und Zweck der Datenverarbeitung sowie zur Art der personenbezogenen Daten und betroffener Kategorien. – Microsoft hat inzwischen unterschiedliche Materialien erstellt, um besser über die Datenverarbeitung zu informieren, und für öffentliche Stellen den DPA überarbeitet, so dass Verantwortliche ausreichende Informationen über die Datenverarbeitung durch Microsoft erlangen und diese in ihr Verarbeitungsverzeichnis einbinden können.
2. Kritikpunkt: Microsoft lasse sich im DPA unzureichend konkretisierte Rechte für Datenverarbeitungen für eigene Geschäftstätigkeiten einräumen. – Microsoft hat klargestellt, dass es nur Log- und Diagnose-Daten, nicht aber Inhaltsdaten, in anonymisierter und aggregierter Form für Zwecke des Auftraggebers (des verantwortlichen Kunden) verarbeite. Diese Datenverarbeitung unterfällt entweder nicht der DS-GVO oder ist datenschutzrechtlich vertretbar.
3. Kritikpunkt: Microsoft behalte sich im DPA im Ergebnis umfangreiche Befugnisse vor, Daten ohne Weisung des Auftraggebers zu verarbeiten und Daten, auch gegenüber Drittstaaten, offenzulegen. – Microsoft hat sich im neuen DPA verpflichtet, personenbezogene Daten nur auf dokumentierte Anweisung des Kunden zu verarbeiten und sich hinsichtlich Offenlegungen der DS-GVO zu unterwerfen.
4. Kritikpunkt: Microsoft verpflichte sich nicht, die von der DS-GVO geforderten technischen und organisatorischen Sicherheitsmaßnahmen einzuhalten. – Microsoft hat sich im neuen DPA verpflichtet, die Vorgaben der DS-GVO ohne Abstriche einzuhalten.

5. Kritikpunkt: Die Ausgestaltung der Rückgabe- und Löschverpflichtung im DPA genüge nicht den gesetzlichen Anforderungen. – Microsoft bietet einen Löschprozess an und ermöglicht allen Kunden, Daten auch selbst zu löschen oder löschen zu lassen, wenn diese schneller gelöscht werden müssen.
6. Kritikpunkt: Microsoft informiere nach dem DPA nicht über jede beabsichtigte Änderung in Bezug auf Unterauftragnehmer. – Microsoft hält dagegen sechs Monate bzw. einen Monat im Voraus in seinem Service Trust Portal detaillierte Informationen über jeden Unterauftragnehmer bereit und informiert darüber alle Kunden, so dass diese die Informationen problemlos zur Kenntnis nehmen können.
7. Kritikpunkt: Microsoft übermittle für den Betrieb von M365 personenbezogene Daten unzulässigerweise in die USA und in andere Staaten. – Inzwischen verarbeitet Microsoft die Daten fast vollständig im Europäischen Wirtschaftsraum. Die verbleibenden Datenübermittlungen in die USA und andere Staaten sind durch Angemessenheitsbeschlüsse der Europäischen Kommission und Standardvertragsklauseln gedeckt.

Auch wenn hinsichtlich der von Microsoft im Rahmen der bereitgestellten Produkte und Services mehr Transparenz besteht und durch die Anpassungen des Datenschutznachtrags mehr Rechtssicherheit entsteht, möchte ich betonen, dass die Möglichkeit eines datenschutzkonformen Einsatzes von M365 nicht automatisch gegeben ist. Denn der rechtmäßige Einsatz setzt voraus, dass Verantwortliche die ihnen nach der DS-GVO obliegenden Pflichten erfüllen. Dazu gehören etwa:

– die Dokumentation von Zwecken und Rechtsgrundlagen der Datenverarbeitung,
– die Überprüfung der zur Verarbeitung vorgesehenen Dienste hinsichtlich der Anforderungen und Voraussetzungen eines datenschutzkonformen Einsatzes,
– die angemessene Konfiguration der eingesetzten Dienste,
– die Einbindung der Nutzung von M365 in das Verzeichnis der Verarbeitungstätigkeiten,
– die Prüfung und Steuerung von Lösch- und Aufbewahrungsfristen sowie
– die laufende Bewertung von Drittlandübermittlungen und Unterauftragsverarbeitern.

Der M365-Bericht enthält hierzu und zu weiteren Punkten konkrete Handlungsempfehlungen, die den Verantwortlichen als Orientierung für eine datenschutzgerechte Nutzung dienen sollen. Auch wenn diese Handlungsempfehlungen nicht abschließend sind, hoffe ich, dass sie einen Beitrag zu

einer praxisnahen und rechtssicheren Umsetzung der datenschutzrechtlichen Anforderungen leisten können.

Mit dem M365-Bericht verfolge ich einen differenzierten und konstruktiven Ansatz. Ziel ist es nicht, den Einsatz bestimmter Produkte pauschal zu untersagen oder zu empfehlen, sondern darauf hinzuwirken, dass Verantwortliche in Kenntnis meiner Rechtsauffassung ihre Bewertung vornehmen und hierauf aufbauend ihren datenschutzrechtlichen Pflichten nachkommen können. Der Bericht ersetzt mithin keine Einzelfallprüfung, schafft aber einen belastbaren Rahmen für die Aufsichtspraxis meiner Behörde.

Losgelöst von einer rein datenschutzrechtlichen Betrachtungsweise möchte ich darauf hinweisen, dass der Einsatz marktbeherrschender, außereuropäischer Cloud-Angebote mit strukturellen Risiken verbunden ist. Auch wenn das DPA zu M365 die Mindestanforderungen der DS-GVO erfüllt: Eine Digitalstrategie, die ausschließlich auf die Nutzung außereuropäischer Cloud-Angebote gerichtet ist, bringt erhebliche Risiken für Staat, Verwaltung und Gesellschaft mit sich. Digitale Souveränität sollte daher ein zentrales strategisches Ziel für öffentliche und nicht-öffentliche Stellen sein. Verantwortliche sollten bei der Digitalisierung daher nicht allein kurzfristige Funktionalität, sondern auch langfristige Souveränitäts- und Resilienzfragen in ihre Entscheidungen einbeziehen.

16.3
Beratung zur Einführung der Bezahlkarte für Asylsuchende

Vier Datenschutzaufsichtsbehörden begleiteten 2024 die zentrale Ausschreibung und Beauftragung der Bezahlkarte zur Gewährung von Leistungen an Asylsuchende in Form eines gemeinsamen Beratungsprojekts. Auf die Ergebnisse konnten alle 14 Datenschutzaufsichtsbehörden der Bundesländer aufbauen, in denen diese zentralisierte Lösung eingeführt wurde. Diese neue Form der effizienten Arbeitsteilung zwischen den deutschen Datenschutzaufsichtsbehörden konnte in diesem Projekt erfolgreich demonstriert werden (s. auch Kap. 1.4).

Problemstellung

Mit der zentralen Ausschreibung der Bezahlkarte für 14 Bundesländer durch die aus den fachministeriellen Vertretern und Vertreterinnen der Länder Hessen, Baden-Württemberg, Niedersachsen und Hamburg bestehende Länder-AG sollte ein einheitlicher technischer Dienstleister für die Bezahlkarte gefunden werden. Mit Hilfe der Bezahlkarte sollten künftig Leistungen nach dem Asylbewerberleistungsgesetz an die Leistungsberechtigten ausgezahlt

werden. In diesem Zusammenhang wurde zusätzlich eine Vorlage für eine Datenschutzfolgeabschätzung (DSFA) erstellt, um die datenschutzrechtlichen Risiken des Systems zu ermitteln und zu minimieren.

Da Hessen den Vorsitz in der Ministerpräsidentenkonferenz führte, bat mich die Hessische Staatskanzlei, eine zentrale datenschutzrechtliche Begleitung dieses Projekts zu organisieren. Eine kontinuierliche, beratende Begleitung solch dynamischer und zeitkritischer Projekte durch den Datenschutz erfordert eine schnelle und einheitliche Beratung. Für die Beratung des Vergabeverfahrens der Länder-AG wurde aus diesem Grund nach Absprache in der DSK eine neue Form der Zusammenarbeit erprobt, die dem Ansatz „Einer für Alle“ (EfA) folgte. Diesem Ansatz entsprechend übernahm eine kleine Gruppe von Aufsichtsbehörden unter meiner Leitung die Beratung der Länder-AG. Die so ins Leben gerufene AG Leistungsbeschreibung wurde aus vier der 14 zuständigen Aufsichtsbehörden, nämlich Baden-Württemberg, Hamburg, Nordrhein-Westfalen und Hessen, gebildet und führte eine gemeinsame Bewertung für alle Aufsichtsbehörden durch. Ziel war es, eine schnelle, am Projekt orientierte Beratung zu gewährleisten, Ressourcen zu bündeln und eine einheitliche Bewertung sicherzustellen. Dies führte zu einer effizienten und effektiven Zusammenarbeit und trug dazu bei, die besonderen datenschutzrechtlichen Herausforderungen solcher bundesländerübergreifender IT-Projekte koordiniert zu meistern.

Bezahlkarte für Asylsuchende

Spätestens Ende 2023 zeichnete sich der politische Wunsch ab, bundesländerübergreifend eine Bezahlkarte zur Gewährung von Leistungen an Asylsuchende einzuführen. Anstelle der bisherigen Ausgabe von Bargeld sollten existenzsichernde Leistungen künftig über eine in das Kreditkartensystem integrierte Debitkarte ausgezahlt werden, jedoch ohne dass leistungsberechtigte Personen ein Bankkonto dafür benötigen. Am 31. Januar 2024 beschlossen die Bundesländer nicht nur einheitliche Mindeststandards hinsichtlich der Funktionen dieser Bezahlkarte, sondern darüber hinaus auch die Durchführung eines gemeinsamen Vergabeverfahrens. Hieran beteiligten sich alle Bundesländer mit Ausnahme von Bayern und Mecklenburg-Vorpommern. Die Rechtsgrundlage für die Nutzung der Bezahlkarte als Mittel der Leistungsgewährung wurde im Mai 2024 durch die Anpassung des Asylbewerberleistungsgesetzes (AsylbLG) geschaffen.

Auf Grund der definierten Anforderungen des einheitlichen Mindeststandards sowie der geplanten zentralen Verarbeitung der Daten der leistungsberechtigten Personen bei einem Dienstleister ergab sich eine Reihe von datenschutzrechtlichen Fragestellungen. Durch den AK Verwaltung der DSK

wurde in Absprache mit dem AK Gesundheit und Soziales hierzu eine Unterarbeitsgruppe (UAG) gegründet. Diese UAG erarbeitete ein Positionspapier zur datenschutzrechtlichen Einordnung der Bezahlkarte (DSK, Positionspapier zu „Datenschutzrechtliche Grenzen des Einsatzes von Bezahlkarten zur Leistungsgewährung nach dem Asylbewerberleistungsgesetz (AsylbLG)“ vom 19. August 2025, https://www.datenschutzkonferenz-online.de/media/dskb/2024_08_19_DSK_Beschluss_Bezahlkarte.pdf).

In diesem Papier wurde festgestellt, dass aus Sicht des Datenschutzes die Nutzung einer Bezahlkarte zur Leistungserbringung grundsätzlich möglich sein kann, soweit ausschließlich die zur Leistungserbringung erforderlichen personenbezogenen Daten verarbeitet werden. Die datenschutzrechtlichen Grenzen der Verarbeitung wurden in dem Positionspapier anhand der Erforderlichkeit zur Umsetzung des definierten Mindeststandards gezogen. Dies betraf insbesondere die folgenden Punkte:

– Einsichtnahme in den Guthabenstand,
– pauschale Einschränkung auf Postleitzahlen-Gebiete,
– Behördenübergreifenden Datenabgleich über den Dienstleister,
– Weitergabe der Ausländerzentralregister-Nummer an den Dienstleister sowie Zugriff der Sicherheitsbehörden auf Buchungsdaten.

Auftrag und Umfang des Beratungsprojekts

Der Beratungsgegenstand sollte die konkrete Leistungsbeschreibung für die Ausschreibung der Bezahlkarte sein. Die frühzeitige Einbindung der Datenschutzaufsichtsbehörden noch vor einer Ausschreibung eines IT-Projekts ist ein Vorgehen, das wir in Hessen in den letzten Jahren etablieren konnten. Die AG Leistungsbeschreibung hatte die Aufgabe, zu den rechtlichen und technischen Datenschutzanforderungen der Leistungsbeschreibung im Vergabeverfahren beratend Stellung zu nehmen und bei Bedarf beispielhafte Ergänzungsvorschläge anzubringen.

Im Rahmen des Beratungsprojekts erfolgte keine förmliche Prüfung oder umfassende Überarbeitung der Dokumente für die Ausschreibung der Bezahlkarte. Die Beratung konzentrierte sich auf ausgewählte wesentliche Datenschutzanforderungen, die als missverständlich oder problematisch identifiziert wurden. Dabei fand ein aktiver Austausch mit der Länder-AG statt. Die Beratung und Befassung mit der rechtlichen und technischen Thematik fanden vollständig auf der Ebene der von der Länder-AG vorgelegten Dokumente statt. Eine Prüfung der konkreten Umsetzung in den Ländern war nicht Aufgabe der AG Leistungsbeschreibung.

Ablauf des Beratungsprojekts

Insgesamt hat die AG Leistungsbeschreibung in den zwei Monaten April und Mai zu zwei Versionen der Leistungsbeschreibung für die Ausschreibung und die Beauftragung des Dienstleisters Stellung genommen und dabei Verbesserungs- sowie konkrete Formulierungsvorschläge entwickelt. Aufgrund der Anmerkungen in den Stellungnahmen hat die Länder-AG die Leistungsbeschreibung überarbeitet und einen Großteil der Formulierungsvorschläge übernommen.

Ende August 2024 wurde der Beratungsauftrag der AG Leistungsbeschreibung auf die Erstellung einer einheitlichen Muster-DSFA für die Leistungsbehörden durch die Länder-AG erweitert. Auf Basis der grundlegenden Hinweise der AG Leistungsbeschreibung zur ersten Version der Muster-DSFA entwarf eine von der Länder-AG beauftragte Anwaltskanzlei eine neue Muster-DSFA. Zur ersten sowie einer überarbeiteten Version dieser neuen Muster-DSFA nahm die AG Leistungsbeschreibung dann Stellung. Das Beratungsprojekt endete nach einem Jahr im März 2025.

Erreichte inhaltliche Ergebnisse

Die Textvorschläge der AG Leistungsbeschreibung zu notwendigen oder sinnvollen Ergänzungen oder Anpassungen der Leistungsbeschreibung wurden fast vollständig übernommen. Bei den grundsätzlichen datenschutzrechtlichen Kritikpunkten zu geforderten oder geplanten Funktionen der Bezahlkarte ist die Akzeptanz des Beratungsergebnisses unterschiedlich ausgefallen. In einigen Punkten wurden nach spezifischen Hinweisen in den Stellungnahmen und Gesprächen die Positionen der Datenschutzaufsichtsbehörden übernommen. Bei anderen Punkten gab es lediglich inhaltliche Annäherungen oder sprachliche Anpassungen.

In Bezug auf die im Positionspapier der DSK definierten datenschutzrechtlichen Grenzen der Bezahlkarten konnte aber erreicht werden, dass die Einsichtnahme in den Guthabenstand oder getätigte Buchungsdaten durch die Leistungsbehörden sowie die Weitergabe der Ausländerzentralregister-Nummer an den Dienstleister ausgeschlossen wurden. Die Funktionen, die einen behördenübergreifenden Datenabgleich notwendig gemacht hätten, wurden im Laufe der Beratung schrittweise funktional reduziert. Verblieben ist u. a. die bei Finanzdienstleistern übliche Prüfung, ob bereits eine Karte auf dieselbe Person ausgestellt wurde. Die Funktion ist weiterhin verfügbar, allerdings konnte erreicht werden, dass sie optional wurde und auf Ebene der Länder aktiviert und eingerichtet werden muss.

Die Rechtsgrundlagen für mögliche Zugriffe der Sicherheitsbehörden auf Buchungsdaten der Bezahlkarte werden durch die entsprechenden Bundes- und Landesgesetze geregelt. Dieser Aspekt war nicht Gegenstand des Beratungsprojekts.

Die Einführung der Bezahlkarte in den Bundesländern

Die abschließende datenschutzrechtliche Bewertung der Bezahlkarte liegt in der Zuständigkeit der Datenschutzaufsichtsbehörden der Bundesländer, die diese tatsächlich einführen. Die von der AG Leistungsbeschreibung erarbeiteten Ergebnisse wurden diesen Behörden zur Verfügung stellt. Bei der Einführung ist damit eine Konzentration auf die verbliebenen Punkte möglich, bei denen es unterschiedliche Rechtsauffassungen zwischen der Länder-AG und der AG Leistungsbeschreibung gab. Entsprechende mögliche Fragestellungen für Prüfungen und die jeweilige rechtliche Einordnung der AG Leistungsbeschreibung wurden sowohl den Aufsichtsbehörden als auch der Länder-AG bereitgestellt.

Im Abschlussgespräch teilte die Länder-AG mit, dass viele Bundesländer angekündigt hätten, von wenigstens einigen oder sogar allen der als datenschutzrechtlich problematisch bewerteten Vorgehensweisen keinen Gebrauch machen zu wollen. In welchem Umfang dies im jeweiligen Bundesland oder der jeweiligen Kommune zutrifft, kann durch die zuständige Aufsichtsbehörde überprüft werden.

Erfahrungen mit dem EfA-Prinzip für Beratungsprojekte

Bei der Beauftragung der AG Leistungsbeschreibung wurde das aus dem OZG-Kontext bekannte EfA-Prinzip angewendet. Dies bot mehrere Vorteile, die gut auf das konkrete Projekt passten. So konnte die kleine Gruppe ein effizientes und effektives Arbeitsumfeld schaffen. Sie war daher in der Lage, innerhalb der sehr kurzen Fristen Inhalte und Bewertungen zu erarbeiten, abzustimmen und diese in Form von schriftlichen Stellungnahmen in Richtung des Projekts zu kommunizieren.

Durch die frühzeitige Einbindung der Datenschutzaufsichtsbehörden in das Projekt konnten datenschutzrechtliche und -technische Aspekte bereits in der Leistungsbeschreibung für die Ausschreibung und Beauftragung des gemeinsamen Dienstleisters für die 14 Bundesländer berücksichtigt werden. Dies ermöglichte es, potenzielle Probleme oder Fragestellungen im Bereich des Datenschutzes frühzeitig zu identifizieren und zwischen der AG Leistungsbeschreibung und der Länder-AG zu diskutieren. Die Sensibilisierung der Länder-AG für die rechtlichen Erfordernisse des Datenschutzes führte

dazu, dass die Anforderungen für die Ausschreibung und Beauftragung des Dienstleisters konkretisiert und potenziell negativen Entwicklungen frühzeitig entgegengewirkt werden konnte.

Durch die aktive beratende Begleitung über einen längeren Zeitraum, auch über die Erstellung der Leistungsbeschreibung hinaus, konnten zudem zunächst kontroverse Positionen bei der Umsetzung der Bezahlkarte zusammengeführt werden. Der Vorteil für die betroffenen Personen besteht darin, dass die so erreichten wertvollen Ergebnisse und rechtlichen Bewertungen allen Aufsichtsbehörden, in deren Ländern die Bezahlkarte eingeführt wird, zugutekommen. Die Umsetzung von zentral berücksichtigten Datenschutzanforderungen muss nicht mehr separat durch die einzelnen Länder beim Dienstleister beauftragt werden. Auch können die Aufsichtsbehörden der Bundesländer gemäß des EfA-Prinzips auf der geleisteten Vorarbeit aufbauen.

Fazit

Es hat sich erneut gezeigt, dass eine frühe Einbindung der Datenschutzaufsichtsbehörden bereits zur Anforderungsphase vorteilhaft und wichtig ist. So konnten aus Sicht des Datenschutzes mögliche organisatorische und technische Probleme frühzeitig erkannt, adressiert und gemeinsam mit den verantwortlichen Stellen angegangen werden. Eine ganze Reihe von Herausforderungen konnte so durch die frühzeitige, schnelle und konstruktive Zusammenarbeit der beteiligten Stellen beseitigt oder zumindest in ausreichendem Maße abgemildert werden. Dies kam letzten Endes den betroffenen Personen zugute. Auf die Ergebnisse der AG Leistungsbeschreibung konnten wiederum die Aufsichtsbehörden der Bundesländer aufbauen.

Die Anwendung des EfA-Prinzips half, die Einheitlichkeit der datenschutzrechtlichen Bewertung gegenüber dem Projekt zu verbessern. Die AG Leistungsbeschreibung konnte sich thematisch tiefergehend in die rechtlichen und technischen Fragestellungen einarbeiten und die Ergebnisse mit allen anderen Aufsichtsbehörden teilen. Diese konnten die Ergebnisse nutzen, um den mit der Einführung der Bezahlkarte verbundenen Aufwand zu reduzieren. Die rechtliche Zuständigkeit der Aufsichtsbehörden der einzelnen Bundesländer für eine datenschutzrechtliche Prüfung und Bewertung wurde hierbei gewahrt. Gleichzeitig wurden mögliche Prüfungen und Umsetzungen von zum Teil länderspezifischen Datenschutzanforderungen erleichtert (s. zur Reformdiskussion auch Kap. 1.4.)

Abschließend kann ich festhalten, dass meine Behörde zusammen mit allen Beteiligten durch die frühzeitige Einbindung und die konstruktive Zusammenarbeit zwischen der AG Leistungsbeschreibung und der Länder-AG viel erreicht hat. Sie konnten bestehende datenschutzrechtliche Probleme bei

der Bezahlkarte für Asylsuchende vor der Einführung in den Bundesländern beseitigen oder abmildern. Davon profitieren nicht nur die öffentlichen Stellen, sondern vor allem die betroffenen Personen.

16.4
Werkzeug zur Analyse von Datenveröffentlichungen im Darknet

Angriffe auf die IT-Infrastruktur von Unternehmen wie auch von öffentlichen Stellen nehmen nach wie vor zu. Dass Angreifer teilweise Daten, die sie bei solchen Angriffen kopiert haben, im sogenannten Darknet veröffentlichen, stellt die angegriffenen Stellen, aber auch mich immer wieder vor Herausforderungen: Dann gilt es festzustellen, welche Daten überhaupt betroffen sind und welche datenschutzrechtlichen Pflichten an den Datenverlust anknüpfen. Hierzu hat meine Behörde ein eigenes Werkzeug programmiert und veröffentlicht.

Motivation

Angreifer kopieren Daten der angegriffenen Stellen, um diese Daten zur Erpressung der Stellen oder zu anderen kriminellen Zwecken, wie z. B. zum Verkauf, zu nutzen. Insbesondere bei den sogenannten Ransomware-Angriffen dient dies zur Erhöhung des Erpressungsdrucks; wird das Lösegeld nicht bezahlt, werden die Daten verkauft oder auch veröffentlicht. Dies führt zu Verletzungen des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12 DS-GVO, insbesondere aufgrund der Verletzung der Vertraulichkeit gegenüber einem unkontrollierbaren Empfängerkreis. Sind auch noch die Daten besonders sensibel, hat dies in der Regel hohe Risiken für die persönlichen Rechte und Freiheiten natürlicher betroffener Personen zur Folge. Die verantwortlichen Stellen müssen in diesem Fall die betroffenen natürlichen Personen unverzüglich gemäß Art. 34 Abs. 1 DS-GVO benachrichtigen, damit diese ihrerseits mögliche negative Folgen abwenden oder abschwächen können. Verzögerungen bei der Benachrichtigung können die Risiken vergrößern und müssen daher vermieden werden. In meiner aufsichtsbehördlichen Praxis sehe ich häufig, dass verantwortliche Stellen bei dieser Art von Vorfällen vor größeren Problemen stehen. Sehr häufig ziehen Angreifer Daten von über das Netzwerk angebundenen Datenspeichern ab, in denen vielfältige Arten von Daten gespeichert sind. Probleme entstehen für die verantwortlichen Stellen insbesondere, wenn an diesen Speicherorten unstrukturiert sehr viele Dateien unterschiedlicher Datenarten gespeichert sind. In der Praxis zeigt sich leider nicht selten, dass verantwortliche Stellen aus der eigenen Datenschutzdokumentation nicht oder nicht hinreichend vollständig entnehmen können, welche Datenkategorien und welche natürlichen Personen konkret

betroffen sind. Um die betroffenen natürlichen Personen in diesen Fällen benachrichtigen zu können, müssen sie und ihre betroffenen personenbezogenen Daten identifiziert werden.

Pflichten von betroffenen Stellen

Führt eine Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen, muss der Verantwortliche mir diese gemäß Art. 33 Abs. 1 DS-GVO melden. Bei einem hohen Risiko müssen die betroffenen natürlichen Personen zusätzlich gemäß Art. 34 Abs. 1 DS-GVO benachrichtigt werden. Sowohl für die Meldung gemäß Art. 33 Abs. 1 DS-GVO als auch für die Benachrichtigung gemäß Art. 34 Abs. 1 DS-GVO muss die verantwortliche Stelle gemäß Art. 33 Abs. 3 Buchst. c DS-GVO die wahrscheinlichen Folgen beschreiben. Diese hängen regelmäßig insbesondere von den betroffenen Datenkategorien ab und können sich für unterschiedliche Gruppen von betroffenen Personen unterscheiden. Weiterhin legt der Art. 34 DS-GVO den Vorzug auf eine möglichst individuelle Benachrichtigung einer betroffenen Person durch die verantwortliche Stelle. Es ist daher in der Regel notwendig, dass verantwortliche Stellen bei einer Datenschutzverletzung die betroffenen natürlichen Personen und deren betroffene Datenkategorien identifizieren. Nur mit diesen Informationen ist eine hinreichend detaillierte Benachrichtigung über die Datenschutzverletzung und deren Folgen möglich.

Werden personenbezogene Daten durch Angreifer kopiert, verkauft, veröffentlicht oder anderweitig unbefugt verarbeitet, führt dies bei sensiblen Daten mit entsprechenden möglichen Folgen in jedem Fall zu hohen Risiken für die Rechte und Freiheiten der betroffenen natürlichen Personen. Für das Überschreiten dieser Risikoschwelle ist es nicht notwendig, dass besondere Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO betroffen sind. Auch andere betroffene Datenkategorien können zu einem hohen Risiko führen, wenn aufgrund der Veröffentlichung Schadensereignisse mit den dazugehörigen Schadenshöhen wahrscheinlicher werden.

Falls es bei einem Auftragsverarbeiter zu einer Verletzung des Schutzes personenbezogener Daten kommt, können weitere Probleme bei der Zusammenarbeit mit den Verantwortlichen und in der Folge zeitliche Verzögerungen auftreten, die es zu vermeiden gilt. In meinem 51. Tätigkeitsbericht habe ich diese Problemstellung bereits detailliert beschrieben (s. 51. Tätigkeitsbericht, Ziff. 17.3).

Identifikation von Datenkategorien und betroffenen natürlichen Personen

Nach einer Verletzung der Vertraulichkeit personenbezogener Daten durch deren Kopieren oder Veröffentlichen durch unberechtigte Dritte müssen Verantwortliche oder ggf. auch deren Auftragsverarbeiter zunächst feststellen, welche Daten betroffen sind. Kurz nach einem entsprechenden Vorfall kann die Lage noch sehr unübersichtlich sein und eine zeitnahe Eingrenzung der betroffenen Daten unmöglich erscheinen. Gerade dann können eine vollständige und aktuelle Datenschutzdokumentation sowie entsprechende weitere Dokumentationen aus der IT-Sicherheit oder den Geschäftsprozessen aussagekräftige Informationen und damit Klarheit liefern. Eine wichtige und verlässliche Quelle können auch die potenziell betroffenen Daten selbst darstellen, die ggf. aus einer wirksamen Datensicherung wiederhergestellt wurden.

