Der Landesbeauftragte für den Datenschutz Niedersachsen

Tätigkeitsbericht 2024

Niedersachsen

Der Landesbeauftragte für den Datenschutz Niedersachsen

30. Tätigkeitsbericht 2024

Impressum

Herausgeber
Der Landesbeauftragte für den Datenschutz Niedersachsen
Prinzenstraße 5, 30159 Hannover
Postfach 221, 30002 Hannover

Verantwortlich
Denis Lehmkemper

Redaktion
Achim Barczok | Marius Engelskirchen | Hagen Benke

Layout
Thomas Kupas | design@in-fluenz.de
Lavesstraße 20/21, 30159 Hannover

Bildnachweis
Adobe Stock: Titelbild (FotoStuss), Seite 19 (Dmitry), Seite 29 (your123), Seite 41 (Robert Kneschke), Seite 47 (your123), Seite 55 (Aleksandr Simonov), Seite 129 (bongkarn), Seite 149 (StockPhotoPro), Seite 159 (flashmovie), Seite 173 (finecki), Seite 191 (nmann77), Seite 199 (Liudmyla)
Daniel George: Seite 8
Dietmar Gust: Seite 207
LfD Niedersachsen: Seiten 61, 203, 209

Das Titelbild zeigt den Leuchtturm „Kleiner Preuße“ am Wremer Granatkutterhafen im Landkreis Cuxhaven.

Druck
Landesamt für Geoinformation und Landesvermessung Niedersachsen
Grafik-Service
Podbielskistraße 331, 30659 Hannover

A Vorwort

Die Vorlage des Tätigkeitsberichts ist für die gesamte Datenschutzbehörde stets ein Höhepunkt im Jahreslauf. Schließlich bietet der Bericht die Möglichkeit, die Arbeit des Hauses zu schildern und das Erreichte darzustellen. Dass der Bericht zunächst den Abgeordneten des Niedersächsischen Landtages und anschließend der Landespressekonferenz vorgestellt wird, gibt zusätzlich Raum, über Datenschutz und Datenschutzthemen zu informieren. Das ist umso wichtiger, da der Datenschutz zurzeit von vielen Seiten unter Druck steht. Oft heißt es: Nur mit weniger Datenschutz sei mehr innere Sicherheit möglich, oder: Nur mit weniger Datenschutz könnten ganze Wirtschaftszweige mit der internationalen Konkurrenz mithalten, oder: Nur mit weniger Datenschutz könnte der Staat effizienter arbeiten. Es wird Sie nicht wundern, dass ich das nicht so sehe. Das Gegenteil ist richtig: Effektive Sicherheitspolitik, innovative Wirtschaft, moderne Verwaltung schließen einen wirksamen Datenschutz nicht aus, sie bedingen ihn sogar.

Für das Verhältnis zwischen Staat und