Die Beauftragung einer IT-forensischen Analyse bei den hier betrachteten Vorfällen sollte grundsätzlich den Untersuchungsgegenstand enthalten, ob und wenn ja, welche Daten durch die Angreifer kopiert wurden und bei welchen IT-Systemen dies geschehen sein könnte. Hierzu sollte mit dem forensischen Dienstleister auch vereinbart werden, dass er dieser Frage mit Priorität nachgeht und dem Verantwortlichen möglichst zeitnah erste Erkenntnisse bereitstellt.

Eine in der Praxis genutzte weitere Quelle für Informationen zur Eingrenzung von potenziell betroffenen Daten können die Angreifer selbst sein. Diese stellen den Angegriffenen häufig Datenproben oder Listen von angeblich kopierten Dateien bereit oder veröffentlichen diese auf Seiten im Darknet. Dabei handelt es sich um Seiten, die mit speziellen, aber allgemein verfügbaren Anwendungen aufgerufen werden können. Dabei wird durch technische Vorkehrungen eine gewisse Anonymität unterstützt, die insbesondere von den Angreifern auch zum Ausweichen der Strafverfolgung genutzt wird. Die dort bereitgestellten Angaben und Informationen können hilfreich sein, um beispielsweise mögliche Datenquellen zu identifizieren. Die mangelnde Beweiskraft dieser Angaben verhindert allerdings einen möglichen Umkehrschluss. Die Angaben der Angreifer können gewollt oder ungewollt unvollständig sein: Wenn potenziell betroffene Daten von den Angreifern nicht aufgeführt werden, kann daher nicht gefolgert werden, dass diese tatsächlich nicht betroffen sind.

Grundsätzlich ist bei Zugriffen auf die Seiten der Angreifer im Darknet und insbesondere auf dort bereitgestellte Dateien besondere Vorsicht geboten. Diese Seiten oder die Dateien können mit Schadcode versehen sein, um

IT-Systeme zu kompromittieren. Es kann daher sinnvoll sein, einen qualifizierten IT-Sicherheitsdienstleister damit zu beauftragen.

Kommt es zu einer Veröffentlichung von Daten durch die Angreifer und die verantwortliche Stelle war noch nicht in der Lage, die betroffenen Daten zu identifizieren, kann es notwendig werden, die veröffentlichten Daten selbst zu analysieren. Spätestens ab dem Zeitpunkt einer Veröffentlichung von personenbezogenen Daten ist deren Vertraulichkeit nicht mehr gewahrt und für die betroffenen natürlichen Personen ein dauerhafter Kontrollverlust entstanden. Daher ist eine möglichst zeitnahe Benachrichtigung dieser Personen erforderlich, um ihnen zu ermöglichen, etwaige nachteilige Folgen zu kontrollieren. Hierzu müssen die Betroffenen dem Verantwortlichen bekannt sein. Für die dahingehende Identifikation der hiervon betroffenen Personen und Datenarten sollten die veröffentlichten Daten durch qualifiziertes Personal oder einen Dienstleister gesichert werden. Wenn es möglich ist, eine Liste der veröffentlichten Dateien mit ihren Verzeichnispfaden zu erstellen, kann diese ggf. in Kombination mit einer vorhandenen vollständigen Datensicherung für die Identifikation genutzt werden.

Stammen die Daten einer Veröffentlichung ursprünglich aus einem Netzlaufwerk, wird eine Analyse häufig zur Herausforderung. Dies liegt nicht selten auch darin begründet, dass die enthaltenen Dateien oftmals relativ unstrukturiert vorliegen und im Falle von Bildern oder gescannten Dokumenten nicht direkt maschinenlesbar sind. Der Aufwand für eine vollständige Analyse dieser Daten kann daher sehr hoch sein. Eine allgemeine Beschreibung eines hinreichenden Vorgehens zur Identifikation ist nicht möglich. Dies hängt immer vom Einzelfall und den jeweiligen betroffenen Daten ab. Soweit dies möglich ist, können ggf. dedizierte und für diese Aufgabe qualifizierte Dienstleister eine verantwortliche Stelle unterstützen.

Der Umstand, dass zumindest aus Sicht des Datenschutzes nur personenbezogene Daten relevant sind, kann für ein effizientes Vorgehen genutzt werden. Die zu analysierende Datenmenge sollte soweit möglich reduziert werden:

1. Alle Dateien, die definitiv keine personenbezogenen Daten enthalten können, können von der weiteren Untersuchung ausgeschlossen werden wie etwa Konfigurationsdateien, Programme, Finanzdaten und Produktinformationen.
2. Soweit möglich sollten Verzeichnisbäume genutzt werden, um nicht personenbezogene Daten aus der weiteren Analyse auszuschließen.
3. Datei- oder Dokumentenarten, die mit hinreichender Wahrscheinlichkeit keine personenbezogenen Daten enthalten, können ebenfalls ausgeschlossen werden wie z. B. Rechnungen an oder Verträge mit juristischen Personen oder technische Zeichnungen.

Oftmals kann eine systematische Reduktion von Dateien, die mit überschaubarem Aufwand möglich ist, die Menge an genauer zu analysierenden Daten erheblich reduzieren. Im nächsten Schritt können die Daten dann manuell gesichtet werden. Je nach Menge und Struktur der Daten können ggf. auch spezielle Software-Werkzeuge helfen, mögliche personenbezogene Daten zu finden.

Umgang mit Datenveröffentlichungen

Meine Technikabteilung beobachtet im Rahmen der vorhandenen Kapazitäten einschlägige Blogs von Angreifern und verfolgt Open Source Intelligence (OSINT)-Quellen. Hierdurch informiert sie sich über potenzielle Datenveröffentlichungen mit Bezug zu verantwortlichen Stellen in Hessen. Sie hat im Berichtszeitraum damit begonnen, entsprechende Daten aus Datenveröffentlichungen zu sichern, sofern die einzelne Veröffentlichung einer hessischen Stelle zugeordnet werden konnte und die Sicherung mit vertretbarem technischem und organisatorischem Aufwand möglich war. Dies diente in dem konkreten Fall dazu, die Angaben der verantwortlichen Stellen zu einer Veröffentlichung bei Bedarf nachprüfen zu können. Weiterhin konnten damit mögliche Pflichtverstöße gegen Melde- und Benachrichtigungspflichten erkannt werden. In mehreren Fällen hat meine Behörde verantwortliche Stellen erstmalig über eine Veröffentlichung in Kenntnis gesetzt – dies sogar bei Vorgängen, bei denen die verantwortlichen Stellen spezialisierte IT-Dienstleister mit genau dieser Aufgabe beauftragt hatten.

Die Datensicherung erfolgt in meinem IT-Labor auch im Sinne der ordnungsgemäßen Aktenführung. In Ausnahmefällen, wie z. B. im Falle eines familiengeführten KMU, stelle ich verantwortlichen Stellen die gesicherten Daten auch zur Verfügung, wenn diese selbst nicht in der Lage sind, diese selbst zu sichern. Die dadurch entstehenden Kosten werden den verantwortlichen Stellen entsprechend der hessischen Verwaltungskostenordnung in Rechnung gestellt.

Entwicklung eines geeigneten Werkzeugs

Die oben beschriebenen Auswertungserfordernisse gelten sowohl für betroffene Verantwortliche oder Auftragsverarbeiter als auch im behördlichen Kontext bei der Bearbeitung von Meldungen, Beschwerden oder Hinweisen. Grundsätzlich sind in allen Anwendungsfällen die folgenden Tätigkeiten erforderlich:

– Es ist festzustellen, ob überhaupt personenbezogene Daten betroffen sind. Nur wenn dies der Fall ist, kann eine Pflicht zur Benachrichtigung

der betroffenen natürlichen Personen für die verantwortlichen Stellen bestehen, die aufsichtsbehördlich kontrolliert und bei Bedarf durchgesetzt werden muss. Dabei ist zu beachten, dass ein Angriff nicht notwendig dazu führen muss, dass auch personenbezogene Daten veröffentlicht werden. So kann ein Angriff auch ohne Offenlegung schon Mängel bei der Gewährleistung der Sicherheit der Verarbeitung mit Blick auf Art. 32 DS-GVO offenbaren.

– Es ist festzustellen, ob und wenn ja welche (weiteren) Stellen als Verantwortliche oder Auftragsverarbeiter von der Datenveröffentlichung betroffen sein könnten. Dann können auch im Zusammenhang mit einer gemeinsamen Verantwortung oder Auftragsverarbeitung weitere Stellen über den Vorfall zu informieren sein.
– Betroffene personenbezogene Daten und betroffene natürliche Personen sind nach Art und Umfang zu kategorisieren. Dies bildet die Grundlage für eine angemessene Risikobewertung. Dies ist sowohl für die Ermittlung des Schwellenwerts des hohen Risikos aus Art. 34 Abs. 1 DS-GVO relevant als auch für den Inhalt der notwendigen Benachrichtigung.

Vor allem die Identifikation und Kategorisierung betroffener Personen und personenbezogener Daten stellen sich häufig als äußerst aufwendig dar. Veröffentlichungen von Daten aus Angriffen liegen nahezu immer mindestens im Bereich mehrerer Gigabyte und reichen bis in den Terabyte-Bereich hinein. Diese Datenmengen verteilen sich üblicherweise auf viele zehntausende oder hunderttausende einzelne Dateien. Bei diesen Datenmengen ist eine manuelle inhaltliche Analyse nicht zu leisten. Daher ist eine Unterstützung durch geeignete Werkzeuge unerlässlich.

Solche spezialisierten Werkzeuge sind zwar am Markt verfügbar, in Anschaffung und Betrieb aber noch mit hohem Ressourcenaufwand verbunden. Für den behördlichen Einsatz habe ich daher den Ansatz gewählt, geeignete Werkzeuge selbst zu entwickeln. Dabei bin ich von zwei Annahmen ausgegangen, welche die Suche nach personenbezogenen Daten in großen unstrukturierten und heterogenen Datenmengen prägen sollten: Zum einen gibt es Datenkategorien, die einem festen, wohldefinierten Format streng folgen – wie die Rentenversicherungsnummer oder IBAN-Nummern. Zum anderen gibt es Datenkategorien, die keinem immer gleichen Format folgen – wie etwa die Namen von Personen. Für die Erkennung dieser Datenkategorien kann jedoch ein KI-basierter Ansatz genutzt werden, der auf einer breiten Grundlage an Trainingsmaterial viele mögliche Ausprägungen von Datenkategorien erkennen können sollte.

Für die Entwicklung des Werkzeugs „pbD-Toolkit“ („pbD“ als Abkürzung für „personenbezogene Daten“) folgte ich den folgenden nicht-funktionalen Anforderungen und Rahmenbedingungen:

– Wegen der guten Vergleichbarkeit der Anwendungsfälle soll das Werkzeug grundsätzlich auch für Verantwortliche und Auftragsverarbeiter nutzbar sein, die dies wünschen.
– Außerdem tausche ich mich seit einiger Zeit vertiefend mit anderen Datenschutzaufsichtsbehörden zu Themen der IT-Labore aus (siehe Kap. 16.6). Auch diesen Aufsichtsbehörden will ich eine Nutzung ermöglichen.
– Die Weitergabe des Werkzeugs soll als Veröffentlichung unter einer geeigneten Open Source-Lizenz erfolgen. Dadurch kann sichergestellt werden, dass Verbesserungen langfristig einem möglichst großen Nutzerkreis zugutekommen.
– Die Voraussetzungen für die Umgebung, in der ein solches Werkzeug eingesetzt werden kann, sollten niedrigschwellig sein. Die Verwendung einer weit verbreiteten Programmiersprache in Verbindung mit einigen wenigen Drittanbieter-Abhängigkeiten sollte dies positiv unterstützen.
– Der Anwenderkreis sollte aus technisch versierten Personen bestehen, eine benutzerfreundliche Bedienoberfläche also nachrangig sein.
– Jeder Verwender lässt die von dem Werkzeug gelieferten Ergebnisse durch einen Menschen kontrollieren und verwendet diese nicht für eine (automatisierte) Entscheidungsfindung. Ein KI-gestützter Ansatz könnte möglicherweise Ergebnisse liefern, die nicht in jedem Fall korrekt sind. Umgekehrt bedeutet dies aber auch, dass bei der Umsetzung eine gewisse Toleranz für falsch-negative und falsch-positive Ergebnisse in Kauf genommen werden kann.

Das pbD-Toolkit wurde ausgehend von den o. g. Anforderungen in der Programmiersprache Python programmiert. Es unterstützt zwei Verfahren für die Erkennung von personenbezogenen Daten. Zum einen werden reguläre Ausdrücke zur Erkennung gleichbleibender Muster verwendet. Zum anderen kommt ein KI-basierter Ansatz auf Basis eines Transformer-Encoder-Modells zur Entdeckung musterfreier Daten (z. B. von Namen von Personen in allen möglichen Formen) zum Einsatz. Ausgehend von einem eingegebenen Stammverzeichnis wird eine Ordnerstruktur dateiweise durchsucht. Von unterstützten Dateitypen können die Inhalte mit beiden Verfahren analysiert werden. Hinweise auf potenziell erkannte personenbezogene Daten werden in eine Ergebnisliste geschrieben, die im Anschluss manuell ausgewertet und überprüft werden kann. Zu den erkannten Datenkategorien gehören z. B. IBAN- und Rentenversicherungsnummern (Erkennung mittels regulärer Ausdrücke) sowie Namen und Ortsangaben (Erkennung mittels KI-Modell).

Eine kritische Auseinandersetzung mit den Ergebnissen ist unerlässlich. Das Werkzeug kann aber wertvolle Hinweise darauf liefern, an welchen Stellen in der Gesamtdatenmenge personenbezogene Daten auffindbar sein könnten.

Das pbD-Toolkit habe ich auf der Plattform opencode.de des Zentrums für Digitale Souveränität der Öffentlichen Verwaltung GmbH (ZenDiS) unter der Open Source-Lizenz „EU Public License“ veröffentlicht (https://datenschutz.hessen.de/presse/hbdi-veroeffentlicht-programmcode-auf-opencodede). Ich freue mich, dass das erste Feedback auf diese Veröffentlichung bislang positiv war, und bin gespannt, welche Beiträge oder Erfahrungswerte mich zu dieser Form der behördlichen Arbeit oder auch zu diesem konkreten Projekt noch erreichen werden.

Fazit

Kommt es zur Verletzung der Vertraulichkeit von personenbezogenen Daten durch eine unberechtigte Veröffentlichung, so kann dies zu schwerwiegenden Folgen für die betroffenen Personen führen, insbesondere auch zu einem vollständigen Kontrollverlust. Oftmals kann nicht nachvollzogen werden, welche Akteure zu welchen Zwecken Kopien der veröffentlichten Daten erstellt haben. Besonders bei illegalen Veröffentlichungen im Darknet sind die Möglichkeiten zu einer Einflussnahme auf diese sehr beschränkt. Daher ist es überaus wichtig, dass betroffene natürliche Personen unverzüglich und vollständig von den verantwortlichen Stellen benachrichtigt und über die möglichen Folgen aufgeklärt werden. Rechtzeitig empfohlene Maßnahmen können dazu beitragen, mögliche negative Folgen zu reduzieren oder ggf. auch auszuschließen.

Um die betroffenen natürlichen Personen benachrichtigen zu können, ist es oftmals notwendig, diese und deren betroffene Daten zuerst zu identifizieren. Bei großen unstrukturierten Datenmengen können geeignete Werkzeuge hilfreich sein. Meine Behörde hat daher mit der Entwicklung entsprechender Werkzeuge begonnen. Diese stelle ich der Allgemeinheit quelloffen zur Verfügung und fordere dem Open Source-Gedanken folgend dazu auf, die weitere Entwicklung zu unterstützen.

16.5
Webseiten-Check für Vereine

In einem Pilotprojekt habe ich Vereinen einen kostenlosen, freiwilligen „Webseiten-Check“ angeboten. Ausgewählte Vereine in Hessen konnten sich anmelden und in der Folge eine Rückmeldung dazu erhalten, ob bestimmte Aspekte der Verbindungsverschlüsselung ihrer Webseiten den datenschutz-

rechtlichen Anforderungen entsprachen. Wo dies nicht der Fall war, habe ich dem jeweils betroffenen Verein Umsetzungshinweise gegeben, um ihn bei der datenschutzkonformen Gestaltung seiner Webseite zu unterstützen.

Hintergrund

Die Umsetzung der gleichen datenschutzrechtlichen Pflichten kann für unterschiedliche Verantwortliche abhängig von den konkreten Rahmenbedingungen verschieden ausfallen. So hat ein kleiner Verein in der Regel weniger Ressourcen für ihre Umsetzung als ein großes Unternehmen und muss dabei meist vollständig auf ehrenamtliche Strukturen setzen. Bei dem Verein könnte aber auch die Verarbeitung personenbezogener Daten so ausfallen, dass ein geringeres Risiko für einen kleineren Personenkreis besteht. Die DS-GVO bietet mir die Möglichkeit, solche Unterschiede zu berücksichtigen. Um Vereine bei der datenschutzfreundlichen Gestaltung ihrer Angebote zu unterstützen, habe ich im Berichtsjahr daher das Pilotprojekt „Webseiten-Check“ ins Leben gerufen.

Angebot an Vereine

Hierbei habe ich ausgewählten Vereinen angeboten, dass sie auf freiwilliger Grundlage ihre Vereins-Webseiten einer technischen Überprüfung unterziehen lassen können. Webseiten habe ich hierbei als Gegenstand der Überprüfung ausgewählt, da Werkzeuge existieren, mit denen sich einfach und automatisiert Erkenntnisse zu ihnen gewinnen lassen (s. 53. Tätigkeitsbericht, Kap. 14.5, „Einsatz neuer Prüftools zur technischen Prüfung von Websites“). Die Möglichkeit zur Automatisierung erlaubt es mir, das Angebot künftig ggf. ohne größeren Aufwand auf einen größeren Teilnehmerkreis auszudehnen.

Bei der Überprüfung wurden drei Aspekte betrachtet, die bei der Verarbeitung personenbezogener Daten mittels einer Webseite relevant sein können:

1. Personenbezogene Daten dürfen nicht unverschlüsselt übermittelt werden. Es muss also mindestens eine sog. Verbindungsverschlüsselung zur Anwendung kommen. Ein Server, der den Versuch eines unverschlüsselten Verbindungsaufbaus identifiziert, muss entweder eine verschlüsselte Weiterleitung erzwingen oder die unverschlüsselte Kommunikation ablehnen.
2. Diese Verbindungsverschlüsselung muss aktuellen Sicherheitserfordernissen genügen. Die Serverkonfiguration muss so angepasst werden, dass niemals eine TLS-Version älter als 1.2 unterstützt wird.
3. Die Verbindungsverschlüsselung darf sich auch nicht einfach umgehen oder in ihrem Sicherheitsniveau abschwächen lassen.

Diese Prüfungspunkte kann ich in meinem IT-Labor entweder für einzelne Webseiten oder für eine größere Liste von Webseiten nacheinander automatisiert abarbeiten lassen. Die daran angeschlossene Berichterstellung zeigt mir für jede Webseite auf, bei welchen Punkten es ggf. Probleme bzw. Verbesserungsbedarf gibt.

Angebot an Vereine

Über die Landesstiftung „Miteinander in Hessen“ habe ich denjenigen Vereinen, die dort an dem Projekt „Verein.fachen“ zur Entbürokratisierung im Ehrenamt teilnehmen, angeboten, an dem Webseiten-Check teilzunehmen. Sechs Vereine haben sich daraufhin gemeldet. Es handelte sich durchweg um kleine und ehrenamtlich geführte Vereine, die für eine solche unbürokratische Einschätzung des Datenschutzes sehr dankbar waren, darunter bspw. ein Turnverein und ein Oldtimer-Verein.

Die Überprüfung der drei obengenannten Punkte habe ich dann in meinem IT-Labor durchgeführt und die jeweiligen Ergebnisse in separaten Anschreiben für die einzelnen Vereine individuell zusammengefasst. Die folgende Auflistung zeigt, dass fünf der sechs geprüften Vereinswebsites Verbesserungsbedarf bezüglich der aufgeführten Prüfpunkte aufwiesen:

	keine Probleme	bei einem Punkt	bei zwei Punkten	bei allen drei Punkten
Anzahl der Vereine	1	3	1	1

In dem Ergebnisschreiben an die Vereine habe ich zu jedem der drei Prüfungspunkte erläutert, warum dieser von Bedeutung ist, und einen jeweils dazu passenden Umsetzungshinweis auf meiner Website verlinkt. Förmliche Anweisungen oder gar Geldbußen waren bei diesem Vorgehen nicht das Ziel und daher auch nicht angedacht. Stattdessen sollten die Umsetzungshinweise die Vereine dabei unterstützen, etwaige datenschutzrechtlich relevante Probleme zu erkennen und zu beheben. Wie genau sie dies erreichen können, kommt auf die jeweils eingesetzte technische Umgebung an, in der die Websites betrieben werden. Nach meiner Erfahrung greifen Vereine wie diejenigen, die an dem Projekt teilgenommen haben, zur Gestaltung ihrer Websites gerne auf Webhosting-Unternehmen zurück. Dabei hat fast jedes dieser Unternehmen eine eigene Logik dafür, wie es die relevanten Konfigurationen für die Verschlüsselung möglich macht. Deshalb habe ich eine Liste verbreiteter Webhosting-Unternehmen zusammengestellt und für

jedes dieser Unternehmen die dazugehörigen Anleitungen und Hilfeseiten zur Umsetzung einer datenschutzkonformen Verschlüsselung verlinkt. Da diese Umsetzungshinweise grundsätzlich auch für andere Stellen als nur die teilnehmenden Vereine interessant sein können, sind diese Seiten auf meinem Webauftritt öffentlich und unter der Einstiegsseite https://datenschutz.hessen.de/datenschutz/vereine/umsetzungshinweise-zur-transportverschluesselung-von-webseiten/verschluesselungsverfahren-entsprechend-dem-stand-der-technik erreichbar.

Da ich das Angebot des Webseiten-Checks als gute und niederschwellige Option gerade für kleine verantwortliche Stellen begreife, die nicht auf die entsprechenden IT-Spezialisten zurückgreifen können, möchte ich es in Zukunft für weitere interessierte Stellen öffnen. Die dazu verwendeten technischen Werkzeuge werde ich, soweit sie der eigenen Entwicklung meiner Behörde entstammen, als Open Source-Angebot veröffentlichen (s. Kap. 16.4).

Fazit

Das Ziel von Datenschutzüberprüfungen durch meine Behörde ist es immer festzustellen, ob die Vorgaben der Datenschutzgesetze eingehalten werden, und ggf. eine notwendige Verbesserung des Datenschutzniveaus zu erwirken. Das Pilotprojekt „Webseiten-Check“ zeigt, dass gerade kleine (ehrenamtlich geführte) verantwortliche Stellen Probleme damit haben können, einfache Vorgaben des Datenschutzes umzusetzen. Ich möchte auch zukünftig diese verantwortlichen Stellen bei ihren Aufgaben unterstützen und plane, den Webseiten-Check weiteren ehrenamtlich geführten verantwortlichen Stellen in Hessen anzubieten.

16.6
Dritter Informationsaustausch der IT-Labore der Datenschutzbehörden

IT-Labore sind ein wichtiges Werkzeug der Datenschutzbehörden zur Ausführung ihrer gesetzlichen Aufgaben im Bereich des technischen und organisatorischen Datenschutzes. Der Austausch zwischen den Behörden über die IT-Labore ermöglicht das Erarbeiten von Best Practices und das gegenseitige Teilen von Erfahrungen. Im Berichtsjahr habe ich daher einen solchen Austausch veranstaltet.

IT-Labore als Gegenstand zwischenbehördlichen Austauschs

Zu meinen Aufgaben gehört das Nachvollziehen und Überprüfen schwerpunktmäßig technisch geprägter Verarbeitungen, ggf. inkl. einer gerichtsfesten Erhebung von Beweismitteln, sei es um

– Beschwerden oder Hinweisen nachzugehen,
– Meldungen gemäß Art. 33 DS-GVO angemessen zu bearbeiten oder
– Beratungen auf der Grundlage eigener Erkenntnisse durchzuführen.

Aus diesem Grund betreibe ich ein IT-Labor, das ich mit den entsprechenden technischen und personellen Ressourcen ausgestattet und organisatorisch in meiner Behörde verankert habe (s. 51. Tätigkeitsbericht, Kap. 17.1). Da es überwiegend bei der Bearbeitung von Beschwerden und Hinweisen auf mögliche Datenschutzverstöße genutzt wird, habe ich es im Referat für technische und organisatorische Datenschutzprüfungen angesiedelt (s. 52. Tätigkeitsbericht, Kap. 14.3). Hier werden anlassbezogen auch eigene Prüfwerkzeuge entwickelt (s. Kap. 16.4 und 5).

Da alle Datenschutzaufsichtsbehörden solche Aufgaben haben, hat sich die Idee eines IT-Labors durchgesetzt. Unterschiede gibt es jeweils bei der konkreten Ausgestaltung, da jede Behörde entsprechend ihrer lokalen Rahmenbedingungen und Bedürfnisse vorgeht. Je nach Anforderung und konkreter Aufgabenstellung im Einzelfall werden mitunter auch andere Werkzeuge in Form von Hardware und Software zur Aufgabenerfüllung gewählt. Die gemeinsame Ausgangslage der Behörden ermöglicht es jedoch, die unterschiedlichen Ansätze zu vergleichen. Hierbei können diejenigen Ansätze identifiziert werden, die besonders gut geeignet sind und vielleicht sogar von anderen Behörden übernommen werden können.

Aus diesem Grund haben die deutschsprachigen Datenschutzaufsichtsbehörden im Jahr 2024 begonnen, sich auf regelmäßigen Präsenzveranstaltungen zu Themen und Fragestellungen ihrer IT-Labore untereinander auszutauschen. Die ersten beiden Veranstaltungen in Bonn und Berlin waren den Schwerpunktthemen „Internet of Things“ (IoT) und „mobile Anwendungen“ (Apps) gewidmet.

Im Berichtszeitraum habe ich die anderen IT-Labore zu einer Austauschveranstaltung mit dem Schwerpunktthema „Webseiten-Prüfung“ in meine Dienststelle eingeladen. Hierzu kamen vom 12.–14. Mai 2025 insgesamt 30 Teilnehmerinnen und Teilnehmer in meiner Dienststelle zusammen, um sich zu ihren Vorgehensweisen bei diesem und weiteren Themen auszutauschen. Darunter waren neben den staatlichen auch spezifische Datenschutzbehörden vertreten, etwa aus dem Bereich der kirchlichen Datenschutzaufsicht.

Themen des gemeinsamen Austauschs

Ein technischer Prüfauftrag, der nahezu alle Aufsichtsbehörden regelmäßig beschäftigt, ist die Prüfung von Webseiten auf Verstöße gegen die Datenschutzgesetze. Dies beinhaltet vielfältige Fragestellungen mit Blick auf die Vorgaben der DS-GVO. Beispiele hierfür sind die Übermittlung personenbezogener Daten an Drittländer oder die gesetzmäßige Berücksichtigung von Einwilligungen betroffener Personen über Consent Banner. Auch § 25 TDDDG kann im Rahmen des Speicherns von Informationen auf Endeinrichtungen (etwa in Form von Cookies) einschlägig sein. Daher war dies ein zentraler Themenblock der Veranstaltung.

Im Austausch der Teilnehmerinnen und Teilnehmer zeigte sich, dass die zur Anwendung kommenden Prüf-Tools und -Verfahren sich teils deutlich voneinander unterschieden. Die Bandbreite reichte dabei von der ausschließlichen Verwendung heute standardmäßig in Webbrowsern integrierter Analysefunktionen bis hin zu einer automatisierten und werkzeuggestützten Überprüfung mittels des Website Evidence Collectors (WEC) oder anderer Anwendungen. Der WEC wird vom Europäischen Datenschutzbeauftragten als Open Source-Tool veröffentlicht (s. https://www.edps.europa.eu/edps-inspection-software_de) und kommt bei mehreren Aufsichtsbehörden zum Einsatz. Auch andere Behörden haben selbstentwickelte Tools in Verwendung, von denen einige im Rahmen der Veranstaltung demonstriert und besprochen werden konnten. Im Ergebnis des Austauschs haben einige Teilnehmerinnen und Teilnehmer Interesse daran bekundet, Tools anderer Behörden zu erproben und ggf. auch regelmäßig zu verwenden. Daher wurden diese Tools sodann über eine digitale Plattform miteinander geteilt.

Neben der Prüfung von Websites standen die Themenblöcke „Labor-Architektur“, „Automatisierung von Webseitenprüfungen“ und „Rechtsfragen technischer Datenschutzprüfungen“ auf der Agenda.

Im Austausch der Teilnehmenden im Rahmen des Themenblocks „Labor-Architektur“ zeigte sich, dass alle vertretenen Aufsichtsbehörden ein eigenes IT-Labor entweder bereits betreiben, gerade aufbauen oder dessen Aufbau zumindest planen. Um die eingangs genannten Ziele erreichen zu können, muss ein IT-Labor über entsprechende Prüfmittel verfügen, sowohl hinsichtlich Hardware (Testgeräte wie z. B. Smartphones) als auch Software (Prüftools). Ein kritischer Punkt, der sich bei der Einrichtung von IT-Laboren in den Aufsichtsbehörden herausgestellt hat, ist die Abtrennung der Prüfmittel des IT-Labors vom eigentlichen Behördennetzwerk. Diese ist zuallererst aus Gründen der Informationssicherheit zum Schutz des Behördennetzes erforderlich. Auf der anderen Seite wird so ermöglicht, dass das IT-Labor nicht den Einschränkungen des Behördennetzes unterliegt. Andernfalls

könnten nicht zuletzt auch Prüfergebnisse verfälscht werden, z. B. durch Internetfilter im Kontext von Website-Überprüfungen. Des Weiteren hat sich gezeigt, dass einige Aufsichtsbehörden in ihren IT-Laboren bereits mit virtualisierten Umgebungen arbeiten, um verschiedene Systemumgebungen für unterschiedliche Prüffälle automatisiert bereitstellen zu können. Dabei kommen u. a. Tools wie Proxmox oder Ansible zum Einsatz.

Am letzten Tag der Veranstaltung stand dann das Thema „Rechtsfragen technischer Prüfungen" im Fokus. Hierbei ergab sich eine spannende Diskussion, inwieweit der auch als „Hacker-Paragraph" bekannte § 202a StGB auf die Labor-Tätigkeiten der Aufsichtsbehörden anwendbar sei oder diese gar einschränke. Ganz überwiegend schlossen sich die Teilnehmerinnen und Teilnehmer der Auffassung an, dass dies nicht der Fall sei. Aufgrund ihrer gesetzlichen Aufgaben und Befugnisse bei dienstlich veranlasstem Tätigwerden werde niemals die Voraussetzung der Vorschrift hinsichtlich „unbefugten" Handelns erfüllt.

Die nachfolgende Veranstaltung zum Austausch der IT-Labore der deutschsprachigen Datenschutzaufsichtsbehörden wurde abschließend für Ende November 2025 terminiert. Dann wird der nächste Austausch auf Einladung der Landesbeauftragten für den Datenschutz Sachsen-Anhalts in Magdeburg stattfinden. Als Themenschwerpunkte wurden „Forensische Laborarbeit", „Hilfsmittel bei Laborprüfungen" und „Organisation des IT-Labors" festgelegt.

Ausblick

Der dritte Austausch der Datenschutzaufsichtsbehörden hat erneut gezeigt, dass ein breites Bewusstsein hinsichtlich der Notwendigkeit technischer Prüfmittel besteht und diese bei den Behörden kompetent angewendet und teilweise auch (weiter-)entwickelt werden. Besonders positiv ist mir bei diesem Austausch aufgefallen, dass die Behörden hier mit einem beachtlichen Maß an digitaler Souveränität agieren und die in Anwendung befindlichen Ressourcen selbst und ohne Abhängigkeit von großen Anbietern mit Sitz in Ländern ohne angemessenes Datenschutzniveau verwenden können. In gemeinsamen Diskussionen konnte eine Vielzahl an für teilnehmende Behörden relevanten Fragen erörtert werden. Auch konnten Informationen zu gut nutzbaren Werkzeugen untereinander geteilt werden. Schließlich konnten Behörden, die eigene Werkzeuge entwickelt haben, diese im Sinne eines „Einer für Alle"-Gedankens anderen zur Verfügung stellen, um ihnen ein effizienteres Arbeiten zu ermöglichen. Insgesamt war der dritte Informationsaustausch der IT-Labore der Datenschutzaufsichtsbehörden somit ein voller Erfolg.

16.7
Erstes abgeschlossenes Akkreditierungsverfahren

Eine Zertifizierung gemäß Art. 42 DS-GVO ist ein wirksames Instrument, um die Einhaltung der Datenschutzvorschriften aus der DS-GVO für eine bestimmte Verarbeitungstätigkeit nachweisen zu können. Im Berichtszeitraum habe ich das erste hessische Unternehmen akkreditiert, das nun solche Zertifizierungen vornehmen darf.

Sinn und Zweck einer Zertifizierung

Kommt es zu Datenschutzbeschwerden, ist häufig eine aufwändige Prüfung erforderlich – sowohl durch den Verantwortlichen, der seine internen Abläufe überprüft, als auch durch mich als Aufsichtsbehörde. Ziel ist es festzustellen, ob bei der betreffenden Verarbeitungstätigkeit die Vorgaben der DS-GVO tatsächlich eingehalten wurden. Verantwortliche Stellen und Auftragsverarbeiter möchten idealerweise schon vor einer solchen Überprüfung durch mich Gewissheit darüber haben, dass sie die Vorgaben der Verordnung derart erfüllen, dass aller Voraussicht nach von aufsichtsbehördlicher Seite aus keine Beanstandungen bestehen werden. Auch die betroffenen Personen wünschen sich Transparenz und ein Zeichen dafür, dass ihre Daten voraussichtlich datenschutzrechtskonform verarbeitet werden. In beiden Fällen bietet die DS-GVO in Art. 42 einen Mechanismus: die Zertifizierung**.** Sie kann bestätigen, dass eine Verarbeitungstätigkeit voraussichtlich datenschutzkonform erfolgt. Auf diesen Artikel verweist die DS-GVO auch an anderen Stellen – etwa wenn es darum geht, eine umfangreiche Einzelfallprüfung einzelner Vorschriften durch die Vorlage eines entsprechenden Zertifikats abkürzen zu können. So kann eine zertifizierte Stelle gemäß Art. 32 Abs. 3 DS-GVO beispielsweise als einen Faktor auf ein solches Zertifikat verweisen, um nachzuweisen, dass sie die Sicherheit der Verarbeitung personenbezogener Daten gewährleistet, anstatt dass alle ergriffenen technischen und organisatorischen Maßnahmen im Detail geprüft werden müssen.

Eine Datenschutzzertifizierung nach Art. 42 DS-GVO bietet für alle Seiten erhebliche Vorteile:

1. Die betroffenen Personen können sich bei einer zertifizierten Verarbeitungstätigkeit darauf verlassen, dass diese vorab geprüft und für datenschutzrechtskonform befunden worden ist. Ihre Rechte und Freiheiten sind damit voraussichtlich gut geschützt.
2. Zertifizierte Stellen erhalten durch ein solches Zertifikat ein wertvolles Indiz, das ihnen eine gewisse rechtliche Sicherheit vermittelt. Insbeson-

dere können Verantwortliche bei der Auswahl von Auftragsverarbeitern eine Zertifizierung besonders berücksichtigen (z. B. im Cloud-Bereich).

3. Datenschutzaufsichtsbehörden können bei Vorhandensein eines Zertifikats ihre Überprüfungen noch gezielter und effizienter gestalten.

Da die Datenschutzzertifizierung ausdrücklich in Art. 42 DS-GVO verankert ist, ist sie die einzige Form der Zertifizierung, die diesen spezifischen datenschutzrechtlichen Mehrwert bieten kann. Zwar existieren am Markt auch andere Zertifizierungen, die Themen mit Datenschutzbezug aufgreifen. Die bekannten Zertifizierungen der ISO 2700X-Reihe treffen z. B. Aussagen zur IT-Sicherheit, was mit Blick auf die Anforderungen zur Sicherheit der Verarbeitung aus Art. 32 DS-GVO Berücksichtigung finden kann. Allerdings fußen diese Zertifizierungen nicht auf dem rechtlichen Fundament des Art. 42 DS-GVO und haben darüber hinaus auch eine andere Zielrichtung. Somit besitzen sie aus Sicht der Datenschutzaufsichtsbehörden nicht denselben Aussagewert. Sie können eine datenschutzrechtliche Prüfung daher auch nicht in gleichem Maße beschleunigen. Hinzu kommt, dass IT-Sicherheit und Datenschutz unterschiedliche Zielrichtungen verfolgen. Während die IT-Sicherheit in erster Linie dem Schutz der Systeme und Daten der datenverarbeitenden Institution dient, steht beim Datenschutz der Schutz der Rechte und Freiheiten der betroffenen Personen im Vordergrund.

Kriterienprüfung und Akkreditierung

Damit eine Datenschutzzertifizierung diese Wirkung entfalten kann, regelt Art. 43 DS-GVO, wer solche Zertifikate ausstellen darf und welche Anforderungen an die jeweilige Stelle bestehen. Es muss sich dabei um sogenannte Zertifizierungsstellen handeln, die zuvor selbst einer umfassenden Prüfung unterzogen worden sind, um sicherzustellen, dass ihre Bewertungen zur Datenschutzkonformität zuverlässig und nachvollziehbar sind und stets nach demselben Standard erfolgen. Im Falle der Zertifizierungsstellen wird dieser Prozess verbunden mit der daran anschließenden Genehmigung, Zertifikate ausstellen zu dürfen, als „Akkreditierung“ bezeichnet.

Für diese Akkreditierung sind in Deutschland die Datenschutzaufsichtsbehörden gemeinsam mit der Deutschen Akkreditierungsstelle GmbH (DAkkS) zuständig. Die DAkkS ist ein von der Bundesrepublik Deutschland beliehenes, also mit besonderen, hoheitlichen Rechten ausgestattetes Unternehmen, das in so vielfältigen Bereichen wie Verkehr, Ernährung oder Explosionsschutz für die Akkreditierung von Inspektions-, Prüf- und Zertifizierungsstellen allein zuständig ist. Im Bereich der Datenschutzzertifizierungen wird die DAkkS gemeinsam mit den Datenschutzaufsichtsbehörden tätig.

Die Akkreditierung orientiert sich in systematischer Hinsicht an der Norm DIN EN ISO/IEC 17065, welche die Arbeit von Zertifizierungsstellen für Produkte, Prozesse und Dienstleistungen normiert. Das Besondere an der Datenschutzzertifizierung gemäß Art. 42 DS-GVO ist dabei allerdings, dass es sich gerade nicht um eine Produktzertifizierung handelt. Ein solches Zertifikat kann also niemals bescheinigen, dass ein bestimmtes Produkt, wie z. B. eine Online-Anwendung, für sich genommen schon datenschutzrechtskonform ist. Gegenstand der Zertifizierung ist vielmehr die konkrete Verarbeitungstätigkeit, also in diesem Beispiel etwa der Einsatz dieser Online-Anwendung

– für die Verarbeitung bestimmter Kategorien personenbezogener Daten,
– zu bestimmten Zwecken,
– aufgrund bestimmter Rechtsgrundlagen,
– unter Umsetzung bestimmter technischer und organisatorischer Maßnahmen,
– mit bestimmten Prozessen zur Wahrung der Rechte betroffener Personen.

Die ISO-Norm wird durch Akkreditierungskriterien der Datenschutzkonferenz ergänzt – konkret die DSK-Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO i. V. m. DIN EN ISO/IEC 17065 (https://www.datenschutzkonferenz-online.de/media/ah/20201008_din17065_Ergaenzungen_deutsch_nach_opinion.pdf). Neben den Aspekten zur Arbeitsweise von Zertifizierungsstellen gemäß der Norm DIN EN ISO/IEC 17065 dient immer auch ein Zertifizierungsprogramm mit dazugehörigen Zertifizierungskriterien als Grundlage für eine Datenschutzzertifizierung. Im Gegensatz zur ISO-Norm sind Zertifizierungsprogramm und -kriterien spezifisch auf die Anforderungen des Datenschutzes zugeschnitten. Sie beschreiben, wie ein bestimmter Zertifizierungsgegenstand – eine Verarbeitung mit Cloud-Diensten, mit Lern-Apps oder eine generische Verarbeitung – geprüft werden muss, um eine datenschutzrechtliche Bewertung zu ermöglichen.

Bevor solche Programme verwendet werden dürfen, müssen auch sie von den Datenschutzaufsichtsbehörden und der DAkkS genehmigt werden. Dieser Abstimmungsprozess findet sogar auf der europäischen Ebene mit anderen Datenschutzaufsichtsbehörden der EU-Mitgliedsstaaten statt, damit sichergestellt ist, dass ein Datenschutzzertifikat überall im Geltungsbereich der DS-GVO denselben Aussagewert besitzt.

Erste abgeschlossene Akkreditierung in Hessen

In Hessen konnte ich die erste Akkreditierung einer Zertifizierungsstelle erfolgreich abschließen. Dabei handelt es sich um die PwC Certification Services GmbH mit Sitz in Frankfurt am Main. Das Unternehmen verwendet

den Zertifizierungskriterienkatalog „AUDITOR“ des Kompetenznetzwerks Trusted Cloud e. V. An der Erstellung dieses Kriterienkatalogs, den die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen im Jahr 2024 genehmigt hat, war ich persönlich beteiligt. Die Akkreditierung ist befristet bis zum 15. Mai 2030. Eine Reakkreditierung ist möglich. Damit die Zertifizierungen des Unternehmens langfristig aussagekräftig und vertrauenswürdig bleiben, schließt sich an die initiale Akkreditierung eine stetige Überwachung an, bei der wiederkehrend unterschiedliche Schwerpunkte auf ihre Tauglichkeit überprüft werden.

Ich freue mich, dass Anbieter von Cloud-Diensten nun die Möglichkeit haben, in Hessen eine Überprüfung von Verarbeitungstätigkeiten auf Datenschutzrechtskonformität vornehmen zu lassen. Ebenso profitieren betroffene Personen, die durch ein solches Zertifikat künftig leichter erkennen können, dass Dienste ihre Rechte und Freiheiten besonders wirksam schützen.

16.8
Meldungen zu Datenschutzverletzungen

Alle Verantwortlichen sind verpflichtet, mir Verletzungen des Datenschutzes zu melden. Auch wenn mit einem großen Dunkelfeld zu rechnen ist, geben diese Meldungen eine Übersicht über die Gefährdung des Grundrechts auf Datenschutz. Diese ist im Berichtszeitraum überdurchschnittlich gestiegen.

Überblick und Entwicklungen

Die Anzahl der Meldungen in Bezug auf Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO, § 65 BDSG i. V. m. § 500 StPO und § 60 HDSIG stieg im Berichtsjahr auf 2.730 und damit um 27,5 % im Vergleich zum Berichtsjahr 2024. Damit wurde erneut ein Höchststand seit Einführung der Meldepflicht nach Art. 33 DS-GVO erreicht und die Bearbeitung der Meldungen von Datenschutzverletzungen stellte weiterhin einen großen Anteil der täglichen Arbeit meiner Behörde dar.

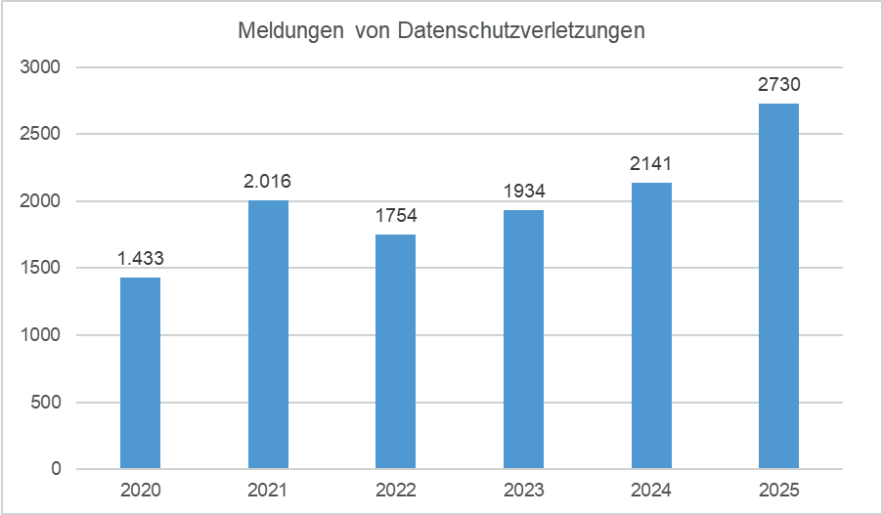


Abb. Entwicklung der Anzahl der Meldungen von Datenschutzverletzungen beim HBDI

Der Großteil der gemeldeten Datenschutzverletzungen war wiederholt auf Vorfälle von Fehlversand und falscher Zuordnung von Daten (1161) sowie auf Vorfälle im Rahmen von Cyberkriminalität (625 im Gegensatz zu 482 im Jahr 2024 = Anstieg um 30 %) zurückzuführen. Am stärksten betroffen waren auch im Jahr 2025 der Wirtschaftssektor einschließlich Kreditwirtschaft, Inkasso, Dienstleister, Handel und Gewerbe sowie die Bereiche Beschäftigtendatenschutz, Gesundheit und Pflege.

Neu im Berichtsjahr und daher auffällig waren vermehrte Meldungen unzulässiger Anfertigungen von Foto- und Videoaufnahmen aus den verschiedensten Bereichen. Teilweise wurden die Aufnahmen nach Anfertigung auf Social-Media-Plattformen veröffentlicht. Auch die unrechtmäßige Nutzung von KI-Software wurde vermehrt gemeldet. Um für diese beiden Bereiche einen genauen Überblick zu bekommen, wird die statistische Erfassung für das kommende Berichtsjahr angepasst.

Cyberangriffe auf Auftragsverarbeiter

Im Jahr 2025 gab es einen signifikanten Anstieg von Cyberangriffen auf Auftragsverarbeiter. Im Gesundheitsbereich gab es z. B. die Meldung eines großen Anbieters eines Antragsportals für Signatur- und Siegelkarten. Aber auch Auftragsverarbeiter im öffentlichen Bereich und im Bereich der Kommunen waren wieder betroffen.

Erfolgreiche Cyberangriffe auf Auftragsverarbeiter, die in der Regel im Auftrag mehrerer Verantwortlicher erhebliche Datenmengen verarbeiten, erreichen zwangsläufig ein großes Ausmaß und verursachen gravierende bereichs- und branchenübergreifende Schäden. Insbesondere Störungen im Betrieb von kritischen Dienstleistungen, hier im Bereich Gesundheit und Pflege, könnten die Versorgungssicherheit der Bürgerinnen und Bürger gefährden.

Auch im Berichtsjahr stellten die Auftragsverarbeiter wieder Listen mit betroffenen Verantwortlichen zur Verfügung. Wie bereits in den letzten Jahren konnte in diesem Jahr wieder festgestellt werden, dass Verantwortliche teilweise keine Meldungen abgeben. Nach Auswertung und Bewertung der Vorfälle wurden diese in einigen Fällen von mir angeschrieben und auf ihre Berichtspflicht hingewiesen.

Im Rahmen der Bearbeitung der Meldungen stand auch die Zusammenarbeit der deutschen Datenschutzaufsichtsbehörden wieder im Mittelpunkt. Sie mussten erneut Fragen der Zuständigkeit sowie des Informationsflusses gemeinsam klären. Darüber hinaus stellen Angriffe auf Auftragsverarbeiter aufgrund ihrer Komplexität und ihrer länderübergreifenden Auswirkungen für alle Beteiligten bei der Bewältigung und Aufarbeitung der Vorfälle besondere Herausforderungen dar. Die Zusammenarbeit war jedoch auch in diesem Berichtsjahr einwandfrei, zielgerichtet und konstruktiv. Möglichkeiten, die Effektivität zu steigern, wurden besprochen. In diesem Rahmen rückte neben den Rollen und Pflichten der für verantwortliche Stellen tätigen Auftragsverarbeiter auch die Diskussion über ein vereinfachtes Meldeverfahren (z. B. die Zulässigkeit der Meldung direkt durch den Auftragsverarbeiter unter Nennung aller betroffenen Verantwortlichen) wieder verstärkt in den Fokus.

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 entsprechend den datenschutzrechtlichen Anforderungen.

Mit Blick auf die Cyberangriffe gerade auf Auftragsverarbeiter ist es jedoch so, dass 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 oder eindämmen und Meldepflichten einhalten.

16.9
Ransomware Angriffe auf Pflegeeinrichtungen

Etwa 2.400 Pflegeeinrichtungen (1.367 ambulante und 1.095 stationäre Einrichtungen) decken allein in Hessen den gesellschaftlich und individuell wichtigen Bereich der Pflege ab (Hessisches Statistisches Landesamt, Statistischer Bericht, Kennziffer: K VIII 1 – 2j/2023, Die Pflegeeinrichtungen in Hessen am 15. Dezember 2023, Januar 2025, https://statistik.hessen.de/sites/statistik.hessen.de/files/2025-02/kviii1_2j23.pdf). Jede einzelne Pflegeeinrichtung verarbeitet zur Erfüllung dieser Aufgabe eine Vielzahl unterschiedlicher, besonders geschützter personenbezogener Daten. Dabei handelt es sich auch um besondere personenbezogene Daten nach Art. 9 DS-GVO. Diese Daten sind nicht nur für die Pflege und Betreuung notwendig, sondern wecken auch das Interesse von Cyberkriminellen. Tatsächlich wurden mir im vergangenen Berichtszeitraum gleich mehrere Fälle von Ransomware-Angriffen auf diesen Bereich der sozialen Infrastruktur Hessens nach Art. 33 DS-GVO gemeldet.

Ransomware-Angriffe

Bei der Umsetzung technischer und organisatorischer Maßnahmen zum Schutz vor Ransomware-Angriffen sowie bei der Prävention und Aufarbeitung solcher Angriffe stehen Pflegeeinrichtungen vor Herausforderungen, die hauptsächlich auf begrenzte Ressourcen zurückzuführen sind. Die im Berichtszeitraum eingegangenen Meldungen nach Art. 33 DS-GVO zeigen, dass es die zuvor geschilderte Situation insbesondere kleinerer Pflegeeinrichtungen nicht leicht macht, sich entsprechend zu schützen.

Ransomware-Angriffe verlaufen häufig nach dem folgenden wiederkehrenden Muster: Die Angreifer dringen über das Internet in die IT-Infrastruktur von Pflegeeinrichtungen ein, exfiltrieren deren Daten und verschlüsseln daraufhin die auf den genutzten IT-Systemen befindlichen Daten. Anschließend erpressen die Angreifer die Pflegeeinrichtungen, indem sie ein Lösegeld für die Entschlüsselung der ansonsten unbrauchbaren Daten verlangen. Zusätzlich drohen sie damit, die Daten im sogenannten Darknet zu veröffentlichen, sollte die Zahlung ausbleiben. Ein solches Vorgehen wird auch als „Double Extortion“ bezeichnet. Weitergehende Informationen zu Ransomware-Angriffen finden sich im 50. Tätigkeitsbericht, Kap. 18.2. (https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-08/50_taetigkeitsbericht_01_0.pdf).

Beispiel eines gelungenen Angriffs

Erste Anzeichen für einen Ransomware-Angriff auf den Pflegedienst (Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO) ergaben sich, als Pflegedienstmitarbeiter während ihrer Tätigkeit feststellten, dass sie nicht mehr auf Daten einer zentralen Anwendung zugreifen konnten. Nachdem der interne IT-Betrieb des Verantwortlichen einen Ransomware-Angriff als Ursache erkannt hatte, reagierte er schrittweise und aufeinander aufbauend auf den Angriff, um mögliche Risiken für die persönlichen Rechte und Freiheiten der Betroffenen zu minimieren oder zu beheben. Hierzu wurde externe Expertise hinzugezogen, darunter der ehemalige IT-Dienstleister und ein IT-Forensiker. Letzterer wurde über die vom Verantwortlichen benachrichtigte Versicherung eingebunden. Der Vorfall wurde bei der Polizei angezeigt und mir gemäß Art. 33 Abs. 1 DS-GVO gemeldet.

Die Analyse des Angriffs ergab, dass der Angreifer alle Daten des Pflegedienstes verschlüsselt und damit unbenutzbar gemacht hatte. Betroffen war auch das Backup der Daten, da dieses räumlich, nicht aber netzwerktechnisch von den betroffenen Systemen getrennt war. Der IT-Forensik-Bericht konnte bei einigen vom Pflegedienst betriebenen IT-Systemen und -Diensten nicht sicher klären, ob zum Zeitpunkt des Ransomware-Angriffs alle sicherheitsrelevanten Updates eingespielt waren. Dadurch konnte nicht ausgeschlossen werden, dass eine oder mehrere ungepatchte Schwachstellen von Angreifern ausgenutzt worden waren und so zu dem gemeldeten Vorfall geführt hatten. Bei der Prüfung fiel außerdem auf, dass Software eingesetzt wurde, für die der reguläre Support durch den Hersteller oder Entwickler bereits eingestellt worden war oder für die ein erweiterter Support individuell hätte erworben werden müssen. Überprüft wurde, ob ein Risiko oder ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen entstanden ist. Die Überprüfung kam zu dem Ergebnis, dass ein hohes Risiko vorlag. Dementsprechend wurden auch die betroffenen Personen gemäß Art. 34 Abs. 1 DS-GVO informiert.

Um die Auswirkungen des Vorfalls zu bekämpfen und mögliche Risiken zu minimieren oder zu beheben, wurden verschiedene Maßnahmen ergriffen. Dazu gehörte u. a. die Rekonstruktion von Daten aus Papierquellen sowie von den Mobilgeräten der Pflegekräfte.

Technisch-organisatorischer Maßnahmen zur Vorbeugung

Um sich zukünftig besser zu schützen und die Wahrscheinlichkeit eines erneuten Datenschutzvorfalls so gering wie möglich zu halten, hat der Verantwortliche eine Reihe technischer und organisatorischer Maßnahmen (TOM) ergriffen. Auf einige ausgewählte Maßnahmen werde ich im Folgenden kurz eingehen.

Um zu verhindern, dass sich mögliche Angreifer zukünftig frei im Netz bewegen können, wurde die zuvor flache Netzarchitektur neu segmentiert. Das Netzwerk wurde mithilfe einer zentralen Firewall in mehrere getrennte Teilnetze aufgeteilt. Die IT-Systeme und -Dienstleistungen wurden entsprechend ihres Schutz- und Kommunikationsbedarfs den einzelnen Netzen zugeordnet.

Das Backup-Konzept des verwendeten Backupsystems wurde in einem eigenen Netzsegment untergebracht. Clients und andere Geräte können nun nicht mehr direkt darauf zugreifen. Zusätzlich wurde ein Offline-Backup eingerichtet, auf dem täglich von Montag bis Freitag die Daten auf externen Festplatten gesichert werden. Diese Festplatten werden getrennt vom Netz sicher verwahrt, so dass Ransomware die Daten auf den Offlinefestplatten nicht verschlüsseln kann und diese Daten im Fall eines erneuten Ransomware-Angriffs wiederhergestellt werden können (s. auch 51. Tätigkeitsbericht, Kap. 17.7, https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-04/51-taetigkeitsbericht-des-hbdi_0.pdf).

Das Patchmanagement wurde überarbeitet, so dass Patches und Updates der verwendeten Software schnellstmöglich eingespielt werden. Um den Einsatz nicht mehr vom Hersteller unterstützter Software zu verhindern, wird im Rahmen des Patchmanagements zukünftig auch auf vorhandenen Support oder erweiterten Support für die verwendete Software geprüft.

Auf den Systemen, die eine Mehr-Faktoren-Authentisierung (MFA) per Authenticator-App unterstützen, wurde diese eingerichtet. Alle über das Internet erreichbaren E-Mail-Konten sowie Konten von IT-Dienstleistungen wurden auch mit MFA per Authenticator-App abgesichert. Stärkere Authentisierungsmechanismen erschweren es Angreifern, ein Netz zu infiltrieren.

Der Verantwortliche hat die Einrichtung eines zentralen Protokollservers geplant. Vorausgesetzt, der Protokollserver ist ausreichend gesichert, stehen im Fall eines erneuten Angriffs wichtige Informationen zur Verfügung. Bei unzureichender Absicherung können diese Informationen allerdings durch den Angreifer manipuliert werden oder verlorengehen. Mithilfe der Informationen könnten Verantwortliche den Hergang eines Angriffs besser nachvollziehen. Hierauf aufbauend könnten sodann entstandene Risiken für die Rechte und Freiheiten der Betroffenen besser eingeschätzt und geeignete technische und organisatorische Maßnahmen ergriffen werden, um diese Risiken zu mindern.

Der Verantwortliche hat die Sensibilisierung der Beschäftigten für Datenschutz und Informationssicherheit in den Vordergrund gestellt, da diese einen weiteren Schutz gegen mögliche Angriffe bieten kann. Die Sensibilisierung von Beschäftigten für Datenschutz und Informationssicherheit ist eine wichtige Maßnahme, da sie auf eine Vielzahl möglicher Angriffe abzielt. Das Bewusstsein für die Risiken von Datenverstößen wird geschärft. Die

jährlichen Schulungen und Sensibilisierungsmaßnahmen sowie die jährliche Datenschutzschulung tragen dazu bei, Risiken für die Rechte und Freiheiten möglicher Betroffener zu erkennen und durch eigenes Handeln zu minimieren.

Die technischen und organisatorischen Maßnahmen im Hinblick auf Datenschutz und IT-Sicherheit werden zukünftig vom Datenschutzbeauftragten in Kooperation mit dem für die IT-Sicherheit Verantwortlichen im Zuge eines jährlichen Audits überprüft.

Rechtliche Einordnung

Pflegeheime sind als „Verantwortliche**“** im Sinne des Art. 4 Nr. 7 DS-GVO verpflichtet, die Einhaltung der Datenschutzbestimmungen sicherzustellen. Die relevanten Pflichten ergeben sich im Wesentlichen aus den folgenden Artikeln der Verordnung.

Die Einrichtung muss entsprechend den Grundsätzen der Verarbeitung gemäß Art. 5 Abs. 1 Buchst. f DS-GVO die Integrität und Vertraulichkeit der Daten gewährleisten. Dies beinhaltet den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung durch geeignete TOMs. Die Einrichtung trägt hierbei gemäß Art. 5 Abs. 2 DS-GVO die umfassende Rechenschaftspflicht.

Es sind dem Risiko angemessene TOMs zu treffen, um die Sicherheit der Verarbeitung personenbezogener Daten entsprechend Art. 32 DS-GVO zu gewährleisten. Diese müssen den Stand der Technik, die Implementierungskosten und die Art der Daten berücksichtigen. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere Risiken durch Vernichtung, Verlust oder unbefugten Zugang zu berücksichtigen.

Der Verantwortliche muss im Rahmen der Verarbeitung personenbezogener Daten gemäß Art. 24 DS-GVO in der Lage sein, die Einhaltung der Vorschriften nachzuweisen. Die Maßnahmen müssen kontinuierlich überprüft und aktualisiert werden.

Ein Ransomware-Angriff führt in der Regel zu einer „Verletzung des Schutzes personenbezogener Daten“ im Sinne von Art. 4 Nr. 12 DS-GVO und zieht weitreichende rechtliche Pflichten und Konsequenzen für die verantwortliche Einrichtung nach sich.

Der Verantwortliche ist verpflichtet, seiner Meldepflicht nach Art. 33 DS-GVO nachzukommen. Er muss die Datenschutzverletzung unverzüglich und, wenn möglich, binnen 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde melden. Dies kann nur unterbleiben, falls die Verletzung des Schutzes personenbezogener Daten nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfahrungsgemäß ist letzteres

bei Ransomware-Angriffen nur selten der Fall (s. auch EDSA Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_de.pdf).

Führt die Datenschutzverletzung voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen, müssen die Betroffenen entsprechend der Informationspflichten des Art. 34 DS-GVO ebenfalls unverzüglich informiert werden. Betroffene Personen können nicht nur die zu pflegenden Personen sein, sondern auch Mitarbeiter, ehemalige Mitarbeiter, Kunden, Angehörige usw. Der Umfang und Inhalt der Information ergibt sich aus Art. 34 Abs. 2 DS-GVO. Hinsichtlich der Form enthält die DS-GVO keine spezifischen Vorgaben (z. B. Brief oder E-Mail), betont jedoch die Unverzüglichkeit und Wirksamkeit der Kommunikation. Für die Informationspflicht des Einzelnen gibt es eine Reihe von Ausnahmen, wie sie in Art. 34 Abs. 3 DS-GVO aufgeführt sind. Durch den Zugriff und die Exfiltration personenbezogener Daten im Rahmen des Ransomware-Angriffs sind die in Art. 34 Abs. 2 Buchst. a und b DS-GVO aufgeführten Ausnahmen in vielen Fällen nicht anwendbar. Nur wenn die direkte Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde (z. B. bei einer sehr großen Anzahl Betroffener und fehlenden Kontaktdaten), kann eine öffentliche Bekanntmachung (z. B. auf der Website des Unternehmens oder in regionalen Medien) ausreichend sein. Es kann vorkommen, dass während der Aufarbeitung erkannt wird, dass das Risiko für die Betroffenen höher ist als ursprünglich eingeschätzt, z. B. weil weitere Kategorien von Daten betroffen sind als ursprünglich angenommen. In solchen Fällen ist eine nachträgliche Benachrichtigung der Betroffenen unverzüglich erforderlich.

Es ist ebenfalls wichtig, dass identifizierte Betroffene sofort benachrichtigt werden, auch wenn noch nicht alle Betroffenen ermittelt wurden. Ein möglicherweise längerer Analyseprozess darf nicht dazu führen, dass die bereits identifizierten Betroffenen nicht umgehend informiert werden. Nur durch eine frühzeitige Benachrichtigung können die Betroffenen schnellstmöglich Maßnahmen ergreifen, um sich vor weiteren Schäden zu schützen. Deshalb darf eine Benachrichtigung nicht auf die Schlussphase der Aufarbeitung verschoben werden.

Jede betroffene Person, der durch den Verstoß ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadensersatz gemäß Art. 82 DS-GVO gegen das Pflegeheim. Die Pflegeeinrichtung haftet als Verantwortlicher, es sei denn, sie kann nachweisen, dass sie in keinerlei Hinsicht für den schadenverursachenden Umstand verantwortlich ist. Diese Haftung stellt ein erhebliches finanzielles Risiko für die Pflegeeinrichtung dar.

Neben den datenschutzrechtlichen Konsequenzen kann ein erfolgreicher Ransomware-Angriff auch weitere gravierende Folgen haben, insbesondere wenn personenbezogene Daten von Bewohnern betroffen sind. Der mit einem Ransomware-Angriff einhergehende Verlust der Verfügbarkeit von IT-Systemen und -Dienstleistungen kann dazu führen, dass die Planung von Pflegerouten und die Verwaltung von Patientenakten (einschließlich Medikationsplänen und Diagnosen) erschwert oder unzugänglich wird. Diese Unterbrechung der Versorgung kann dazu führen, dass Termine abgesagt werden müssen, Pflegekräfte nicht wissen, welche Patienten sie besuchen sollen oder welche spezifische Pflege erforderlich ist, was damit die Patientensicherheit erheblich gefährdet.

Durch das Ausleiten von Daten vor der Verschlüsselung durch die Angreifer können Patientendaten nicht nur verschlüsselt, sondern auch gestohlen werden. Dies kann zu Identitätsdiebstahl, Finanzbetrug oder sogar Erpressung der Patienten selbst führen. Die Kosten für die Wiederherstellung der Systeme, mögliche Lösegeldzahlungen (die oft dennoch keine vollständige Datenwiederherstellung garantieren), die Behebung von Datenlecks, rechtliche Konsequenzen und Umsatzeinbußen können immens sein.

Fazit

Ransomware-Angriffe auf Pflegeeinrichtungen können schwerwiegende Folgen haben. Im vorliegenden Fall konnten glücklicherweise viele Daten, die sich auf nicht betroffenen mobilen Endgeräten wie Smartphones und Tablets sowie in Ordnerarchiven befanden, wiederhergestellt werden. Dies ist jedoch nicht die Regel. Deshalb müssen Pflegeeinrichtungen sicherstellen, dass sie angemessene technische und organisatorische Maßnahmen implementiert haben, um die Sicherheit der personenbezogenen Daten zu gewährleisten und die rechtlichen Anforderungen der DS-GVO zu erfüllen. Im Falle eines Angriffs ist eine schnelle und strukturierte Reaktion entscheidend, um die Auswirkungen zu minimieren. Verantwortliche sollten deshalb präventiv handeln, sowohl um sich vor Angriffen zu schützen als auch um im Falle eines Angriffs angemessen reagieren zu können. Die Liste der zuvor vorgestellten Maßnahmen ist keinesfalls abschließend und ausreichend, um sich umfassend gegen Ransomware-Angriffe abzusichern. Es handelt sich vielmehr um Beispiele aus der Praxis, die Orientierung geben können. Deshalb ist es wichtig, ein vollumfängliches Konzept zu verfolgen, das sowohl die datenschutzspezifischen als auch die aus der Informationssicherheit resultierenden Aspekte berücksichtigt. Dabei können eine Datenschutzfolgeabschätzung (DSK, Kurzpapier Nr. 5, Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO; https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.

pdf), die Abschätzung von Risiken (DSK; Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen; https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf) sowie das konzeptionelle und inhaltliche Know-how des IT-Grundschutzes (BSI, IT-Grundschutz; https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html) helfen, geeignete Maßnahmen zu identifizieren und umzusetzen.

16.10
Datenschutzvorfall bei einem Luftfahrtkonzern

Bei einem Cyberangriff auf einen Auftragsverarbeiter der Luftfahrtbranche wurden durch Angreifer Passagierdaten eines Luftfahrtkonzerns erbeutet. Die Identifikation und Benachrichtigung der betroffenen Personen gestaltete sich aufgrund fehlender Kontaktdaten der Betroffenen und einer anfänglich unzureichenden Kooperation durch den verantwortlichen Luftfahrtkonzern schwierig. Es zeigte sich bei der Benachrichtigung der Betroffenen, dass die vorherige Erfassung geeigneter Kontaktdaten hierfür essenziell ist.

Sicherheitsvorfall bei Auftragsverarbeiter

Durch ein Update eines aus dem Internet erreichbaren Anwendungsportals eines Auftragsverarbeiters zur Abwicklung von Hotelübernachtungen bei Flugausfällen für Passagierairlines entstand eine Schwachstelle. Diese resultierte aus versehentlich eingebetteten Anmeldedaten der Entwickler im veröffentlichten Quellcode des Anwendungsportals. Die offengelegten Anmeldedaten wurden von Angreifern bereits nach kurzer Zeit entdeckt. Sie konnten durch die Ausnutzung der Schwachstelle unberechtigten Zugriff auf das Backend des Anwendungsportals erlangen. Diesen Zugang nutzten sie über Monate hinweg, um sich lateral in der IT-Infrastruktur des Auftragsverarbeiters auszubreiten. Auf diese Weise gelang es den Angreifern, in eine IT-Anwendung einzudringen, in der u. a. personenbezogene Daten zu Flugausfällen und den zugehörigen Hotelaufenthalten der Passagiere gespeichert waren. Dadurch gelang es den Angreifern, die Daten von ca. 100.000 betroffenen Passagieren des Luftfahrtkonzerns über das Internet auszuleiten (Exfiltration). Um unerkannt zu bleiben, erfolgte die Exfiltration in mehreren Etappen. Trotzdem gelang es dem Auftragsverarbeiter, den Angriff zu erkennen und so die vorbereitete Exfiltration der Datensätze von ca. 1 Million weiteren Passagieren zu verhindern. Dies gelang dem Auftragsverarbeiter durch das Isolieren der betroffenen Teilnetze und eine Separierung der entsprechenden Datenbanken. Nachdem der Auftragsverarbeiter den Vorfall erkannt hatte, wurden die IT-Systeme gesichert und eine Untersuchung

eingeleitet, um die betroffenen Kundenairlines als verantwortliche Stellen zu ermitteln. Nachdem dies abgeschlossen war, wurde der Luftfahrtkonzern als Ziel der Angreifer vom Auftragsverarbeiter identifiziert und von diesem informiert. Die vom Luftfahrtkonzern und den zugehörigen Airlines selbst betriebene IT-Infrastruktur war durch den Angriff nicht betroffen.

Sachverhaltsaufklärung und Unterstützung

Nachdem der Auftragsverarbeiter den Luftfahrtkonzern über den Datenschutzvorfall informiert hatte, meldete mir dieser den Vorfall nach Art. 33 Abs. 1 DS-GVO. Eine Reihe von Informationen, wie z. B. Angaben zur Anzahl betroffener Personen und zu den Kategorien der betroffenen Daten, standen bei der Meldung noch nicht abschließend fest.

Zu diesem Zeitpunkt wurden sowohl durch den Luftfahrtkonzern als auch durch den Auftragsverarbeiter noch IT-forensische Untersuchungen durchgeführt. Deshalb war zur Klärung des Sachverhalts eine Reihe von Rückfragen notwendig, ohne deren Beantwortung eine Einschätzung des Risikos für die Rechte und Freiheiten der Betroffenen durch mich nicht möglich war.

Der Luftfahrtkonzern ließ jedoch mehrmals gesetzte Fristen zur Beantwortung der Rückfragen verstreichen, beantwortete Fragen teilweise nicht, hielt angefragte IT-forensische Untersuchungsberichte zurück und machte widersprüchliche Angaben. So wurde z. B. zunächst erklärt, dass kein Reisedatum der Passagiere in den betroffenen Datensätzen enthalten wäre. Auf meine Rückfragen hin stellte sich jedoch heraus, dass die Flugnummern zusammen mit dem Datum des Hotelaufenthalts erfasst und auch in den exfiltrierten Datensätzen enthalten waren. Auch wurde zunächst angegeben, dass nur die Daten von Passagieren für einen Zeitraum von zwei Monaten exfiltriert wurden. Erst auf Rückfragen wurde mitgeteilt, dass die Vorbereitungen zur Exfiltration der Daten durch die Angreifer innerhalb von zwei Monaten getroffen worden waren und Datensätze der Passagiere für einen Zeitraum von fünf Jahren exfiltriert wurden. Da die Nachmeldung zum Sachverhalt gemäß Art. 33 Abs. 4 DS-GVO durch den Luftfahrtkonzern nicht erfolgte, kam es zu weiteren Verzögerungen.

Die Sachverhaltsaufklärung erforderte auch den Abgleich der übermittelten IT-forensischen Berichte mit den zuvor von dem Verantwortlichen übermittelten Informationen. Entgegen der ursprünglichen Aussage des Luftfahrtkonzerns konnte z. B. durch die IT-forensische Analyse nicht belegt werden, dass nur Passagiere vom Vorfall betroffen waren, die von zwei bestimmten Flughäfen aus abgeflogen waren. Durch die Analyse stellte sich schließlich heraus, dass aus einem Zeitraum von fünf Jahren ca. 100.000 Passagiere internationaler Herkunft von den Verletzungen personenbezogener Daten betroffen waren.

Beteiligte, Verantwortlichkeiten und Pflichten

Passagierfluggesellschaften unterliegen regulatorisch unter anderem der EU-Fluggastrechteverordnung 261/2004. Diese sieht für Passagiere z. B. bei Flugausfällen einen von dem Airline-Konzern zu organisierenden Hotelaufenthalt vor, damit Passagiere bei Flugausfällen nicht über Nacht auf Flughäfen stranden.

Der geschilderte Vorfall ereignete sich bei einem internationalen Auftragsverarbeiter, der eine Vielzahl auch international tätiger Luftfahrtgesellschaften als Kunden hat. Daher waren mehrere Töchter des Airline-Konzerns vom Vorfall betroffen. Da der Luftfahrtkonzern seinen operativen Sitz in der EU hat, greifen hier die Melde- und Benachrichtigungspflichten der DS-GVO. Der Auftragsverarbeiter hat gemäß Art. 33 Abs. 2 DS-GVO die Pflicht, die Verantwortlichen unverzüglich über den Vorfall zu informieren und alle relevanten Informationen bereitzustellen (weitere Ausführungen zu den Pflichten der Auftragsverarbeiter finden sich im 51. Tätigkeitsbericht, Kap. 17.3).

Nachdem er Kenntnis vom Datenschutzvorfall erlangt hatte, meldete mir der Luftfahrtkonzern diesen gemäß Art. 33 Abs. 1 DS-GVO binnen 72 Stunden. Bei der weiteren Sachverhaltsaufklärung war der Luftfahrtkonzern gemäß Art. 31 DS-GVO zur Kooperation mit mir verpflichtet. Er hätte mir alle weiteren Informationen zum Datenschutzvorfall gemäß Art. 33 Abs. 4 DS-GVO nachmelden müssen. Auch wenn der Vorfall beim Auftragsverarbeiter stattfand, blieb der Luftfahrtkonzern als Verantwortlicher vollständig für die Einhaltung der für ihn geltenden gesetzlichen Vorgaben verantwortlich.

Zusätzlich hat ein Verantwortlicher gemäß Art. 34 Abs. 1 DS-GVO die Pflicht, die Betroffenen bei einem hohen Risiko für ihre Rechte und Freiheiten über den Datenschutzvorfall zu informieren. Dies muss unverzüglich erfolgen, damit die Betroffenen sich der für sie bestehenden Risiken bewusst sind und entsprechend reagieren können.

Bewertung des potenziellen Risikos

Vom Vorfall waren Daten betroffen, deren unbefugte Offenlegung zu hohen Risiken für die betroffenen Personen führte, etwa Identitätsdiebstahl, diskriminierende Rückschlüsse oder finanzielle Schäden. Beispielsweise ließ sich aus den Flugnummern und dem jeweiligen Datum auf die genutzte Flugverbindung schließen. Auch ließ sich aus den betroffenen Daten rekonstruieren, welche Personen zu welchem Zeitpunkt mit welchem Ziel verreist waren. Es war auch zu erkennen, welche Personen gemeinsam gereist waren. Verschärfend kam hinzu, dass aus den Datensätzen zu erkennen war, ob besonders vulnerable Personen wie Kleinkinder gereist waren. Beispielhaft wären im

Zusammenhang mit der Kontaktaufnahme durch Angreifer in betrügerischer Absicht Social-Engineering-Angriffe, Erpressung, Anrufe im Zusammenhang mit den Hotelaufenthalten oder Zahlungsaufforderungen möglich gewesen. Zusätzlich war zu berücksichtigen, dass die Daten mit weiteren, ggf. öffentlich zugänglichen Datenquellen abgeglichen werden könnten, was potenziellen Angreifern eine feinere Profilbildung ermöglichen würde.

Verstärkt wurden die zuvor beschriebenen Risiken dadurch, dass die exfiltrierten Datensätze den Zeitraum von Ende 2019 bis Anfang 2024 abdeckten. Das führte dazu, dass die Daten mancher Passagiere mehrfach von dem Datenschutzvorfall betroffen waren. Daraus resultierte ein höheres Risiko durch eine umfassendere Profilbildung und einen größeren Umfang personenbezogener Daten, die von Angreifern ausgenutzt werden konnten.

Diese Risikoeinschätzung wurde zunächst nicht vom Luftfahrtkonzern geteilt, so dass dieser entgegen meiner Einschätzung von keiner Benachrichtigungspflicht gemäß Art. 34 Abs. 1 DS-GVO ausging.

Benachrichtigung der Betroffenen

Aufgrund der grenzüberschreitenden Datenverarbeitung meldete der Airline-Konzern den Vorfall im sogenannten One-Stop-Shop-Verfahren gemäß Art. 56 DS-GVO ausschließlich an mich als federführende Aufsichtsbehörde. Da vom Datenschutzvorfall auch Passagiere aus dem europäischen Wirtschaftsraum betroffen waren, war vor dem Abschluss des Verfahrens eine informierende Konsultation der betroffenen Aufsichtsbehörden des EWR gemäß Art. 60 DS-GVO erforderlich. Diese wurden entsprechend durch mich informiert und die Konsultation konnte erfolgreich abgeschlossen werden.

Erst nach mehrmaligen Rückfragen und Empfehlungen sowie wiederholten Darstellungen meiner Einschätzung zur Benachrichtigungspflicht wurde vom Luftfahrtkonzern eine Benachrichtigung der betroffenen Passagiere per E-Mail durchgeführt. Bei dieser zeigte sich, dass nicht für alle betroffenen Passagiere eine E-Mail-Adresse bekannt war, da diese bis 2024 nicht bei allen Buchungen über Reiseportale angegeben werden musste. Auch waren nicht alle E-Mail-Adressen gültig. So konnten nur ca. 80.000 der ca. 100.000 Betroffenen per E-Mail benachrichtigt werden.

Da ca. 20.000 betroffene Passagiere nicht individuell informiert werden konnten, habe ich eine öffentliche Benachrichtigung empfohlen, um so möglichst viele Betroffene erreichen zu können. Die öffentliche Benachrichtigung erfolgte ebenfalls erst nach weiteren umfangreichen Interventionen meinerseits. So beabsichtigte der Luftfahrtkonzern zunächst, die öffentliche Benachrichtigung für seine Hauptmarke und die drei Tochterairlines über ein konzerneigenes

Fachanwenderportal für die Reiseverkehrsbranche umzusetzen. Dies stellte sich jedoch als nicht ausreichend heraus, da das Fachanwenderportal einen bestehenden Nutzeraccount erforderte und sich nicht an die betroffenen Passagiere, sondern an Mitarbeiter der Reiseverkehrsbranche richtete. Schließlich wurde vom Luftfahrtkonzern auf den jeweiligen Websites der vier betroffenen Fluggesellschaften eine öffentliche, mehrsprachige Benachrichtigung umgesetzt.

Im Zusammenhang mit der Erforderlichkeit der Erhebung und Nutzung von Kontaktdaten bei der Flugbuchung ist zu berücksichtigen, dass diese Informationen regelmäßig Bestandteil des sogenannten Passenger Name Record (PNR) sind. Der PNR stellt den zentralen Buchungsdatensatz im Luftverkehr dar und enthält sämtliche Informationen, die für die Durchführung des Beförderungsvertrags sowie für gesetzlich vorgeschriebene Abläufe im Luftverkehr erforderlich sind. Hierzu gehören neben den Reisedaten und organisatorischen Angaben insbesondere auch die vom Passagier bereitgestellten Kontaktinformationen wie z. B. die E-Mail-Adresse. Gleichzeitig bildet der PNR eine gute Grundlage dafür, betroffene Personen im Falle eines Datenschutzvorfalls gemäß Art. 34 Abs. 1 DS-GVO unverzüglich benachrichtigen zu können. Aufgrund eines fehlerhaften, bis 2024 genutzten Prozesses für Selbstbucher wurden in Reiseportalen die E-Mail-Adressen nicht verlässlich erfasst. Dies führte zu Problemen bei der individuellen Benachrichtigung der betroffenen Personen.

Durch den Verantwortlichen kam es zu wiederholten Überschreitungen der zur Sachverhaltsaufklärung gesetzten Fristen. Auch wurden inhaltlich widersprüchliche und teilweise fehlerhafte Angaben zum Sachverhalt gemacht sowie Informationen zurückgehalten. Hierdurch gestaltete sich die Bearbeitung des Vorfalls unnötig schwierig. Außerdem verzögerte sich die Benachrichtigung der Betroffenen.

Schlussfolgerung

Mit ca. 100.000 betroffenen Passagieren handelte es sich um einen bedeutenden Datenschutzvorfall bei einem europäischen Luftfahrtkonzern. Durch die Analyse der vorgelegten IT-forensischen Berichte sowie gezielte Rückfragen zur Sachverhaltsklärung und intensive Gespräche mit dem Verantwortlichen konnte letztlich die Benachrichtigung der betroffenen Passagiere erreicht werden. Dabei zeigte sich, wie wichtig verfügbare Kontaktdaten für alle Betroffenen sind. Diese sind notwendig, um mit vertretbarem Aufwand für den Verantwortlichen Betroffene individuell und schnell über potenziell hohe Risiken informieren zu können und nicht den Weg einer öffentlichen

Benachrichtigung gehen zu müssen. Im vorliegenden Fall war hierfür die E-Mail-Adresse der Betroffenen am besten geeignet.

Im aktuellen Fall besteht Anlass zu prüfen, ob gegen den Luftfahrtkonzern ein Verfahren zur Verhängung einer Geldbuße gemäß Art. 83 Abs. 2 DS-GVO einzuleiten ist. Ein möglicher Verstoß betrifft insbesondere Art. 31 DS-GVO, der den Verantwortlichen verpflichtet, mit der Aufsichtsbehörde zusammenzuarbeiten. Die Fristversäumnisse und die unzureichende Mitwirkung könnten als Verletzung dieser Mitwirkungspflicht zu bewerten sein.

16.11
Aufarbeitung und Prävention von Datenschutzvorfällen durch Phishing

Phishing kann mehrere Straftatbestände erfüllen (z. B. 202a, 202d, 263, 263a, 265, 303a und 303b StGB) und bedroht die Rechte und Freiheiten natürlicher Personen. Phishing-Angriffe nehmen immer mehr zu und erfolgen auf einem hohen Niveau. Dabei stehen insbesondere über das Internet zugängliche E-Mail-Konten und die damit verbundenen Plattformen im Fokus der Angreifer.

Beim Phishing, einer Form der Internetkriminalität, versuchen Angreifer, an vertrauliche Informationen wie z. B. Benutzernamen und Passwörter zu gelangen. Dies tun sie, indem sie sich als vertrauenswürdige Kommunikationspartner ausgeben. Mit Hilfe der dadurch erlangten Informationen verschaffen sich die Angreifer Zugriff auf personenbezogene Daten in über das Internet erreichbaren E-Mail-Konten. Dadurch kam es vielfach zu Verletzungen des Schutzes personenbezogener Daten gemäß Art. 4 Nr. 12 DS-GVO.

Ablauf eines Phishing-Angriffs

Im Folgenden beschreibe ich zur Verdeutlichung meiner Ausführungen exemplarisch einen vereinfachten Ablauf der Phishing-Angriffe, wie er sich mit Varianten in den eingegangenen Meldungen widerspiegelt.

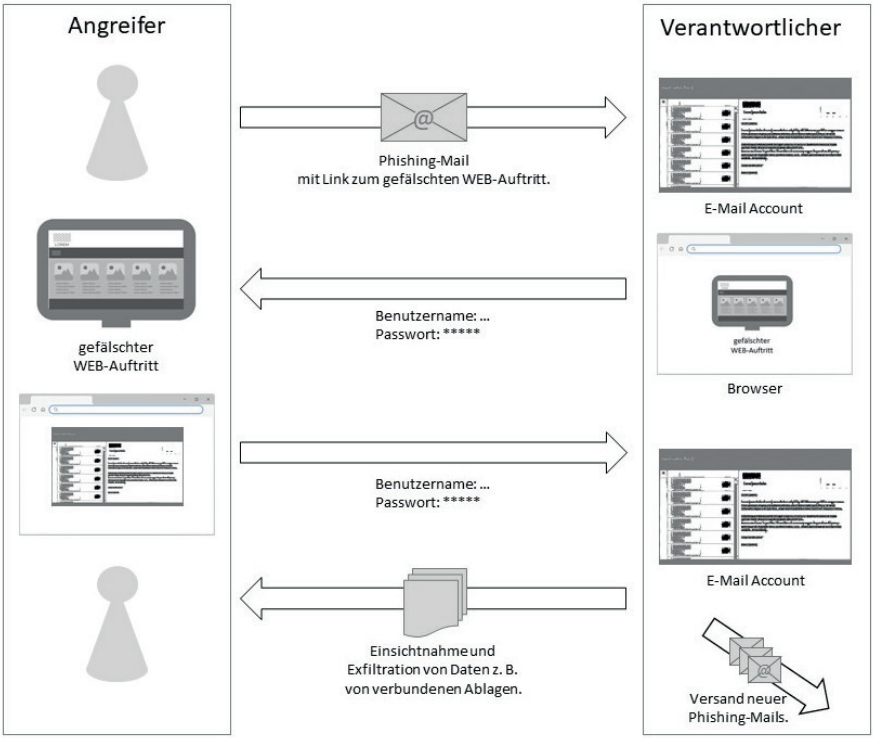


Abb. 1 Phishing-Angriff charakteristischer Ablauf

Die beobachteten Angriffe erfolgten i. d. R. gemäß den in Abbildung 1 dargestellten Schritten. Zu Beginn der Angriffe erhielten Beschäftigte des jeweiligen Verantwortlichen Phishing-Mails, die häufig vertrauenswürdige Absender vortäuschten. Die Phishing-Mails enthielten Hinweise auf vermeintlich wichtige Informationen. Als Lockmittel wurden in den Phishing-Mails Links angeboten, die sich zum Teil in angehängten Dateien befanden. Diese Links sollten zu den vermeintlich wichtigen Informationen führen. Klickte ein Empfänger auf einen solchen Link, wurde er auf eine gefälschte Webseite weitergeleitet. Die gefälschten Webseiten waren häufig den Original-Webseiten des E-Mail-Anbieters optisch nachempfunden, um auf die Beschäftigten authentisch zu wirken. Dabei wurde eine den Beschäftigten vertraute Anmeldeseite vorgetäuscht, um an die Anmeldedaten zu gelangen. Die so getäuschten Beschäftigten gaben dann auf den gefälschten Websites ihre Anmeldedaten (Passwort, Benutzernamen, z. T. weitere Anmeldedaten) ein. Diese wurden daraufhin von den Angreifern gespeichert. Im Anschluss kam es zu unterschiedlichen

Effekten. Zum Teil erfolgte keine Rückmeldung auf die Eingabe oder das Fenster schloss sich mit einer Fehlermeldung.

Im nächsten Schritt meldeten sich die Angreifer über das Internet an den E-Mail-Konten der jeweiligen Beschäftigten an und erhielten so unberechtigten Zugriff auf die im E-Mail-Postfach vorhandenen personenbezogenen Daten. Teilweise nahmen die Angreifer auch Konfigurationsänderungen vor, um sich zu einem späteren Zeitpunkt mit einer eigenen, zusätzlich eingerichteten zweiten Zwei-Faktoren-Authentisierung (2FA) bei gleichem Benutzernamen und Passwort wieder an das E-Mail-Konto anzumelden.

Im darauffolgenden Schritt griffen die Angreifer auf die Informationen in den somit zugänglichen E-Mails der Verantwortlichen zu und versendeten neue Phishing-Mails an die im jeweiligen E-Mail-Konto vorgefundenen E-Mail-Adressen.

In einigen Meldungen fielen zum Beispiel folgende Gestaltungsmerkmale auf, mit denen die Angreifer eine hohe Authentizität der Phishing-Mails vortäuschten, um die Beschäftigten der Verantwortlichen in Sicherheit zu wiegen. Die Phishing-Mails wurden so gestaltet, dass sie von vermeintlich vertrauenswürdigen Absendern wie Geschäftspartnern oder Kolleginnen und Kollegen stammten. Dieser Eindruck wurde von den Angreifern zum Teil dadurch erreicht, dass die Phishing-Mails von bereits zuvor kompromittierten E-Mail-Konten dieser Kommunikationspartner versendet wurden. Um die Vertrauenswürdigkeit der Phishing-Mails weiter zu steigern, wurden diese zum Teil auch mit Informationen aus erbeutetem E-Mail-Verkehr angereichert, der zuvor zwischen dem Verantwortlichen und z. B. seinen Geschäftspartnern stattgefunden hatte.

Vielfach haben Angreifer auch eine 2FA überwunden. Bei einer 2FA handelt es sich um ein bisher als vergleichsweise sicher angesehenes Authentisierungsverfahren. Die Anzahl der Meldungen, bei denen ein solches Verfahren überwunden wurde, zeigt jedoch, dass es vor allem auch auf die korrekte Anwendung eines solchen Verfahrens ankommt. Bei einer 2FA handelt es sich um eine technische Maßnahme, die einen Phishing-Angriff deutlich erschweren kann. Unter den Faktoren zur Authentisierung versteht man Wissen, Besitz oder Sein. Die verschiedenen Faktoren können durch unterschiedliche technische Lösungen umgesetzt werden. Passwort und Benutzernamen sind beispielsweise eine technische Umsetzung des Faktors Wissen. Um eine 2FA zu erhalten, muss eine technische Lösung einer der beiden verbliebenen Faktoren Besitz oder Sein als zweiter, zusätzlicher Authentisierungsfaktor hinzugefügt werden. Weit verbreitet ist die Verwendung von Token oder Smartphone Apps, die in kurzen Zeitabständen Einmalpasswörter generieren. Bei der Authentisierung werden diese nur kurze Zeit gültigen Einmalpasswörter

zusammen mit dem Passwort und dem Benutzernamen zur Authentisierung eingegeben. Um diese Einmalpasswörter zu erhalten, muss der Benutzer im Besitz des Smartphones oder des Tokens sein, weshalb diese technische Maßnahme dem Faktor Besitz zugerechnet wird. Alternativ stellen biometrische Verfahren wie beispielsweise Fingerabdrücke technische Maßnahmen dar, die dem Faktor Sein zuzuordnen sind.

Wenn Benutzername und Passwort Angreifern bekannt sind (Wissen), kann eine Authentifizierungsmethode wie die Zwei-Faktor-Authentifizierung gerade bei IT-Diensten im Internet die Sicherheit erhöhen und den Zugriff von Angreifern auf das System erschweren.

Immer wieder wird jedoch gemeldet, dass 2FA-Verfahren überwunden wurden, die ergänzend als technische Maßnahme Apps auf Smartphones einsetzten. Der Grund dafür ist darin zu suchen, dass in dieser Form der 2FA das Einmalpassworts vom Nutzenden vom Token oder von der Smartphone-App abgelesen und wie der Benutzername und das Passwort in eine Anmeldemaske eingegeben wird. In diesen Fällen konnten sich die Angreifer dann trotz der 2FA mit dem Benutzernamen, dem Passwort und dem Einmalpasswort Zugang zu den E-Mail-Konten der Verantwortlichen verschaffen. Abbildung 2 zeigt, wie sich diese Variante im Detail von dem in Abbildung 1 gezeigten Ablauf unterscheidet.

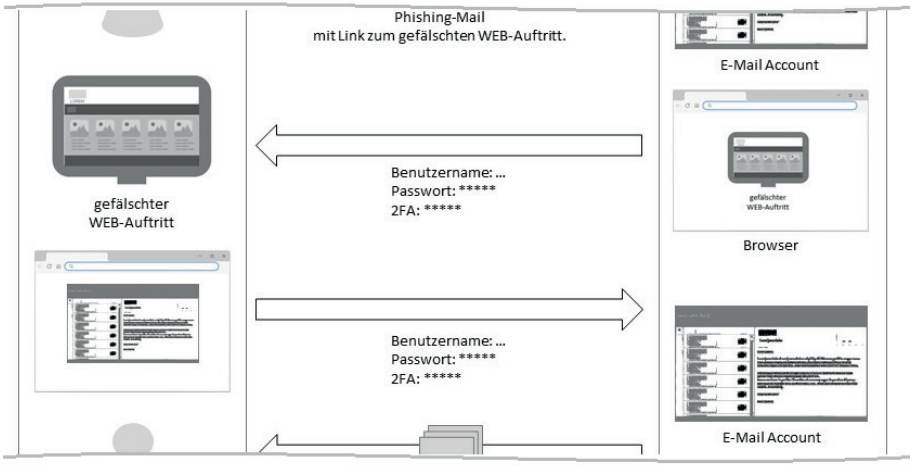


Abb. 2 Phishing-Angriff charakteristischer Ablauf – mit Überwindung 2FA

Im Gegensatz zu Benutzernamen und Passwörtern ist bei einigen 2FA-Verfahren die Gültigkeit des Einmalpassworts zeitlich auf ein paar Sekunden oder Minuten beschränkt, was die Sicherheit gegenüber einem manuell durchgeführten Angriff grundsätzlich verbessert. Es ist aber davon auszugehen, dass gerade bei einer Vielzahl von versendeten Phishing-Mails das Abfischen der Einmalpasswörter und das darauffolgende Anmelden am E-Mail-Account des Verantwortlichen unmittelbar und automatisiert erfolgte.

Bewertung der Angriffe

Sollte ein Verantwortlicher Opfer eines Phishing-Angriffs werden, muss er unverzüglich prüfen, ob eine „Verletzung des Schutzes personenbezogener Daten" vorliegt und ob sich daraus Risiken für die Rechte und Freiheiten natürlicher Personen ergeben können. Auffallend war, dass den Verantwortlichen dabei häufig Fehler in der Sachverhaltsklärung unterliefen. Zunächst müssen über die E-Mail-Adressen und Namen der E-Mail-Absender und -Empfänger hinaus auch die in den E-Mail-Inhalten enthaltenen personenbezogenen Daten bei einer Analyse berücksichtigt werden. Sind mit E-Mail-Konten weitere Dienste verbunden, so müssen die in diesen ggf. verarbeiteten Daten ebenfalls betrachtet werden. So ist etwa bei Dateiablagen zu beachten, dass auch die in den Dateiablagen abgelegten Dateien und die darin ggf. gespeicherten Daten betroffen sein könnten. Von den Verantwortlichen wurden diese immer wieder übersehen, was zu unvollständigen und letztlich nicht aussagekräftigen Risikobewertungen für die Rechte und Freiheiten der Betroffenen führte. Es ist zu bedenken, dass die Risikobewertung die Grundlage für alle weiteren Schritte zur Behandlung von Datenschutzvorfällen war.

Inhalt der Meldung an die Aufsichtsbehörde

Die Meldung an die Aufsichtsbehörde muss nach Art. 33 Abs. 3 DS-GVO mindestens folgende Informationen enthalten:

– Art der Verletzung des Schutzes personenbezogener Daten (z. B. Verlust, unbefugter Zugriff),
– Kategorien und Anzahl betroffener Personen,
– Kategorien und Anzahl betroffener Datensätze,
– Name und Kontaktdaten des Datenschutzbeauftragten oder Ansprechpartners,
– wahrscheinliche Folgen der Verletzung des Schutzes personenbezogener Daten,
– ergriffene oder vorgeschlagene Maßnahmen zur Behebung und Schadensminderung.

In den Meldungen an mich fehlten immer wieder Informationen zu den Phishing-Angriffen selbst. So wurde es von den Verantwortlichen zum Teil versäumt, eine ausreichend präzise Schilderung des Ablaufs zu melden. Einfache Stichworte wie Hacking-Angriff, Phishing o. ä. sind wichtig und helfen bei der Klassifizierung. Sie sind aber für die Darstellung des Sachverhalts, dessen Bewertung und die hierauf aufbauende Risikobetrachtung bei weitem nicht ausreichend. Unvollständige oder fehlende Meldungen führen zu vermeidbaren Nachfragen und erhöhen den Aufwand für alle Beteiligten.

Benachrichtigung der betroffenen Personen

Auch die Benachrichtigung der betroffenen Personen nach Art. 34 DS-GVO beruht auf einer fundierten und aussagekräftigen Risikobewertung des Verantwortlichen. Wenn die Verletzung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der Betroffenen führt, muss der Verantwortliche zusätzlich die betroffenen Personen unverzüglich informieren. Hierbei sollte die Information gemäß Art. 34 Abs. 2 DS-GVO

– in klarer und einfacher Sprache formuliert sein,
– den Namen und die Kontaktdaten des Datenschutzbeauftragten oder Ansprechpartners enthalten,
– die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten für die betroffenen Personen darlegen sowie
– die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und Schadensminderung darstellen.

Auch wenn dies nicht explizit durch die DS-GVO gefordert wird, ist es hilfreich, den betroffenen Personen in der Benachrichtigung auch die Kategorien der betroffenen Daten mitzuteilen. Daraus ergeben sich für die Betroffenen weitere, ggf. wichtige Anhaltspunkte zur Reaktion auf Risiken.

Aufarbeitung und Prävention

Gemäß Art. 32 Abs. 1 DS-GVO sind Verantwortliche unter anderem dazu verpflichtet, die Vertraulichkeit, Integrität und Verfügbarkeit der von ihnen verarbeiteten personenbezogenen Daten zu gewährleisten. Zur Umsetzung des erforderlichen Schutzniveaus sind in diesem Zusammenhang vom Verantwortlichen geeignete technische und organisatorische Maßnahmen (TOM) zu ergreifen. Eine unverzichtbare Maßnahme für über das Internet nutzbare IT-Dienste ist die Implementierung angemessener Authentifizierungsverfahren. Eine beträchtliche Anzahl der Verantwortlichen hatte zum Zeitpunkt des Phishing-Angriffs für die Authentisierung an den aus dem Internet erreichbaren E-Mail-Konten nur Benutzernamen und Passwort verwendet. Durch

die Verwendung stärkerer Authentifizierungsmethoden, wie beispielsweise einer 2FA, können Verantwortliche das Risiko eines unberechtigten Zugriffs auf die personenbezogenen Daten in E-Mail-Konten verringern.

Zur Prävention von Phishing-Vorfällen sollten sich Verantwortliche als Ausgangspunkt zunächst die zugehörigen Risiken systematisch vergegenwärtigen. Hierzu ist ein wie im Kurzpapier Nr. 18 der DSK zu „Risiko für die Rechte und Freiheiten natürlicher Personen“ (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf) erläuterter Ansatz zielführend. Nur so können im Vorfeld geeignete Maßnahmen ermittelt und ergriffen werden. In diesem Zusammenhang sei auch auf das Kurzpapier Nr. 5 der DSK zur Durchführung von Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO verwiesen (https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf). Darüber hinaus möchte ich einige hilfreiche, wenn auch keinesfalls abschließende Hinweise für Verantwortliche geben, die sich unmittelbar aus den gemeldeten Phishing-Angriffen ergaben.

Zur Vermeidung eines erfolgreichen Phishing-Angriffs müssen sich die ergriffenen TOMs ergänzen. Wie zuvor berichtet, ist es möglich, technische Maßnahmen wie zum Beispiel eine 2FA auf der Basis von Einmalpasswörtern zu überwinden, wenn es den Angreifern gelingt, die Beschäftigten des Verantwortlichen zu täuschen. Zur Unterstützung der Beschäftigten sind daher regelmäßige Sensibilisierungsveranstaltungen und Schulungen erforderlich. Sind die Gefahren von Phishing-Mails den Beschäftigten bekannt und bewusst, verbessern sich die Chancen, eine Phishing-Mail zu erkennen und einem Täuschungsversuch zu widerstehen.

Verantwortliche müssen möglichen Schwächen einer bereits eingesetzten technischen Maßnahme für die Authentisierung entgegenwirken. So kann etwa die Verwendung von unterkomplexen Passwörtern durch eine geeignete Passwortrichtlinie und deren technische Durchsetzung begegnet werden. Das gilt auch für die Einführung einer 2FA auf der Basis von Einmalpasswörtern, auch wenn viele Phishing-Angriffe im Berichtszeitraum die Grenzen der technischen Maßnahme einer 2FA mittels Einmalpasswörtern aufgezeigt haben. Zu bedenken sind in diesem Zusammenhang auch Formen der 2FA, deren zweiter Faktor nicht durch Einmalpasswörter, sondern beispielsweise durch kryptographische Verfahren technisch umgesetzt wird. Sie alle erhöhen im Gegensatz zu einer ausschließlichen Authentisierung durch Passwort und Benutzernamen den Schutz auch vor einer Vielzahl anderer Angriffe, die alle zu einem Datenschutzvorfall führen können.

Bei einem Phishing-Vorfall sind unrechtmäßige Zugriffe auf personenbezogene Daten vollumfänglich zu prüfen. Bei der Identifizierung Betroffener geht es nicht nur um die Personen, deren Namen und E-Mail-Adressen aus den

E-Mails direkt ersichtlich sind. Es geht auch um Betroffene, deren personenbezogene Daten sich zum Beispiel in E-Mail-Inhalten, in Dateiablagen oder in anderen mit dem E-Mail-Konto verbundenen Anwendungen befunden haben.

Bei der Analyse der eigenen Log-Dateien ist auch an Daten zu denken, die Auftragsverarbeiter nach Art. 28 Abs. 3 Buchst. f DS-GVO zur Verfügung stellen können. Log-Dateien über Zugriffe und Aktivitäten in den betroffenen E-Mail-Konten werden häufig nur für eine begrenzte Zeit von Anbietern und Auftragsverarbeitern zur Verfügung gestellt und dann automatisiert gelöscht. Daher sind nach einem Vorfall Log-Dateien möglichst frühzeitig zu sichern, um diese wichtigen Informationen zu einem späteren Zeitpunkt für eine Auswertung zur Verfügung zu haben. Zum gleichen Zweck können auch Screenshots relevanter Anzeigen helfen, zu denen ggf. nicht mit Informationen aus den Log-Dateien zu rechnen ist.

Notwendig ist auch bei großen Mengen betroffener Daten, so schnell wie möglich die betroffenen Personen zu identifizieren und diese nach Art. 34 DS-GVO zu benachrichtigen. Zeit spielt eine Rolle, da im Fall einer Benachrichtigung der Betroffenen nach Art. 34 Abs. 1 DS-GVO diese unverzüglich zu erfolgen hat. Betroffene Personen können nur dann auf durch Phishing-Angriffe entstandene Risiken reagieren, wenn sie ausreichend informiert sind. Bei umfangreicheren Auswertungen sollten die Betroffenen ggf. in mehreren Etappen benachrichtigt werden, damit die bereits identifizierten Personen möglichst frühzeitig auf Risiken reagieren können.

Fazit

Phishing ist eine anhaltende Bedrohung für den Schutz personenbezogener Daten und die Rechte und Freiheiten natürlicher Personen. Die Zahl von Meldungen zu Datenschutzverletzungen aufgrund von erfolgreichen Phishing-Angriffen ist signifikant angestiegen. Betroffen waren im Wesentlichen über das Internet zugängliche E-Mail-Konten.

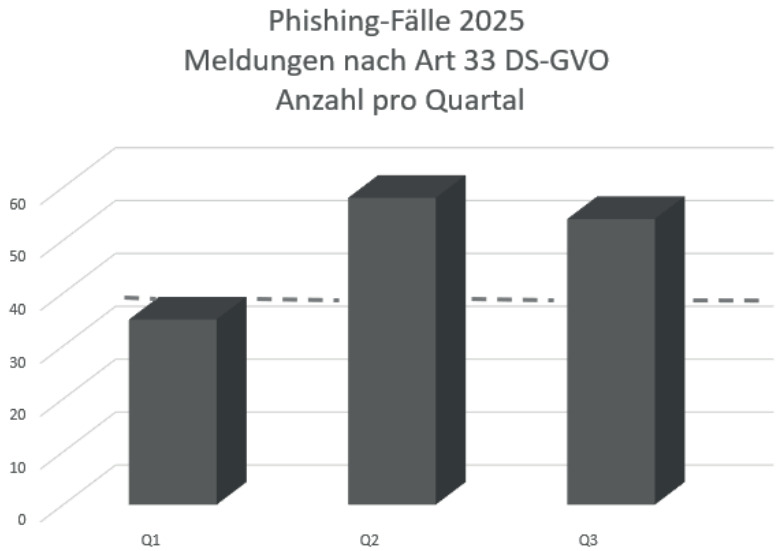


Abb. 3 Phishing-Fälle, Meldungen nach Art. 33 DS-GVO

Es ist zu befürchten, dass die Anzahl erfolgreicher Phishing-Angriffe gleichermaßen zugenommen hat. Mit der gestiegenen Bedrohung wäre für Verantwortliche auch die Wahrscheinlichkeit, Opfer eines erfolgreichen Phishing-Angriffs zu werden, gestiegen. Dies muss nicht zuletzt auch bei der Betrachtung der Risiken für die Rechte und Freiheiten betroffener Personen Berücksichtigung finden. Bisherige technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung müssen regelmäßig überprüft, bewertet, evaluiert und bei Bedarf angepasst werden. Hierbei müssen auch geänderte Risikobeurteilungen mit einfließen.

17. 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. 17.1). Darüber hinaus haben meine Mitarbeitenden und ich im Rahmen von Schulungen (Kap. 17.2), Vorträgen und Podiumsdiskussionen (Kap. 17.3) sowie verschiedenen Veröffentlichungen (Kap. 17.4) datenschutzrechtliche Zusammenhänge erläutert. Diese Anstrengungen zur Öffentlichkeitsarbeit werden ergänzt durch Beiträge in elektronischen Medien (Kap. 17.5) und Kommunikationen mit der Presse (Kap. 17.6).

17.1 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).

Europäischer Datenschutztag „Digitalisierung um jeden Preis?“

Zum 19. Europäischen Datenschutztag habe ich am 28. Januar 2025 als scheidender Vorsitzender der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Vortrags- und Diskussionsveranstaltung der DSK zum Thema „Digitalisierung um jeden Preis? Kein Zwang zur Preisgabe personenbezogener Daten“ organisiert. Etwa 150 Vertreterinnen und Vertreter aus Politik, Wirtschaft, Wissenschaft und Gesellschaft trafen in der Hessischen Landesvertretung in Berlin zusammen. Gegenstand der Tagung waren bestimmte Folgen der Digitalisierung aller Lebensbereiche: Inwieweit kann der Zugang zu Bahnfahrten und Paketabholungen, zu Arztterminen, zu Schwimmbädern und Museen, zu öffentlichen Zuschüssen und Leistungen eines Bürgeramts von der Nutzung digitaler Kommunikationsmittel abhängig gemacht werden? Wie wirken sich solche digitalen Zugangshürden auf diejenigen aus, die kein Smartphone oder keinen Internetzugang besitzen oder die ihre personenbezogenen Daten nicht für diesen Zweck preisgeben wollen? Ist die durch ausschließliche digitale Zugangshürden entstehende Datenverarbeitung gerechtfertigt? Welche

datenschutzrechtlichen Gestaltungsvorgaben müssen die Verantwortlichen beachten?

Prof. Dr. Heribert Prantl (Süddeutsche Zeitung) präsentierte eine Reihe von Beispielen für digitale Zugangshürden. Seine Untersuchung der dadurch entstehenden Folgen fasste er in der Feststellung zusammen: „Wer kein Smartphone hat, wird ausgeschlossen." Die Strategie „digital only" führe in die Verfassungswidrigkeit. Daher forderte er ein „Recht auf analogen Zugang zur Daseinsvorsorge".

Die Bedeutung von digitaler Teilhabe aus der Sicht des Verbraucherschutzes beleuchtete Jutta Gurkmann (Verbraucherzentrale Bundesverband). Die willkürliche Erweiterung der Datenerhebung durch datengetriebene Geschäftsmodelle um digitale Zugangshürden dürfe Verbraucherinnen und Verbraucher nicht von Gütern und Leistungen ausschließen, die sie für ein lebenswertes Leben benötigen. Ansonsten verkehre sich das Teilhabeversprechen der Digitalisierung in sein Gegenteil. Wo digitale Exklusion existenzielle Bereiche des Zusammenlebens betreffe, wie etwa bei Mobilität, Gesundheit und Zahlungsverkehr, müssten auch alternative Zugänge angeboten werden, so Gurkmann.

Ich stellte in meinem Vortrag klar, dass die Verarbeitung personenbezogener Daten durch digitale Zugangshürden datenschutzrechtlich unzulässig ist und gegen die Grundsätze von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen verstoßen kann. Dem müssen und können Datenschutzaufsichtsbehörden entgegentreten (s. näher Roßnagel, Kein Zwang zur Preisgabe personenbezogener Daten, Zeitschrift für Datenschutz (ZD) 2025, 184–189).

Rena Tangens (Digitalcourage e. V.) zeigte in ihrem Vortrag „Wahlfreiheit statt Digitalzwang" an zahlreichen Beispielen auf, dass Teilhabe am gesellschaftlichen Leben in vielen Bereichen nur noch digital möglich ist. Der Verein Digitalcourage habe sich in den letzten Jahren immer wieder intensiv mit derartigen Fällen beschäftigt. Sie argumentierte, dass dieser „Digitalzwang" Freiheitsrechte beeinträchtige, und forderte deshalb ein Grundrecht auf analoges Leben.

Eine differenzierte Sicht auf den Themenbereich nahm Prof. Dr. Steffen Augsberg (Universität Gießen) ein. In seinem Überblick über „datenschutzrelevante Interessenkonflikte und Interessenkonvergenzen in der Digitalisierung" zeigte er, welche verfassungsrechtlich geschützten Interessen für eine Digitalisierung sprechen und wo andere ebenfalls verfassungsrechtlich geschützte Interessen einer ausschließlichen Digitalisierung Grenzen setzen. Er plädierte für Einzelfallbetrachtungen anstelle pauschaler Verweise etwa auf Grundrechte oder Menschenwürde.

Schließlich kam mit Nico Lüdemann (bluecue consult, Bundesverband der mittelständischen Wirtschaft) ein Interessenvertreter der Digitalwirtschaft zu Wort, der aus seiner Sicht den „Zwiespalt zwischen Innovation und Datenschutz“ erläuterte. Er sah zwar die Nachteile einer Digital-Only-Strategie, warb aber auch um Verständnis, dass Effizienzsteigerung und Aufgabenerleichterung durch Digitalisierung möglich sein müssten. In diesem Zusammenhang warb er zudem für mehr Medienbildung, die zu einem angemessenen Umgang mit der zunehmend digitalisierten Welt führe.

Die Diskussionen zu den Vorträgen hatten besonders die praktische Umsetzbarkeit von Datenschutz und dem Recht auf analoge Teilhabe zum Gegenstand. Zu berücksichtigen ist dabei aber das Spannungsfeld zwischen datenschutzrechtlichen Zielsetzungen und wirtschaftlichen Zwängen.

Zum Abschluss der Veranstaltung übergab ich offiziell den DSK-Vorsitz an die Berliner Beauftragte für Datenschutz und Informationsfreiheit Meike Kamp.

CAST-Forum „Datenschutzgerechter Umgang mit Künstlicher Intelligenz“

Am 6. März 2025 haben das „Competence Center for Applied Security Technology (CAST)“, die vom Bundesministerium für Forschung, Technologie und Raumfahrt geförderte „Plattform Privatheit – Forschung für ein selbstbestimmtes Leben in der digitalen Welt“ und ich gemeinsam ein Forum zum Thema „Recht und IT-Sicherheit: Datenschutzgerechter Umgang mit Künstlicher Intelligenz – Anforderungen der KI-VO und DS-GVO in der Praxis“ durchgeführt. Die Veranstaltung wurde von mir moderiert. Im Rahmen des Forums wurden praktische Fragen im Umgang mit Künstlicher Intelligenz behandelt, die für die Handlungsmöglichkeiten von Entscheidern und Datenschutzbeauftragten von Betreibern von KI-Systemen relevant sind.

Der Vortrag von Privatdozent Dr. Christan Geminn vom Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel „Das Zusammenspiel von KI-VO und DS-GVO – Ein harmonisches Miteinander?“ bot eine Übersicht über das fehlende Zusammenspiel und die begrifflichen Widersprüche zwischen KI-VO und DS-GVO im Umgang mit KI-Systemen.

Sodann erläuterte Prof. Dr. Tobias Keber, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, in seinem Vortrag „Zulässigkeit des Einsatzes von KI-Systemen“ die Anforderungen an die datenschutzrechtliche Zulässigkeit des Einsatzes von KI-Modellen aus datenschutzrechtlicher Sicht.

Dr. Marit Hansen, die Landesbeauftragte für Datenschutz und Informationsfreiheit Schleswig-Holstein, erläuterte in ihrem Vortrag „Organisations- und

Managementaufgaben nach KI-VO und DS-GVO“, in welcher Weise die Vorgaben von KI-VO und DS-GVO zusammenwirken können, um die erforderliche Dokumentation zu erreichen.

Dr. Christoph Bausewein, Assistant General Counsel, Data Protection & Policy von CrowdStrike, untersuchte in seinem Beitrag „Überschneidungen von Betreiberpflichten nach KI-VO und DS-GVO“, inwiefern Überschneidungen bei den Transparenzpflichten der DS-GVO und der KI-VO bestehen.

Welche Informationspflichten die Verantwortlichen und Betreiber gegenüber betroffenen Personen und welche Transparenzanforderungen betroffene Personen ihnen gegenüber haben, erörterte Dr. Vyacheslav Bortnikov, Leiter des Referats „Künstliche Intelligenz“ bei der BfDI, in seinem Vortrag „Transparenz bei KI-Systemen“.

Sowohl die KI-VO als auch die DS-GVO sehen Pflichten von Verantwortlichen und Betreibern vor, die Sicherheit von KI-Systemen zu gewährleisten. Oren Halvani, Abteilungsleiter „AI and Security“ im Fraunhofer-Institut SIT in Darmstadt, beschrieb in seinem Beitrag „Sicherheitsanforderungen und -möglichkeiten im Umgang mit KI-Systemen“, welche spezifischen neuen Sicherheitsaufgaben durch den Betrieb von KI-Systemen entstehen und wie diese erfüllt werden können.

27. Wiesbadener Forum Datenschutz „Bürokratieabbau im Datenschutz“

Am 5. Mai 2025 habe ich zusammen mit der Präsidentin des Hessischen Landtages, Astrid Wallmann, das 27. Wiesbadener Forum Datenschutz im Plenarsaal des Hessischen Landtages veranstaltet. Die Fachtagung widmete sich dem aktuellen Thema „Bürokratieabbau im Datenschutz“ und erfreute sich mit knapp 150 Teilnehmenden aus Politik, Wirtschaft und Wissenschaft in diesem Jahr besonders großen Interesses.

Soweit im Datenschutz bürokratische Auswüchse bestehen, sind diese abzubauen. Bürokratie ist jedoch nicht grundsätzlich schlecht, sondern eine Form der rationalen Ausübung von Herrschaft in der Demokratie. Die Unterschiede zwischen notwendiger und zu weitgehender Bürokratie zu identifizieren, liegt nicht nur im Interesse von Politik und Verantwortlichen, sondern auch im eigenen Interesse der Aufsichtsbehörden. Das 27. Wiesbadener Forum Datenschutz ging daher der Frage nach, wo im Datenschutz Regelungen notwendig sind und wo überflüssige bürokratische Regelungen und Praktiken festzustellen und zu beseitigen sind.

Beleuchtet wurde das Thema „Bürokratieabbau im Datenschutz“ in Vorträgen von Manfred Pentz, dem Hessischen Minister für den Bund, Europa, Internati-

onales und Entbürokratisierung („Bürokratisierung und Entbürokratisierung“), Prof. Dr. Wolfgang Ziebarth von der Hochschule der Polizei Baden-Württemberg („Kontrollaufgaben und Gesetzesbindung der Datenschutzaufsicht“), Privatdozent Dr. Christian Geminn von der Universität Kassel („Risikoorientierung bei Datenschutzgrundsätzen und Erlaubnistatbeständen?“), dem Bayerischen Landesbeauftragten für den Datenschutz Prof. Dr. Thomas Petri („Ermessen im Vollzug des Datenschutzrechts“) und dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg Prof. Dr. Tobias Keber („Bürokratieabbau im Vollzug von KI-Verordnung und Datenschutz-Grundverordnung“).

Die Vorträge und Diskussionen wurden in dem Buch Roßnagel/Wallmann (Hrsg.), Bürokratieabbau im Datenschutz, Nomos Verlag 2025, veröffentlicht.

4. Datenschutztag Hessen & Rheinland-Pfalz

Zum vierten Mal habe ich am 2. Juli 2025 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, den Datenschutztag Hessen & Rheinland-Pfalz ausgerichtet. Unter dem Motto „Information Overload? Über- und Durchblick für Datenschutzbeauftragte“ beleuchteten Vertreterinnen und Vertreter aus Politik, Aufsichtsbehörden und Praxis zentrale Herausforderungen für Datenschutzbeauftragte – von Gesetzesflut über Künstliche Intelligenz bis hin zur Bürokratiebelastung – und zeigten auf, wie menschenzentrierte Digitalisierung gelingen kann.

Der Datenschutztag bot den zahlreich anwesenden behördlichen, kommunalen und betrieblichen Datenschutzbeauftragten mit einem Mix aus Vorträgen und interaktiven Formaten Orientierung im immer dichter werdenden Informationsdschungel sowie praxisnahe Hilfsmittel und ermöglichte einen umfassenden Überblick über die aktuellen Entwicklungen in Gesetzgebung, Rechtsprechung und Aufsichtspraxis. Ein besonderes Highlight bildete wie in den Vorjahren das Abschlusspanel „Die Aufsichtsbehörden beantworten Ihre Fragen“. Hier konnten Teilnehmende direkt mit den Aufsichtsbehörden in den Dialog treten. Neben dem LfDI und mir beantwortete auch die saarländische Landesbeauftragte für Datenschutz und Informationsfreiheit, Monika Grethel, Fragen aus dem Publikum. Monika Grethel schlug abschließend eine Brücke in das kommende Jahr, in dem die saarländische Behörde Teil des Veranstalterteams sein wird, und befand, dass sich der Datenschutztag zu einem Pflichttermin für behördliche und betriebliche Datenschutzbeauftragte im Südwesten Deutschlands entwickelt hat.

Fachmessen

Um ein niedrigschwelliges Informationsangebot für Bürgerinnen und Bürger zu schaffen, die in ihrem Arbeitsalltag regelmäßig mit Datenschutzfragen konfrontiert sind, war meine Behörde im Berichtsjahr auch auf zwei Fachmessen präsent.

So habe ich mich an einem gemeinsamen Infostand mehrerer Mitglieder der DSK auf der Bildungsmesse Didacta beteiligt. Die Didacta ist die größte Bildungsmesse Europas und richtet sich an unterschiedliche Akteure aus dem Bildungsbereich. Der Stand wird seit mehreren Jahren in wechselnder Besetzung von Mitgliedern der DSK betrieben und stößt regelmäßig auf großes Interesse. Hier konnten wir gemeinsam über Bildungsangebote im Bereich Datenschutz für Kinder und Jugendliche informieren und Besucherinnen und Besucher für Datenschutzfragen in der täglichen Arbeit sensibilisieren.

Zudem war meine Behörde auf der 18. Frankfurter Ehrenamtsmesse mit einem Stand vertreten. Die Messe richtet sich an Personen, die bereits in einem Ehrenamt tätig sind oder eine solche Tätigkeit suchen. Auch hier haben meine Mitarbeitenden für Datenschutzfragen sensibilisiert oder auf Informationsangebote hingewiesen.

17.2
Schulungen

Mitarbeitende meiner Behörde haben im Berichtszeitraum viele Schulungen veranstaltet, um über Datenschutzfragen zu informieren. Im Folgenden werden die wichtigsten Schulungsveranstaltungen aufgelistet.

Datum	Titel	Referent/in
4.2.2025	BvD-qualifizierte:r Datenschutzkoordinator:in	Katja Horlbeck
6.2.2025	KI-Einsatz in der Verwaltung	Katja Horlbeck, Volker Zimmer
11.3.2025	Datenschutz in Kommunen (KSV Medien)	Dr. Sebastian Rapp
5.4.2025	Fit für die Prüfung Klausurtechnik Wirtschaftslehre-Privatrecht (Hessischer Verwaltungsschulverband, HVSV)	Markus Thor
8.4.2025	Datenschutz in Kommunen (KSV Medien)	Dr. Sebastian Rapp
22.4.2025	Praxiswissen Datenschutz: Datenschutz bei der Verarbeitung von Personaldaten in öffentlichen Stellen (HVSV)	Stephanie Wetzstein

Datum	Titel	Referent/in
23.4.2025	Beschäftigtendatenschutz in der öffentlichen Verwaltung	Stephanie Wetzstein
8.5.2025	Praxiswissen Datenschutz: Datenschutz in Kommunen (HVSV)	Dr. Sebastian Rapp
15.5.2025	Einführung in die KI-Verordnung Teil I: Allgemeine Bestimmungen und verbotene Praktiken	Katja Horlbeck, Volker Zimmer
21.5.2025	Praxiswissen Datenschutz: Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten (HVSV)	Roman Mehner
4.6.2025	Praxiswissen Datenschutz: Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten (HVSV)	Roman Mehner
11.6.2025	Praxiswissen Datenschutz: Datenschutz-Folgenabschätzung und Verzeichnis von Verarbeitungstätigkeiten (HVSV)	Roman Mehner
5.9.2025	KI-Einsatz in der Verwaltung	Katja Horlbeck, Volker Zimmer
3.11.2025	Workshop für Datenschutzbeauftragte der Justiz	Neele Zander
6.11.2025	Praxiswissen Datenschutz: Datenschutz bei der Verarbeitung von Personaldaten in öffentlichen Stellen (HVSV)	Stephanie Wetzstein
11.11.2025	Praxiswissen Datenschutz: Datenschutz in Kommunen (HVSV)	Dr. Sebastian Rapp
24.11.2025	Einführung in die KI-Verordnung Teil II: Hochrisiko-KI-Systeme und Transparenzpflichten	Katja Horlbeck, Volker Zimmer
24.11.2025	Einführung in die KI-Verordnung Teil II: KI-Modelle mit allgemeinem Verwendungszweck & Governance	Katja Horlbeck, Volker Zimmer
9.12.2025	BvD-qualifizierte:r Datenschutzkoordinator:in	Katja Horlbeck

17.3
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	Mitarbeiter/in
28.1.2025	Zwang zur Preisgabe personenbezogener Daten aus Sicht des Datenschutzes	19. Europäischer Datenschutztag der DSK „Digitalisierung um jeden Preis?“, Berlin	Prof. Dr. Alexander Roßnagel
30.1.2025	Interessenkonflikte bei Datenschutzbeauftragten in öffentlichen Stellen	BvD Regionalgruppe Mitte	Dr. Viktoria Friedrichsen, Dr. Sebastian Rapp
30.1.2025	Aufsichtsrechtliche Maßnahmen gegenüber öffentlichen Stellen	BvD Regionalgruppe Mitte	Dr. Viktoria Friedrichsen, Dr. Sebastian Rapp
27.2.2025	Cyberkriminalität, Datensicherheit und Datenschutz aus Sicht des HBDI	Deutscher Anwaltverein – AG Sozialrecht	Dr. Nils Gaebel
2.4.2025	KI-VO und DSGVO im Spannungsverhältnis	Datenschutz-Stammtisch, pwc, Frankfurt	Prof. Dr. Alexander Roßnagel
5.5.2025	Bürokratieabbau im Datenschutz – Einführung in die Tagung	Wiesbadener Forum Datenschutz „Bürokratieabbau im Datenschutz“ im Hessischen Landtag	Prof. Dr. Alexander Roßnagel
7.5.2025	Aktuelles aus der Aufsichtsbehörde	Frühjahrstagung des GDD Erfa-Kreises Hessen	Martin Buchter
13.5.2025	Datenschutz in Digital-Only-Modellen	Datenschutzkongress 2025, Berlin	Prof. Dr. Alexander Roßnagel
27.5.2025	POLAS-Datensätze aus datenschutzrechtlicher Sicht	Hochschule für öffentliches Management und Sicherheit	Carina Tepper

Datum	Vortragstitel	Veranstaltung	Mitarbeiter/in
2.6.2025	Datenschutz und KI? Was sind personenbezogene Daten? Funktionsweise von LLMs?	KI-Cafe im Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz	Katja Horlbeck, Martin Wedekind, Martin Buchter, Volker Zimmer
17.6.2025	Datenschutzrechtliche Herausforderungen für den Betrieb von KI-Systemen	IAPP, Frakfurt	Prof. Dr. Alexander Roßnagel, Katja Horlbeck
24.6.2025	Die elektronische Patientenakte ePA – Ist das Vertrauen in die ärztliche Schweigepflicht noch möglich?	168. Bad Nauheimer Gespräche bei der Landesärztekammer Hessen	Dr. Nils Gaebel
2.7.2025	Entbürokratisierung im Datenschutz	4. Datenschutztag Hessen & Rheinland-Pfalz	Prof. Dr. Alexander Roßnagel
2.7.2025	DS-GVO und 3. Teil HDSIG – eine Gegenüberstellung	4. Datenschutztag Hessen & Rheinland-Pfalz	Silvana Hornjak
2.7.2025	Datenschutz im Vergabeverfahren	4. Datenschutztag Hessen & Rheinland-Pfalz	Katja Horlbeck (mit Dr. Daniela Franke, LfDI RLP)
2.7.2025	Hilfestellungen der Aufsicht: Veröffentlichungen der Aufsichtsbehörden, des EDSA und der DSK	4. Datenschutztag Hessen & Rheinland-Pfalz	Clara Bormann
2.7.2025	KI im Kontext von Sicherheit und Justiz	4. Datenschutztag Hessen & Rheinland-Pfalz	Ines Walburg (mit Antonia Buchmann, LfDI RLP)
2.7.2025	KI aus Sicht des Datenschutzbeauftragten	4. Datenschutztag Hessen & Rheinland-Pfalz	Volker Zimmer (mit Dr. Philipp Richter, LfDI RLP)
2.7.2025	Datenschutzbeauftragte – Fachkunde, Ressourcen, Interessenkollision – Umfragen in Rheinland-Pfalz und Hessen	4. Datenschutztag Hessen & Rheinland-Pfalz	Dr. Sebastian Rapp (mit Gerd Fischer, LfDI RLP)

Datum	Vortragstitel	Veranstaltung	Mitarbeiter/in
2.7.2025	Aktuelle Fragestellungen aus der kommunalen und behördlichen Praxis	4. Datenschutztag Hessen & Rheinland-Pfalz	Silvana Hornjak (mit Michael Smolle, LfDI RLP)
2.7.2025	Technischer Datenschutz unter der Lupe: Das IT-Labor des HBDI	4. Datenschutztag Hessen & Rheinland-Pfalz	Rouven Wachhaus, Dr. Jens Bruhn
2.7.2025	KI im Kontext von Sicherheit und Justiz – Neuerungen durch die KI-VO	4. Datenschutztag Hessen & Rheinland-Pfalz	Ines Walburg (mit Antonia Buchmann, LfDI RLP)
28.8.2025	Reform der DSGVO	Dritte Sommerklausur der DSK, Verwaltungsuniversität Speyer	Prof. Dr. Alexander Roßnagel
3.9.2025	Datenethik und KI – Chancen, Grenzen, rechtlicher Rahmen	Wirtschaftsrat Deutschland, Landesfachkommission Digitalisierung, Frankfurt	Prof. Dr. Alexander Roßnagel
16.9.2025	Beschäftigtendatenschutz und KI aus aufsichtsbehördlicher Perspektive	Datenschutztag HessenChemie	Katja Horlbeck
24.9.2025	Podiumsdiskussion zu aktuellen Fragen des Datenschutzes	Kommunaler Datenschutztag der ekom21	Prof. Dr. Alexander Roßnagel, Dr. Jens Bruhn, Katja Horlbeck
25.9.2025	Rolle des HBDI in IT-Projekten der Hessischen Landesverwaltung	Klausurtagung der Hauptpersonalräte der Hessischen Landesverwaltung	Dr. Jens Bruhn, Katja Horlbeck
8.10.2025	Gesellschaftlich wünschenswerte IT-Gestaltung	Tagung „Gesellschaftlich wünschenswerte IT-Gestaltung – 20 Jahre ITeG“, Universität Kassel	Prof. Dr. Alexander Roßnagel
8.10.2025	Selbstbestimmung in der digitalen Gesellschaft (Podiumsdiskussion),	Tagung „Gesellschaftlich wünschenswerte IT-Gestaltung – 20 Jahre ITeG“, Universität Kassel	Prof. Dr. Alexander Roßnagel

Datum	Vortragstitel	Veranstaltung	Mitarbeiter/in
10.10.2025	Auswirkungen der DSGVO (Podiumsdiskussion)	Zehn Jahre Datenschutz im Wandel. Wissenschaftliches Symposium, Landesmuseum Mainz	Prof. Dr. Alexander Roßnagel
16.10.2025	Neues von der Hessischen Datenschutzaufsicht / Interessenkonflikte bei Datenschutzbeauftragten und aktuelle Themen der Datenschutzaufsicht	GSE-Tagung	Dr. Viktoria Friedrichsen
16.10.2025	Konzerndatenschutz, berechtigte Interessen und das Urteil des Bundesarbeitsgerichts vom 08.05.2025 (AZR 209/21)	BvD-Regionalgruppe Mitte	Katja Horlbeck, Stephanie Wetzstein
23.10.2025	Künstliche Intelligenz und Justiz – KI im Spannungsfeld zwischen Datenschutzrecht und Technik	Hessische Justizakademie	Ines Walburg, Dr. Jens Bruhn
30.10.2025	Aktuelle Datenschutzthemen in der Kreditwirtschaft aus der Aufsichtspraxis	Verband Internationaler Banken in Deutschland e. V.	Dr. Viktoria Friedrichsen
30.10.2025	Impulsvortrag Beschäftigtendatenschutz	Arbeitsgemeinschaft Steuerung Personal hessischer Landkreise	Stephanie Wetzstein
1.11.2025	Datenschutz in der Arztpraxis – Vermeidbare Fehler und Eingaben Klassiker	15. Frankfurter Medizinrechtstage	Dr. Nils Gaebel
4.11.2025	Stellungnahme zu den Gesetzentwürfen zum Schutz des Landtages	Ältestenrat des Hessischen Landtags	Prof. Dr. Alexander Roßnagel

Datum	Vortragstitel	Veranstaltung	Mitarbeiter/in
4.11.2025	Vorstellung der Arbeit des HBDI	Besuch der Regionalgruppe des HBDI	Prof. Dr. Alexander Roßnagel, Stephanie Wetzstein, Rouven Wachhaus, Katja Horlbeck
6.11.2025	Anhörung zum Gesetzentwurf für KI in der Hessischen Landesverwaltung	Ausschuss für Digitalisierung und Datenschutz des Hessischen Landtags	Prof. Dr. Alexander Roßnagel
20.11.2025	Vortrag zum Datenschutzrecht	DEXT-Netzwerktreffen	Ines Walburg, Carina Tepper
21.11.2025	Bündelung der Datenschutzaufsicht, KI-VO-Umsetzung, Reform der DSGVO	Tagung der Projektgruppe verfassungsverträgliche Technikgestaltung, Berlin	Prof. Dr. Alexander Roßnagel
24.11.2025	Datenschutzrechtliche Herausforderungen des KI-Einsatzes in der Verwaltung	Veranstaltung des HBDI in Zusammenarbeit mit dem BvD	Prof. Dr. Alexander Roßnagel, Katja Horlbeck, Volker Zimmer
3.12.2025	Datenschutz in Hessen	PSITA-Praxisaustausch	Prof. Dr. Alexander Roßnagel, Lisa-Marie-Lange, Dr. Jens Bruhn, Jens Kirch, Katja Horlbeck
4.12.2025	Künstliche Intelligenz im Öffentlichen Dienst	Personalversammlung Regierungspräsidium Gießen	Ines Walburg, Dr. Jens Bruhn

17.4
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 Publikationen aufgelistet.

– Friedrichsen, V.: § 33 Auskunftsrecht der betroffenen Person, Ronellenfitsch et al., Hessisches Datenschutz- und Informationsfreiheitsgesetz, 21. NL 9.2025.
– Fuchs, T./Kamp, M./Roßnagel, A.: Die Datenschutzaufsicht reformieren, Frankfurter Allgemeine Zeitung vom 10.7.2025, S. 18.
– Gaebel, N.: Ist die elektronische Patientenakte sicher? Was man aus der Causa ePA für künftige Digitalisierungsprojekte lernen kann, Hessisches Ärzteblatt 4/2025, 246.
– Rapp, S.: § 3 Verarbeitung personenbezogener Daten, Auftragsverarbeitung, Ronellenfitsch et al., Hessisches Datenschutz- und Informationsfreiheitsgesetz, 21. NL 9. 2025.
– Rapp, S.: Datenschutz bei politischen Informationssystemen, KommJur 2025, 201 ff.
– Rettig, S.: § 60 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten, Ronellenfitsch et al., Hessisches Datenschutz- und Informationsfreiheitsgesetz, 21. NL 9.2025.
– Rettig, S.: Die Kooperationspflicht aus Art. 31 DS-GVO. Überblick über Tatbestand und normative Grenzen der allgemeinen Mitwirkungspflicht, Zeitschrift für Datenschutz (ZD), Heft 9, ZD 2025, 501–505.
– Roßnagel, A./Wallmann, A. (Hrsg.), Bürokratieabbau im Datenschutz, Reihe Wiesbadener Forum Datenschutz, neue Reihe Band 5, Baden-Baden 2025, 138 Seiten.
– Roßnagel, A./Gierich, A.: Patientenakten in Klinikinsolvenzen. Durchsetzung von Datenschutzanforderungen nach einer Betriebsschließung, Zeitschrift für Datenschutz (ZD), Heft 3, 2025, 123–127.
– Roßnagel, A.: Anmerkung zu EuGH vom 9.1.2025 – C-416/23 – Österreichische Datenschutzbehörde/FR, EuZW 2025, 223, Europäische Zeitschrift für Wirtschaftsrecht (EuZW), 35. Jg. (2025) Heft 5, 227–229.
– Roßnagel, A.: Weg mit den Landesdatenschutzbeauftragten? Zeitschrift für Datenschutz (ZD), 15. Jg. (2025), Heft 4, 181–182.
– Roßnagel, A.: Kein Zwang zur Preisgabe personenbezogener Daten. Datenschutzrechtlicher Rahmen für digitale Zugangshürden zu analogen Leistungen, Zeitschrift für Datenschutz (ZD), 15. Jg. (2025), Heft 4, 184–189.
– Roßnagel, A.: 7 Jahre DSGVO – Ein Blick zurück und ein Blick voraus aus Sicht der Datenschutzaufsicht, Privacy in Germany (PinG), 13. Jg. (2025), Heft 3, 118–124.
– Roßnagel, A.: Datenschutzgerechter Umgang mit KI (Editorial), Datenschutz und Datensicherheit (DuD), 49. Jg. (2025), Heft 5, 273.
– Roßnagel, A.: Anmerkung zu EuGH, Urteil vom 4.9.2025 – C-413/23 – SRB, ZD 2025, 631, Zeitschrift für Datenschutz (ZD), 15. Jg. (2025), Heft 11, 637–638.
– Roßnagel, A.: Einführung – Ansätze zum Abbau von Bürokratie im Datenschutz, in: Roßnagel, A./Wallmann, A. (Hrsg.), Bürokratieabbau im Datenschutz, Reihe Wiesbadener Forum Datenschutz, neue Reihe Band 5, Baden-Baden 2025, 11–22.

- Roßnagel, A.: Datenschutzrechtliche Verhaltensregeln. Rechtliche Bedeutung für unterschiedliche Adressaten, Zeitschrift für Datenschutz (ZD), 15. Jg. (2025), Heft 12, 669–674.
- Wedekind, M.: § 32 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, Ronellenfitsch et al., Hessisches Datenschutz- und Informationsfreiheitsgesetz, 21. NL 9.2025.
- Wedekind, M.: § 34 Recht auf Löschung („Recht auf Vergessenwerden"), Ronellenfitsch et al., Hessisches Datenschutz- und Informationsfreiheitsgesetz, 21. NL 9.2025.
- Wedekind, M.: § 35 Widerspruchsrecht, Ronellenfitsch et al., Hessisches Datenschutz- und Informationsfreiheitsgesetz, 21. NL 9.2025.

17.5
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 versuche ich, über andere Mittel auszugleichen.

Homepage

Im Berichtsjahr habe ich intensiv auf meiner Homepage über praktische Fragen des Datenschutzes informiert. Auf der Homepage wurden 26 Beiträge veröffentlicht und zahlreiche Bereiche inhaltlich aktualisiert.

Mastodon

Den Mastodon-Account meiner Dienststelle im Fediverse habe ich weiter gepflegt und insgesamt 38 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.

17.6
Presseanfragen und Pressemitteilungen

Im Berichtsjahr habe ich intensiven Kontakt mit der Presse gehalten. Presseorgane haben insgesamt 85 Presseanfragen an uns gerichtet, die ich alle behandelt habe. Meine Mitarbeitenden und ich haben zudem im Rahmen mehrerer Interviews in Presseorganen zu Datenschutzfragen Stellung genommen. Im Berichtsjahr habe ich 21 Pressemitteilungen veröffentlicht. Auf

besonderes Interesse sind meine Pressemitteilungen zu den Vorschlägen aus dem Koalitionsvertrag der Bundesregierung, die Datenschutzaufsicht im Bereich der Wirtschaft zu zentralisieren („Koalitionspläne zum Datenschutz bringen Nachteile für regionale Wirtschaft und Menschen vor Ort"), und zum Urteil des OLG Frankfurt am Main vom 10. Juli 2025 (Az. 6UKl 14/24) gestoßen, mit dem meine Rechtsauffassung bestätigt und die DB Fernverkehr AG verurteilt wurde, es beim Vertrieb von Sparpreis- oder Super-Sparpreistickets zu unterlassen, von Verbrauchern E-Mail-Adressen und/oder Mobiltelefonnummern ohne Alternative zu verarbeiten (s. hierzu auch Kap. 3.1). Auch mein „Bericht zum Einsatz von Microsoft 365" (s. hierzu auch Kap. 16.2) und die zugehörige Pressemitteilung fanden große Resonanz.

18. Arbeitsstatistik

18.1 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 1.1.2024 bis 31.12.2024	Fallzahlen 1.1.2024 bis 31.12.2024
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).	3.839	**6.070**
Beratungen Anzahl von schriftlichen Beratungen. Dies umfasst summarisch Beratungen von Verantwortlichen, betroffenen Personen und der eigenen Regierung. **Nicht:** (Fern-)mündliche Beratungen, Schulungen, Vorträge etc.	1.171	**1.198**
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)	741	**1.220**
Abhilfemaßnahmen Anzahl der getroffenen Maßnahmen, die im Berichtszeitraum getroffen wurden.	115	**124**
(1) nach Art. 58 Abs. 2 a (Warnungen)	0	**0**
(2) nach Art. 58 Abs. 2 b (Verwarnungen)	55	**58**

(3) nach Art. 58 Abs. 2 c – g und j (Anweisungen und Anordnungen)	13	**19**
(4) nach Art. 58 Abs. 2 i (Geldbußen)	47 in Höhe von insg. € 544.986	**47** **in Höhe von insg. € 190.100**
(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	16	**27**
(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	289	**308**
(2) Anzahl der Verfahren mit Federführung (Art. 56 DS-GVO)	12	**10**
(3) Anzahl der Verfahren gemäß Kap. VII DS-GVO (Art. 60 ff. DS-GVO)	848	**1.589**
gesamte Verfahren nach Art. 56 DS-GVO		**1.072**
Amtshilfeverfahren (Art. 61 DSGVO)		**204**
Begleitung bei Rechtsetzungsvorhaben		
Anzahl der Beratungen in Rechtssetzungsverfahren	15	**12**

18.2
Ergänzende Erläuterungen zu Zahlen und Fakten

Die nachstehenden Darstellungen erläutern und ergänzen die Zahlen und Fakten auch im Vergleich mit dem Vorjahr und den weiteren Arbeitsgebieten im Berichtsjahr. Die Zahl der Eingaben ist in diesem Jahr auf ein Allzeithoch geschnellt. Die Anzahl der Beschwerden allein ist um 58 % angestiegen. In manchen Bereichen hat sich die Zahl der Eingaben im Vergleich zum Vorjahr verdoppelt oder gar verdreifacht.

Dieser Anstieg ist zum Teil mit konkreten Ereignissen wie z. B. einem Urteil zu Speicherfristen von Daten bei Auskunfteien oder auch mit Presseberichterstattung zu datenschutzrelevanten Themen, die die öffentliche Aufmerksamkeit auf datenverarbeitende Unternehmen in Hessen lenken, verknüpft. Im Bereich der Videoüberwachung spielt auch eine Rolle, dass die dafür notwendige

Technik immer günstiger angeboten wird und ein erhöhtes Bedürfnis nach Sicherheit die Installation privat betriebener Überwachungstechnik begünstigt.

Über alle Bereiche hinweg ist jedoch zu beobachten, dass die von sehr vielen verwendeten KI-Bots darauf verweisen, dass die betroffenen Personen ihre Sorgen und Probleme mit Datenschutzbezug kostenlos an mich als Aufsichtsbehörde adressieren können. Viele lassen sich dann ihre Beschwerden und Hinweise von KI-Tools formulieren.

All dies führt zu einer Überlast an Eingaben, die meine Behörde bei gleichbleibender Personalausstattung nicht in den gesetzlich vorgesehenen Fristen bewältigen kann. Daher kommt es auch vermehrt dazu, dass Menschen, die sich mit ihren Problemen an mich gewandt haben, unzufrieden mit den Bearbeitungszeiten ihrer Anliegen sind und diese Unzufriedenheit auch deutlich zum Ausdruck bringen.

Beschwerden, Hinweise und Beratungen

Die nachfolgende Übersicht stellt die Zahl der Eingaben (Beschwerden und Beratungen) des Berichtsjahres im Vergleich zum Vorjahr dar:

Fachgebiete	2024				2025			
	Beschwerden	Beratungen	Hinweise	Eingaben insgesamt	Beschwerden	Beratungen	Hinweise	Eingaben insgesamt
Auskunfteien, Inkasso	503	4	2	**509**	1.613	12	4	**1.629**
Schule, Hochschule, Archive	140	136	13	**289**	82	127	23	**232**
e-Kommunikation, Internet	260	45	112	**417**	319	25	233	**577**
Beschäftigtenverhältnisse	287	150	25	**462**	525	122	55	**702**
Videobeobachtung	295	87	306	**688**	539	106	436	**1.081**
Kreditwirtschaft	401	3	2	**406**	513	7	1	**521**
Handel, Handwerk, Gewerbe	236	17	8	**261**	323	13	20	**356**
Verkehr, Geodaten, Landwirtschaft	342	13	53	**408**	374	19	71	**464**

Gesundheit, Pflege	183	85	55	**323**	276	113	47	**436**
Betriebliche/ Behördliche DSB	6	188	0	**194**	6	174	5	**185**
Kommunen, Wahlen	88	131	7	**226**	159	124	29	**312**
Polizei, Justiz, Verfassungs-schutz	196	93	32	**321**	293	147	65	**505**
Vereine, Verbände	105	27	8	**140**	92	40	12	**144**
Adresshandel, Werbung	367	5	9	**381**	418	1	31	**450**
Wohnen, Miete	114	30	17	**161**	119	13	14	**146**
Soziales	83	41	5	**129**	136	21	13	**170**
Versorgungs-unternehmen	35	14	51	**100**	47	12	73	**132**
IT-Sicherheit, DV-Technik**	5	46	15	**66**	8	65	7	**80**
Versicherungen	41	9	14	**64**	44	6	49	**99**
Rundfunk, Fernsehen, Presse	43	4	3	**50**	28	2	12	**42**
Religionsge-meinschaften	1	4	0	**5**	13	5	0	**18**
Datenschutz außerhalb der EU	2	10	1	**13**	1	13	0	**14**
Forschung, Statistik	8	17	0	**25**	6	19	1	**26**
Ausländerrecht	3	1	0	**4**	24	3	0	**27**
Steuerwesen	10	2	0	**12**	30	0	3	**33**
Sonstige Themen (z. B. Glücksspiel, Zensus, Archive, Geodaten)	84	9	3	**96**	82	9	16	**107**
Zwischen-summe Beschwerden, Beratungen und Hinweise	3.839	1.171	741	**5.751**	6.070	1.198	1.220	**8.488**
Meldungen von Daten-pannen*				**2.141**				**2.730**

Gesamtsumme dokumentierter Eingaben	**7.892**	**11.218**
Telefonische Beratungen und Auskünfte von mehr als 10 Minuten**	**3.084**	**2.796**
Gesamtsumme dokumentierter + telefonischer Eingaben	**10.976**	**14.014**

*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.

Abhilfemaßnahmen und Gerichtsverfahren

Abhilfemaßnahmen	Anzahl 2024	Anzahl 2025
(1) Warnungen (Art. 58 Abs. 2 a DS-GVO)	0	**0**
(2) Verwarnungen (Art. 58 Abs. 2 b DS-GVO)	55	**58**
(3) Anweisungen und Anordnungen (Art. 58 Abs. 2 c-g, j DS-GVO)	13	**19**
(4) Geldbußen (Art. 58 Abs. 2 i DS-GVO)	47	**47**
(5) Widerruf von Zertifizierungen (Art. 58 Abs. 2 h DS-GVO)	0	**0**
Gesamt	115	**124**

Gerichtsverfahren	Anzahl 2024	Anzahl 2025
Klagen gemäß Art. 78 Abs. 1 DS-GVO	21	**25**
Klagen gemäß Art. 78 Abs. 2 DS-GVO	6	**3**
Verfahren vor dem VGH in 2. Instanz	7	**7**
Verfahren vor dem Bundesverfassungsgericht	1	**2**
Eilverfahren	1	**5**
Güterichterverfahren	-	**1**
Verfahren vor Landgerichten	-	**1**
Verfahren vor Oberlandesgerichten	-	**2**
Grundrechtsklagen	-	**1**
Isolierte Prozesskostenhilfeverfahren	-	**1**
Sonstige	1	**2**
Gesamt	37	**50**

Meldungen von Datenschutzverletzungen nach Art. 33 DS-GVO und §60 HDSIG

Gesamtübersicht		
Grund	**Anzahl 2024**	**Anzahl 2025**
Fehlversand/Fehlzuordnung von Daten/Dokumenten	895	**1.161**
Hackerangriffe, Phishing, Schadsoftware, Sicherheitslücke	482	**625**
Verlust/ Diebstahl von Unterlagen, Datenträgern, Geräten	140	**293**
Unrechtmäßige Offenlegung/Weitergabe von Daten	185	**168**
Unzulässige Einsichtnahme (fehlerhafte Einrichtung von Zugriffsrechten u. a.)	153	**134**
Offener E-Mail-Verteiler	110	**120**
Missbrauch von Zugriffsrechten	92	**102**
Unzulässige Veröffentlichung	34	**40**
Nicht datenschutzkonforme Entsorgung	14	**29**
Unverschlüsselter E-Mail-Versand	21	**20**
Sonstige	15	**38**
Gesamt	**2.141**	**2.730**

Am stärksten betroffene Bereiche	Fälle 2024	Fälle 2025
Kreditwirtschaft, Auskunfteien, Handel und Gewerbe	537	**672**
Technischer Bereich, IT	477	**641**
Gesundheitsbereich	323	**461**
Beschäftigtendatenschutz	294	**325**

Anhang zu I

Ausgewählte Materialien der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder aus dem Jahr 2025

1. Entschließungen

1.1
Eckpunkte für eine freiheitliche und grundrechtsorientierte digitale Zukunft vom 26.3.2025

https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Datenschutzpolitisches_Eckpunktepapier.pdf

1.2
Confidential Cloud Computing vom 16.6.2025

https://www.datenschutzkonferenz-online.de/media/en/DSK-Entschliessung_Confidential_Cloud_Computing.pdf

1.3
Ohne Sicherheit keine Freiheit – Ohne Freiheit keine Sicherheit vom 16.6.2025

https://www.datenschutzkonferenz-online.de/media/en/DSK-Entschliessung_Innere_Sicherheit.pdf

1.4
Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten! vom 17.9.2025

https://www.datenschutzkonferenz-online.de/media/en/2025-09-17_DSK-Entschliessung_Automatisierte-Datenanalyse.pdf

1.5
Verbesserung des Datenschutzes von Kindern in der Datenschutz-Grundverordnung vom 20.11.2025

https://www.datenschutzkonferenz-online.de/media/en/Entschliessung_Datenschutz-von-Kindern.pdf

1.6
DS-GVO-Reform: IT-Hersteller in die Verantwortung nehmen! vom 12.12.2025

https://www.datenschutzkonferenz-online.de/media/en/DSK_Entschliessung_DSGVO_Herstellerverantwortung.pdf

1.7
DS-GVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich vom 12.12.2025

https://www.datenschutzkonferenz-online.de/media/en/DSK_Entschliessung_DSGVO_KI_Anpassungen.pdf

2. Beschlüsse

2.1
Meldung von Mieter:innendaten an Grundversorger vom 28.5.2025

https://www.datenschutzkonferenz-online.de/media/dskb/Beschluss_Meldung_von_Mieter-innendaten_an_Grundversorger.pdf

2.2
Datenschutz bei der Terminverwaltung durch Heilberufspraxen. Positionspapier zum datenschutzkonformen Einsatz von Dienstleistern für Online-Terminbuchungen und das Terminmanagement vom 16.6.2025

https://www.datenschutzkonferenz-online.de/media/dskb/DSK-Beschluss_Positionspapier_Terminverwaltungsunternehmen.pdf

2.3
Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz (OZG), 12/2025

https://www.datenschutzkonferenz-online.de/media/dskb/DSK_Standardisierter_Pruefprozess_OZG.pdf

3. Orientierungshilfen und Anwendungshinweise

3.1
Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Version 1.0, 6/2025

https://www.datenschutzkonferenz-online.de/media/oh/DSK-OH_KI-Systeme.pdf

3.2
Empfehlungen für Informationspflichten bei Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken (Anlage zu Orientierungshilfe zu Anwendungshinweisen), 9/2025

https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen_Anlage.pdf

3.3
Anwendungshinweise zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen der wissenschaftlichen Forschung zu medizinischen Zwecken, 9/2025

https://www.datenschutzkonferenz-online.de/media/oh/20250917_DSK_OH_Datenuebermittlungen.pdf

3.4
Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode, Version 1.0, 10/2025

https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_RAG.pdf

3.5
Orientierungshilfe zur Zusammenarbeit mehrerer Aufsichtsbehörden im Rahmen von § 5 GDNG, Version 1.0, 12/2025

https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_Zusammenarbeit_mehrerer_Aufsichtsbehoerden_GDNG.pdf

3.6
Orientierungshilfe zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes (OZG) Anwendungshilfe für Stellen, die (länderübergreifende) Onlinedienste nach OZG betreiben oder nutzen, Version 1.1, 12/2025

https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_OZG_Version_1_1.pdf

3.7
Anforderungen an datenschutzrechtliche Zertifizierungsprogramme. Datenschutzrechtliche Prüfkriterien, Prüfsystematik und Prüfmethoden zur Anpassung und Anwendung der technischen Norm DIN EN ISO/IEC 17067 (Programmtyp 6), Version 3.0 vom 17.11.2025

https://www.datenschutzkonferenz-online.de/media/ah/DSK_Zertifizierungskriterien_Version_3_0.pdf

II
Zweiter Teil
8. Tätigkeitsbericht zur Informationsfreiheit

1. Entwicklung der Informationsfreiheit

Der vorliegende achte Tätigkeitsbericht zur Informationsfreiheit beschreibt und analysiert die Informationsfreiheit in Hessen im Jahr 8 seit der Regelung des Rechts eines allgemeinen und voraussetzungslosen Zugangs zu Akten der öffentlichen Verwaltung im Hessischen Datenschutz und Informationsfreiheitsgesetz (HDSIG) und spricht Entwicklungsmöglichkeiten der Informationsfreiheit an, die auf notwendige Anpassungen an die dynamischen Entwicklungen der digitalen Gesellschaft zurückzuführen sind.

Der Informationsanspruch

Seit dem 25. Mai 2018 sind der Anspruch des Zugangs zu amtlichen Informationen, 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. Ich nehme als Hessischer Beauftragter für den Datenschutz auch das Amt des Hessischen Informationsfreiheitsbeauftragten wahr. Ich bin Aufsichtsbehörde für die Umsetzung der Informationsfreiheit. Bürgerinnen und Bürger, die sich in ihrer Informationsfreiheit beeinträchtigt sehen, können sich mit einer Beschwerde an mich wenden.

Dieser Regelung zur Umsetzung der Informationsfreiheit liegt folgende Zielsetzung zugrunde. In einer Demokratie darf die öffentliche Verwaltung kein geschlossener Bereich mehr sein, sondern muss ihr Handeln offen und transparent gestalten. Bürgerinnen und Bürger sollen zum einen die Möglichkeit haben, das Handeln der von ihnen gewählten und demnächst wieder zur Wahl 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. Sie sollen wissen können, was und wie in ihrem Namen entschieden wird. Dies stärkt nicht nur die Transparenz des Staates, sondern auch das Vertrauen der Bürgerinnen und Bürger in sein Handeln. Informationsfreiheit hat somit eine wichtige demokratische und rechtsstaatliche Funktion, stärkt die bürgerschaftliche Partizipation und die Kontrolle staatlichen Handelns.

Die Entwicklung des Informationsanspruchs

Die Bundesrepublik Deutschland und vierzehn Bundesländer haben seit vielen Jahren Informationsfreiheitsgesetze, die den Informationszugang zu allen öffentlichen Stellen eröffnen. In einigen Bundesländern wurden diese Gesetze inzwischen zu Transparenzgesetzen weiterentwickelt, welche die öffentliche Verwaltung verpflichten, von sich aus möglichst viele Informationen öffentlich zu stellen.

Hessen war in dieser Entwicklung ein Nachzügler und hat erst vor acht 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.

Open Data

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, Teil 2, 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 Daten offen für alle Interessierten 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.

Ausblick auf Zukunftsentwicklungen

Die Entwicklungen in Technik, Wirtschaft, Verwaltung und Gesellschaft gehen rasant weiter. An diese Entwicklungen muss sich auch die Informationsfreiheit dynamisch anpassen. Neue Chancen sind zu unterstützen, neuen Herausforderungen ist rechtzeitig zu begegnen. Die Transparenz staatlichen Handelns muss sich in der digitalen Gesellschaft weiterentwickeln und muss zukunftsfähig werden.

Die Digitalisierung der Verwaltung vermehrt zum einen die verfügbaren und hilfreichen Informationen. Sie erzeugt damit Mehrwerte für die Nutzung dieser Informationen, die der Gesellschaft, insbesondere für die Forschung und weitere Allgemeininteressen, zur Verfügung gestellt werden müssen. Regelungen wie die des Gesundheitsdatennutzungsgesetzes oder des im Gesetzgebungsprozess befindlichen Forschungsdatengesetzes zeigen die Richtung der notwendigen Entwicklung. Zum anderen erleichtert und befördert die Digitalisierung der Verwaltung die Erfüllung von Informationsansprüchen. Sofern Prinzipien der „Informationsfreiheit by Design“ zur Anwendung gelangen, könnte die Digitalisierung der Verwaltung auch lästige Mehrarbeit in der Verwaltung und die damit verbundenen Abwehrreflexe gegen Informationsbegehren vermeiden oder reduzieren.

Künstliche Intelligenz

Eine besondere Rolle wird dabei Künstliche Intelligenz (KI) spielen. Ihre zunehmende Verbreitung und Nutzung verändert grundlegend, wie Informationen erzeugt, verarbeitet und verbreitet werden. Sie wird auch die Art und Weise, wie Informationsansprüche geltend gemacht und für unterschiedliche Zwecke eingesetzt werden, ebenso verändern wie die Möglichkeiten, in der Verwaltung mit Informationsansprüchen umzugehen.

KI braucht viele Daten, bereichsspezifische KI-Systeme benötigen viele Daten aus der öffentlichen Verwaltung. Um KI-Systeme zu unterstützen, empfiehlt sich daher eine breite Open Data-Strategie. Ein bedeutendes Problem von KI ist die Verlässlichkeit ihrer Ergebnisse. Sie bietet immer Ergebnisse, auch wenn diese auf Halluzinationen beruhen. Umso wichtiger sind amtliche Informationen für die Verlässlichkeit, Nachvollziehbarkeit und Kontrolle ihrer Antworten. Der direkte Zugang zu solchen Informationen ist ein entscheidender Faktor, um der Verbreitung ungesicherter oder gefälschter Inhalte entgegenzuwirken.

Der Informationsanspruch der Bürgerinnen und Bürger wird sich künftig auch auf Systeme der KI erstrecken müssen. Wenn die Verwaltung ihre Informationen (überwiegend) mit KI generiert, verwaltet, auswertet und nutzt, wird der Anspruch auf „Zugang zu amtlichen Informationen“ nicht auf digitale Dokumente und Dateien beschränkt werden können, sondern sich auch auf die Informationen in amtlichen KI-Systemen erstrecken müssen. Dann wird sich der Anspruch auch darauf richten, Zusammenfassungen, Auswertungen, Rechtsauskünfte oder fachliche Bewertungen aus amtlichen KI-Systemen zu erhalten. Fraglich ist dann, wie Kompetenzgrenzen von öffentlichen Stellen und Zweckbindungen von Daten gewährleistet werden können, wenn das KI-System nicht nur eine Einzelauskunft gibt, sondern auch umfangreiches Überblickswissen ermöglicht.

Auch die Anfragenden werden KI nutzen, um ihre Informationsziele zu verfolgen. Durch gezielte Nachfragen – eventuell bei unterschiedlichen Behörden – könnten sie Kontextwissen erhalten, das ihnen erlaubt, aus den erhaltenen Antworten auch Informationen zu entnehmen, auf die sie – wie auf personenbezogene Daten, Betriebsgeheimnisse oder öffentliche Projektplanungen – zum Schutz der Rechte Dritter oder öffentlicher Interessen keinen Anspruch haben. Die Grenzen des Informationsanspruchs werden dann neu austariert werden müssen.

KI hilft aber auch den verpflichteten Verwaltungsbehörden. Sie können in vielen Fällen die gewünschten Informationen „auf Knopfdruck“ erzeugen und bereitstellen. Bei entsprechendem Training könnte die KI sie unterstützen, die Berechtigung der Informationsanfrage zu bewerten und notwendige

Abwägungen zwischen einem berechtigten Informationsinteresse und dem Schutz der Interessen Dritter und der Allgemeinheit vorzunehmen.

Die Informationsfreiheit im Berichtsjahr

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 achte Tätigkeitsbericht eine kleine Auswahl. Er greift die neue gesetzliche Möglichkeit für Gemeindevertretungen, Stadtverordnetenversammlungen und Kreistage auf, die Protokolle der Kommunalparlamente im Internet öffentlich zugänglich zu machen. Ob ein Kommunalparlament das will, kann es durch Satzung entscheiden (Kap. 2). Der Tätigkeitsbericht beantwortet die Frage, welche Auswirkungen es hat, wenn in amtlichen Informationen Geschäftsgeheimnisse enthalten sind. Diese sind zwar zu schützen, dürfen aber nicht dazu führen, dass der Informationszugang pauschal verweigert wird. Vielmehr ist zu prüfen, ob eine Unkenntlichmachung der Geschäftsgeheimnisse möglich ist (Kap. 3). Schließlich untersucht er, ob Forscherinnen und Forscher im Rahmen eines Forschungsprojekts an einer öffentlichen Hochschule als natürliche Personen anzusehen sind, die sich auf die Informationsfreiheit berufen können. Außerdem wird geprüft, welche Informationen sie als amtliche Informationen von einer öffentlichen Stelle verlangen dürfen (Kap. 4).

2. Veröffentlichung von Protokollen der Kommunalparlamente

Es dient dem Informationsbedürfnis der Bürgerinnen und Bürger, wenn die Protokolle (Niederschriften) der Gemeindevertretungen/Stadtverordnetenversammlungen sowie der Kreistage sowohl mittels (analoger) Einsichtnahme vor Ort als auch öffentlich (digital) im Internet zugänglich sind. Dieses Ergebnis kann durch eine transparenzfreundliche Gestaltung des Kommunalrechts erreicht werden. In Hessen wird den Einwohnern die Einsichtnahme in diese Protokolle gewährleistet. Die Nutzung des Internets zur öffentlichen Bereitstellung der Sitzungsniederschriften wird den Kommunalparlamenten überlassen.

Ein Thema der Konferenz der Informationsfreiheitsbeauftragten von Bund und Ländern

Im Berichtsjahr 2025 hatte der Thüringer Beauftragte für den Datenschutz und die Informationsfreiheit als Vorsitzender der Konferenz der Informationsfreiheitsbeauftragten (IFK) zurecht darauf hingewiesen, dass es mit Blick auf die Informationsinteressen der Bürgerinnen und Bürger bedeutsam ist, dass die Niederschriften von Sitzungen der kommunalen Vertretungsorgane zugänglich sind. Denn gerade in den Kommunalparlamenten werden viele Themen behandelt, die unmittelbare Auswirkungen auf den Alltag der Bürgerinnen und Bürger vor Ort haben wie etwa kommunale Bauvorhaben, Verkehrsregelungen und andere Vorhaben. Von daher sei zu kritisieren, so der Thüringer Informationsfreiheitsbeauftragte zurecht, dass jedenfalls in Thüringen, aber auch in einigen anderen Bundesländern die Veröffentlichung dieser kommunalen Sitzungsprotokolle nicht uneingeschränkt gewährleistet sei. Vor diesem Hintergrund hat dann auch die IFK eine auf Verbesserung der kommunalen Transparenz zielende Entschließung gefasst (https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/48_Konferenz_Entschlie%C3%9Fung-Kommunalordnung.pdf?__blob=publicationFile&v=3).

Die Rechtslage in Hessen

In Hessen war bis März 2025 die Rechtslage so, dass eine Offenlegung dieser Sitzungsprotokolle für die Gemeindebewohner nicht vorgesehen war, sondern nur für die Gemeindevertreter selbst (§ 61 Abs. 3 HGO). Nunmehr gibt es seit April 2025 in Hessen eine ergänzende neue Regelung in § 61 Abs. 4 HGO.

§ 61 Abs. 4 HGO

(4) Die Einsichtnahme in die Niederschriften über öffentliche Sitzungen der Gemeindevertretung ist den Einwohnern zu ermöglichen. Zu diesem Zweck kann die Geschäftsordnung vorsehen, dass Niederschriften mit dem Inhalt nach Absatz 1 auf der Internetseite der Gemeinde veröffentlicht werden.

Mit eben dieser Regelung wird die Informationsfreiheit verbessert (s. auch LT-Drs. 21/1303 zu § 61 HGO). Diese Rechtslage gilt nach § 32 HKO entsprechend auch für die Landkreise. Allerdings ist die Gewährleistung der Einsichtnahme auf die Einwohnerinnen und Einwohner der entsprechenden Kommune beschränkt. Denn die mit der digitalen Veröffentlichung der Sitzungsprotokolle auf der Internetseite der Gemeinde verbundene Transparenz auf kommunaler Ebene ist den dortigen Vertretungsorganen überlassen. Dies bedeutet offenkundig eine gewisse Parallele zum allgemeinen Informationsfreiheitsrecht in Hessen in §§ 80 ff. HDSIG insoweit, als die Entscheidung über dessen Geltung im kommunalen Bereich nach § 81 Abs. 1 Nr. 7 HDSIG ebenfalls auf die Kommunalparlamente übertragen worden ist (kommunaler Satzungsvorbehalt).

3. Ausgleich zwischen Informationszugang und Geschäftsgeheimnissen

Der Schutz von Dritten, deren Geschäftsgeheimnisse in amtlichen Informationen enthalten sind, darf nicht dazu führen, dass der Informationszugang pauschal verweigert wird. Vielmehr ist zu prüfen, ob eine Unkenntlichmachung der Geschäftsgeheimnisse möglich ist.

Informationsantrag

Ein Bürger hatte sich an mich gewandt, weil er bei einer hessischen öffentlichen Stelle Unterlagen zu Sitzungen einer Arbeitsgruppe angefragt hatte, in denen es um die Einführung eines Produkts ging. Die Behörde berief sich auf den Ausnahmetatbestand des § 82 Nr. 4 HDSIG, da die Informationen auch Geschäftsgeheimnisse enthalten würden.

Rechtslage

Wie ich in meinem 2. Tätigkeitsbericht zur Informationsfreiheit ausgeführt habe, besteht ein Anspruch auf Informationszugang nicht gegenüber Geschäftsgeheimnissen. Dies ergibt sich aus § 82 Nr. 4 HDSIG.

§ 82 Nr. 4 HDSIG

Ein Anspruch auf Informationszugang besteht nicht (…)

4. bei zum persönlichen Lebensbereich gehörenden Geheimnissen oder Betriebs- oder Geschäftsgeheimnissen, sofern die betroffene Person nicht eingewilligt hat (…).

Diese Ausnahme vom Anspruch auf Informationszugang darf jedoch nicht dazu führen, dass eine öffentliche Stelle sich pauschal auf diesen Ausschlusstatbestand beruft, wenn einige der angefragten Informationen Geschäftsgeheimnisse enthalten. Sind Geschäftsgeheimnisse betroffen, ist ein Drittbeteiligungsverfahren nach § 86 HDSIG durchzuführen.

§ 86 HDSIG

Die informationspflichtige Stelle gibt einem Dritten, dessen Belange durch den Antrag auf Informationszugang berührt sind, schriftlich Gelegenheit zur Stellungnahme innerhalb eines Monats, sofern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann. Die Einwilligung des Dritten zum Informationszugang der antragstellenden Person gilt als verweigert, wenn sie nicht innerhalb eines Monats nach Anfrage durch die zuständige Stelle vorliegt.

Die Behörde hatte hier bereits ein Drittbeteiligungsverfahren durchgeführt. Sie teilte mir mit, dass die dritte Stelle pauschal die Einwilligung zur Herausgabe aller Informationen verweigert habe und der Beschwerdeführer deswegen keinen Anspruch auf Informationszugang habe. Dies diene dem Schutz der Rechte Dritter.

Ausgleich

Da meine Behörde bei den Sitzungen der Arbeitsgruppe beteiligt war, war mir bekannt, dass nur sehr wenige der angefragten Unterlagen überhaupt Geschäftsgeheimnisse enthielten. Ich habe daraufhin der Behörde angeboten, zur Sichtung und Schwärzung der Unterlagen zu beraten. Ein Anspruch auf Informationszugang darf nicht pauschal verneint werden, wenn nur einige der Informationen Geschäftsgeheimnisse enthalten. Vielmehr sind diese vor der Herausgabe der Informationen an die antragstellende Person unkenntlich zu machen. Das Recht auf Zugang zu amtlichen Informationen und die schutzwürdigen Belange Dritter können so in einen Ausgleich gebracht werden.

4. Anspruch auf Informationszugang von Forschenden

Forscherinnen und Forscher sind natürliche Personen im Sinne des § 80 Abs. 1 HDSIG, auch wenn sie im Rahmen eines Forschungsprojekts Informationen anfragen. Bei den Informationen ist zu differenzieren, ob es sich um amtliche Informationen handelt. Es kommt nicht allein darauf an, ob die Behörde die Informationen als aktenwürdig eingestuft hat.

Antrag auf Informationszugang

Ein Forscher einer Hochschule hatte bei einer öffentlichen Stelle in Hessen einen Antrag auf Informationszugang gestellt und wollte für ein Forschungsprojekt zwei Kennzahlen von der Behörde genannt haben. Er gab an, dass er diese Zahlen benötige, um im Rahmen eines laufenden bundesweiten Befragungsprojekts abschätzen zu können, wie repräsentativ seine Stichproben sind. Es handelte sich bei den angefragten Kennzahlen um Informationen zum Personalstatus eines Bereichs innerhalb der Behörde.

Die angefragte Behörde lehnte den Antrag zunächst mit der Begründung ab, sie könne aus datenschutzrechtlichen Gründen keine Auskunft geben. Der Beschwerdeführer wandte sich daraufhin an mich, damit ich ihn bei der Wahrnehmung seines Informationsfreiheitsrechts unterstütze.

Rechtslage

Die Datenschutzrechte sind bei der Erteilung von Auskünften im Rahmen von Informationsfreiheitsanfragen gemäß § 83 HDSIG zu beachten.

> *§ 83 HDSIG*
> *Der Informationszugang zu personenbezogenen Daten ist nur dann und soweit zulässig, wie ihre Übermittlung an eine nicht öffentliche Stelle zulässig ist.*

Ich habe die Behörde daraufhin um Stellungnahme gebeten. In der Antwort berief sich die informationspflichtige Stelle nicht länger auf die Datenschutzrechte von betroffenen Personen, da evident war, dass hier keine Rückschlüsse von den Kennzahlen auf personenbezogene Daten gezogen werden konnten.

Die Behörde stellte sich jedoch auf den Standpunkt, es handele sich bei den angefragten Kennzahlen nicht um amtliche Informationen im Sinne des § 80 Abs. 1 HDSIG. Außerdem sei der Beschwerdeführer als Forscher keine natürliche Person oder juristische Person des Privatrechts, sondern handele

für die Hochschule als juristische Person des öffentlichen Rechts. Daher sei er nicht anspruchsberechtigt.

Was sind amtliche Informationen im Sinne des § 80 Abs. 1 HDSIG?

Der Anspruch auf Informationszugang bezieht sich auf amtliche Informationen.

> *§ 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.*

Die Behörde begründete ihre Auffassung, es handele sich bei den angefragten Informationen nicht um amtliche Informationen im Sinne des § 80 Abs. 1 HDSIG, da die Zahlen nicht einem Verwaltungsvorgang zugeordnet werden könnten, keinen Bezug zu behördlichem Handeln hätten und nicht aktenwürdig seien, da keine Nachvollziehbarkeit behördlichen Handelns im Einzelfall durch die Informationserteilung geschaffen werde.

Ich habe der Behörde daraufhin meine abweichende Rechtsauffassung mitgeteilt. Danach handelte es sich bei den beiden angefragten Zahlen um amtliche Informationen. Dass die Zahlen nicht einem einzelnen Verwaltungsvorgang zuzuordnen waren, war dabei unerheblich. Das VG Berlin (VG Berlin ZUM 2008, 353, 354) hat entschieden, dass solche Informationen amtlich sind, die in Erfüllung amtlicher Tätigkeit angefallen sind. Dabei kommt es weder auf die Art der Verwaltungsaufgabe noch auf die Handlungsform der Verwaltung an. Ohne Bedeutung ist auch, ob sich die Informationen auf ein hoheitliches, schlichthoheitliches oder fiskalisches Handeln beziehen. Dabei ist auch der Bezug zu einem konkreten Verwaltungsvorgang nicht notwendig (Brink/Polenz/Blatt, IFG, 2017, § 2 Rn. 18). Die Information war jedenfalls in Erfüllung einer der angefragten Behörde durch Gesetz zugewiesenen Kernaufgabe angefallen und damit als amtliche Information zu qualifizieren (Schoch, IFG, § 2 Rn. 61). Eine Ausnahmevorschrift war nicht ersichtlich.

Sind Forscherinnen und Forscher natürliche Personen?

Die Beschwerdegegnerin begründete die Ablehnung des Antrags auch damit, dass nur natürliche und juristische Personen des Privatrechts anspruchsberechtigt im Sinne des § 80 Abs. 1 HDSIG sind, und stellte sich auf den

Standpunkt, dass der Forscher für eine öffentliche Hochschule und damit für eine juristische Person des öffentlichen Rechts handelte. Dieser Rechtsauffassung bin ich entgegengetreten. Um Informationen angefragt hatte nicht die Hochschule als juristische Person des öffentlichen Rechts, sondern der Beschwerdeführer persönlich. Es handelte sich hier nicht um einen Fall, in dem eine natürliche Person in ihrer organschaftlichen Stellung einen Antrag stellt. Vielmehr hatte der Beschwerdeführer als natürliche Person in Ausübung seines Grundrechts auf Forschungsfreiheit nach Art. 5 Abs. 3 GG den Antrag gestellt. Dass er die Anfrage im Rahmen eines Forschungsprojekts, das er an einer Hochschule durchführt, gestellt hatte, führt nicht dazu, dass er für diese handelte. Sämtliche Korrespondenz seinerseits wurde nicht im Auftrag oder in Vertretung geführt. Es waren auch keine Verwaltungsaufgaben der Hochschule betroffen, sondern vielmehr der Kernbereich des individuellen Grundrechts der Forschungsfreiheit. Das Forschungsprojekt erfolgte gegenüber der Hochschule weisungsunabhängig. Außerdem ist der Beschwerdeführer als Inhaber einer Vertretungsprofessur persönlich Grundrechtsträger nach Art. 5 Abs. 3 Satz 1 GG (Dürig/Herzog/Scholz, Grundgesetz 106. EL Oktober 2024, Art. 5 Abs. 3 Rn. 129). Daher war er im vorliegenden Fall als natürliche Person anspruchsberechtigt.

Aufforderung zur Beseitigung eines Verstoßes

Da die Beschwerdegegnerin auch nach Mitteilung meiner Rechtsauffassung an der Ablehnung des Antrags festhielt, forderte ich sie gemäß § 89 Abs. 3 Satz 3 HDSIG auf, Ihren Verstoß gegen die Informationsfreiheit innerhalb einer angemessenen Frist zu beheben.

Zudem informierte ich nach § 89 Abs. 3 Satz 4 HDSIG die zuständige Aufsichtsbehörde.

§ 89 Abs. 3 Sätze 3 und 4 HDSIG

Stellt die oder der Hessische Informationsfreiheitsbeauftragte Verstöße gegen die Vorschriften des Vierten Teils fest, kann sie oder er ihre Behebung in angemessener Frist fordern. Darüber ist die zuständige Aufsichtsbehörde zu unterrichten.

Wie mich der Beschwerdeführer zum Zeitpunkt der Erstellung des Berichts informierte, nahm die Behörde, bei der die Informationen angefragt wurden, Kontakt zu ihm auf. Es bleibt abzuwarten, ob die beantragten Informationen nunmehr erteilt werden.

5. Arbeitsstatistik Informationsfreiheit

Im Vergleich zum Vorjahr nahmen sowohl die Beschwerden als auch die Beratungen zu.

IFG	2024	2025
Beschwerden	65	**84**
Beratungen	51	**49**

Anhang zu II

Ausgewählte Materialien der Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) aus dem Jahr 2025

1. Entschließungen

1.1
Entschließung zwischen der 47. und 48. IFK zu: Mehr Transparenz und Open Data nach der Bundestagswahl! vom 13.3.2025

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/47_48_Konferenz_Entschließung-Bundestagswahl.pdf?__blob=publicationFile&v=3

1.2
Pressemitteilung anlässlich der Koalitionsverhandlungen der 21. Legislaturperiode des Deutschen Bundestags zu: Abschaffung der Informationsfreiheit auf Bundesebene völlig falscher Weg! vom 28.3.2025

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/Pressemitteilung-Koalitionsverhandlung-2025.pdf?__blob=publicationFile&v=3

1.3
Entschließung der 48. IFK zu: Transparenz bei Wahlleitungen klar regeln! vom 18.6.2025

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/48_Konferenz_Entschließung-Wahlleiter.pdf?__blob=publicationFile&v=4

1.4
Entschließung der 48. IFK zu: Protokolle der öffentlichen Sitzungen der Kommunalparlamente offenlegen! vom 18.6.2025

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/48_Konferenz_Entschließung-Kommunalordnung.pdf?__blob=publicationFile&v=3

1.5
Entschließung der 49. IFK zu: Privat finanzierte Forschung an Hochschulen muss transparenter werden! vom 26.11.2025

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/IFG/AGID_IFK/49_Konferenz_Entschließung-Forschung.pdf?__blob=publicationFile&v=2

Verzeichnis der Abkürzungen

Abkürzung	ausgeschriebene Schreibweise
2FA	Zwei-Faktoren-Authentisierung
a. A.	andere Ansicht
Abs.	Absatz
AG	Amtsgericht
AK	Arbeitskreis
Art.	Artikel
Art.	Artikel, mehrere
Aufl.	Auflage
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BMG	Bundesmeldegesetz
Bspw.	beispielsweise
BT-Drucks.	Bundestags-Drucksache
BTLE	Borders, Travel & Law Enforcement (Subgroup)
Buchst.	Buchstabe
BVerfG	Bundesverfassungsgericht
BvR	Aktenzeichen für eine Bundesverfassungsbeschwerde
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa
Co.	Company
CoC	Verhaltensregeln für die Prüf- und Speicherfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien vom 24.05.2025
DAkkS	Deutsche Akkreditierungsstelle GmbH
d. h.	das heißt

DIN	Deutsches Institut für Normung
DOC	Department of Commerce (US-Handelsministerium)
DPA	Data Protection Addendum, Datenschutznachtrag
DSFA	Datenschutz-Folgenabschätzung
DS-GVO, DSGVO	Datenschutz-Grundverordnung
DSK	Konferenz der unabhängigen Datenschutzaufsichts-behörden des Bundes und der Länder; kurz: Datenschutzkonferenz
Ed.	Edition
EDSA	Europäischer Datenschutzausschuss
EDSB	Europäischer Datenschutzbeauftragte
EfA	Einer für Alle
EL	Ergänzungslieferung
E-Mail	electronic mail
ErwGr	Erwägungsgrund
etc.	et cetera
EU	Europäische Union
EuG	Europäisches Gericht
EuGH	Gerichtshof der Europäischen Union
EU-US DPF	EU-US Data Privacy Framework
e. V.	eingetragener Verein
eWoG	Wohngeldfachverfahren
EWR	Europäischer Wirtschaftsraum
f.	folgende
ff.	folgende (Seiten) / fortfolgende
gem.	gemäß
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GVBl	Gesetz- und Verordnungsblatt für das Land Hessen

HArchivG	Hessisches Archivgesetz
HBDI	Hessischer Beauftragter für Datenschutz und Informa--tionsfreiheit
HDSIG	Hessisches Datenschutz- und Informationsfreiheits-gesetz
HGO	Hessische Gemeindeordnung
HKO	Hessische Landkreisordnung
HLT	Hessischer Landtag
HMdI	Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz
HMKB	Hessisches Ministerium für Kultus, Bildung und Chancen
HMVEVW	Hessisches Ministerium für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum
HMWVW	Hessisches Ministerium für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum
HSchG	Hessisches Schulgesetz
HSOG	Hessisches Sicherheits- und Ordnungsgesetz
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
IDPC	Information and Data Protection Commissioner (nationale Datenschutzbehörde Malta)
i. d. R.	in der Regel
IFK	Konferenz der Informationsfreiheitsbeauftragten
IKU	Inkassounternehmen
INA	Innenausschuss des Hessischen Landtags
inkl.	inklusive
insb.	insbesondere
i. S. d.	im Sinne der/des
i. V. m.	in Verbindung mit
IP-Adresse	Internetprotokoll-Adresse
ISO	International Organization for Standardization

IT	Information Technologie
IT-System	Informationstechnisches System
Kap.	Kapitel
KI	Künstliche Intelligenz
KI-VO	KI-Verordnung
KommJur	Kommunaljurist (Zeitschrift)
KTE	Kompetenzzentrum für Telemedizin & E-Health
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie
lit.	Litera, Buchstabe
LG	Landgericht
LfV Hessen	Landesamt für Verfassungsschutz Hessen
LLM	Large Language Model (Großes Sprachmodell)
Ltd.	Limited
LT-Drs.	Landtags-Drucksache
LTDrucks	Landtags-Drucksache
m. E.	meines Erachtens
M365	Microsoft 365
MeldDÜV	Verordnung über Datenübermittlungen der Melde-behörden
MHD	Mindesthaltbarkeitsdatum
MFA	Mehr-Faktoren-Authentisierung
ML	maschinelles Lernen
m. w. N.	mit weiteren Nachweisen
Nachlief.	Nachlieferung
NJW	Neue juristische Wochenschrift
Nr.	Nummer
o. g.	oben genannt/oben genannte/oben genannter
OLG	Oberlandesgericht
OWASP	Open Web Application Security Projects
OWiG	Gesetz über Ordnungswidrigkeiten

OZG	Onlinezugangsgesetz
PDF	Portable Document Format
PIMS	Personal Information Management Systeme
PNR	Passenger Name Record
RAG	Retrieval Augmented Generation
RBStV	Rundfunkbeitragsstaatsvertrag
Rdnr./Rn.	Randnummer
RED	Rechtsextremismus-Datei
RED-G	Rechtextremismus-Datei-Gesetz
Rn.	Randnummer
Rs.	Rechtssache
S.	Seite *oder* Satz
s.	siehe
SchDSV	Verordnung über die Verarbeitung personenbezogener Daten durch Schulen und Schulaufsichtsbehörden (Schul-Datenschutzverordnung)
SDM	Standard-Datenschutzmodell
Sept.	September
SIM-Karte	Subscriber Identity Module-Karte
S/MIME	Secure / Multipurpose Internet Mail Extensions
sog.	sogenannte/sogenannter/sogenanntes
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TB	Tätigkeitsbericht
TDDDG	Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz)
TLS	Transport Layer Security
TOM	Technisch-organisatorische Maßnahmen
u. a.	unter anderem

UAbs.	Unterabsatz
UAG	Unterarbeitsgruppe
URL	Uniform Resource Locator
Urt.	Urteil
UWG	Gesetz gegen den unlauteren Wettbewerb
VG	Verwaltungsgericht
vgl.	vergleiche
VO	Verordnung
WoGG	Wohngeldgesetz
WoGZustG	Hessisches Wohngeldzuständigkeitsgesetz
WoGZustV	Hessische Wohngeldzuständigkeitsverordnung
WWW	World Wide Web
z. B.	zum Beispiel
ZD	Zeitschrift für Datenschutz
Ziff.	Ziffer
ZUM	Zeitschrift für Urheber- und Medienrecht

Register der Rechtsvorschriften

Zitiert werden die jeweils zum Bearbeitungszeitpunkt geltenden Fassungen.

Gesetz/Vorschrift	Fundstelle(n)
AsylbLG	Asylbewerberleistungsgesetz in der Fassung der Bekanntmachung vom 5. August 1997 (BGBl. I S. 2022), zuletzt geändert durch Artikel 8 Absatz 3 des Gesetzes vom 23. Dezember 2024 (BGBl. 2024 I Nr. 449)
ATDG	Antiterrordateigesetz vom 22. Dezember 2006, zuletzt geändert durch Art. 2 Abs. 1 G v. 30. März 2021 I 402
BGB	Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), zuletzt geändert durch Artikel 14 des Gesetzes vom 23. Oktober 2024 (BGBl. 2024 I Nr. 323)
BDSG	Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), zuletzt geändert durch Artikel 10 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858)
BDSG	BDSG-neu (Gesetzentwurf der Bundesregierung, Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes, Stand: 31. Januar 2024)
BMG	Bundesmeldegesetz vom 3. Mai 2013 (BGBl. I S. 1084), zuletzt geändert durch Artikel 6 des Gesetzes vom 23. Oktober 2024 (BGBl. 2024 I Nr. 323)
BO	Berufsordnung für die Ärztinnen und Ärzte in Hessen (Stand: 2022) vom 26. März 2019 (HÄBL 6/2019, S. 396), geändert am 30. November 2021 (HÄBL 1/2022, S. 46), zuletzt geändert am 26. November 2024 (HÄBL 1/2025, S. 62)
BORA	Berufsordnung für Rechtsanwälte, erlassen von der Satzungsversammlung der Bundesrechtsanwaltskammer, zuletzt geändert durch Beschluss der Satzungsversammlung vom 26. Mai 2025
BRAO	Bundesrechtsanwaltsordnung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 303-8, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 4 des Gesetzes vom 22. Dezember 2025 (BGBl. 2025 I Nr. 349)
DGA	Verordnung (EU) 2022/868 des Europäischen Parlaments und Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)

DSA	Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste) (ABl. EU L 277/1)
DS-GVO	Verordnung (EU) 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 L 119 S. 1)
EU-Fluggastrechteverordnung 261/2004	Verordnung (EG) Nr. 261/2004 des Europäischen Parlaments und des Rates vom 11. Februar 2004 über eine gemeinsame Regelung für Ausgleichs- und Unterstützungsleistungen für Fluggäste im Fall der Nichtbeförderung und bei Annullierung oder großer Verspätung von Flügen und zur Aufhebung der Verordnung (EWG) Nr. 295/91
GG	Grundgesetz vom 23. Mai 1949 zuletzt geändert durch Art. 1 ÄndG (Art. 82) vom 19. Dezember 2022 (BGBl. I S. 2478)
GDNG	Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz – GDNG) vom 22. März 2024 (BGBl. 2024 I Nr. 102, Nr. 102 a)
HArchivG	Hessisches Archivgesetz (HArchivG) vom 13. Oktober 2022
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 3. Mai 2018 (GVBl. S. 82), in Kraft gesetzt am 25. Mai 2018, geändert durch Art. 5 des Gesetzes vom 12. September 2018 (GVBl. S. 570)
HDSIG	Hessisches Datenschutz- und Informationsfreiheitsgesetz vom 3. Mai 2018 (GVBl. S. 82), in Kraft gesetzt am 25. Mai 2018, geändert durch Art. 9 des Gesetzes vom 15. November 2021 (GVBl. S. 718, 729)
HGO	Hessische Gemeindeordnung in der Fassung der Bekanntmachung vom 7. März 2005, zuletzt geändert durch Artikel 1 des Gesetzes vom 1. April 2025 (GVBl. 2025 Nr. 24)
HKO	Hessische Landkreisordnung in der Fassung der Bekanntmachung vom 7. März 2005, zuletzt geändert durch Artikel 2 des Gesetzes vom 1. April 2025 (GVBl. 2025 Nr. 24)
HSchG	Hessisches Schulgesetz vom 17. Dezember 2022, zuletzt geändert durch Gesetz vom 28. März 2023 (GVBl. S. 183, 216)
HSOG – alt	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung vom 14. Januar 2005 (GVBl. I S. 14); FFN 310-63, zuletzt geändert durch Art. 10 Hess. Ausländer-TeilhabeG Kommunalpolitik vom 7. Mai 2020 (GVBl. S. 318)

HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung vom 14. Januar 2005 (GVBl. I S. 14); FFN 310-63, zuletzt geändert durch Art. 2, Art. 4 G zur Änd. sicherheitsrechtlicher Vorschriften und zur Umorganisation der hessischen Bereitschaftspolizei vom 29. Juni 2023 (GVBl. S. 456)
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung vom 14. Januar 2005 (GVBl. I S. 14) FFN 310-63, zuletzt geändert durch Art. 1 G zur Stärkung der Inneren Sicherheit in Hessen vom 13. Dezember 2024 (GVBl. Nr. 83)
HVSG	Hessisches Verfassungsschutzgesetz (HVSG) in der Fassung vom 20. Juli 2023 (GVBl. S. 614) FFN 18-7; Neubekanntmachung des HVSG vom 25. Juni 2018 (GVBl. S. 302) in der ab 12. Juli 2023 geltenden Fassung
IFG	Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz – IFG) vom 5. September 2005, zuletzt geändert durch Art. 44 V v. 19. Juni 2020 (BGBl. 2020. 1328)
KI-Verordnung	Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 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)
KunstUrhG	Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, zuletzt geändert durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266)
MDR	Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates vom 5. April 2017 über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates.
MeldDüV	Verordnung über Datenübermittlungen der Meldebehörden (Meldedatenübermittlungsverordnung – MeldDüV) vom 3. September 2023
OZG	Onlinezugangsgesetz vom 14. August 2017 (BGBl. I S. 3122, 3138), zuletzt geändert durch Artikel 1 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245)
ProdSG	Produktsicherheitsgesetz vom 27. Juli 2021 (BGBl. I S. 3146, 3147), geändert durch Artikel 2 des Gesetzes vom 27. Juli 2021 (BGBl. I S. 3146)

RBStV	Rundfunkbeitragsstaatsvertrag vom 15.–21. Dezember 2010, zuletzt geändert durch den Medienstaatsvertrag vom 14. bis 28. April 2020, in Kraft getreten am 7. November 2020, Hess. GVBl. 2020 S. 607 ff.
RED-G	Rechtsextremismus-Datei-Gesetz vom 20. August 2012 (BGBl. I S. 1798), zuletzt geändert durch Artikel 2 Absatz 2 des Gesetzes vom 30. März 2021 (BGBl. I S. 402)
SchDSV	Verordnung über die Verarbeitung personenbezogener Daten durch Schulen und Schulaufsichtsbehörden (Schul-Datenschutzverordnung – SchDSV) vom 1. Dezember 2023
SGB II	Sozialgesetzbuch (SGB) Zweites Buch (II) – Bürgergeld, Grundsicherung für Arbeitsuchende (Artikel 1 des Gesetzes vom 24. Dezember 2003, BGBl. I S. 2954)
StGB	Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), zuletzt geändert durch Artikel 2 Abs. 2 des Gesetzes vom 7. November 2024 (BGBl. I S. 351)
StPO	Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), zuletzt geändert durch Art. 2 des Gesetzes vom 26. Juli 2023 (BGBl. I Nr. 203)
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. Mai 2024 (BGBl. 2024 I Nr. 149)
UKlaG	Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz – UKlaG), neugefasst durch B. v. 27. August 2002 BGBl. I S. 3422, 4346, zuletzt geändert durch Artikel 18 G. v. 8. Dezember 2025 BGBl. 2025 I Nr. 318; Geltung ab 1. Januar 2002; FNA: 402-37 Nebengesetze zum Recht der Schuldverhältnisse
UWG	Gesetz gegen den unlauteren Wettbewerb; Gesetz vom 3. Juli 2004 (BGBl. I S. 1414), zuletzt geändert durch Gesetz vom 24. Juni 2022 (BGBl. I S. 959) m. W. v. 1. August 2022
VAG	Gesetz über die Beaufsichtigung der Versicherungsunternehmen (Versicherungsaufsichtsgesetz) vom 1. April 2015, zuletzt geändert durch Art. 11 G v. 27. Dezember 2024 (BGBl. 2024 I Nr. 438)
WoGG	Wohngeldgesetz vom 24. September 2008 (BGBl. I S. 1856), zuletzt geändert durch Artikel 50 des Gesetzes vom 2. Dezember 2024 (BGBl. 2024 I Nr. 387)
WoGZustG	Gesetz zur Bestimmung der zuständigen Stellen für die Durchführung des Wohngeldgesetzes (Wohngeldzuständigkeitsgesetz – WoGZustG) vom 11. Juli 2024*

WoGZustV	Verordnung über die Zuständigkeiten zur Ausführung des Wohngeldgesetzes (Wohngeldzuständigkeitsverordnung – WoGZustV) vom 30. Oktober 2012
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

A

E

H

I

J

K

L

M

N

O

P

U

V

Z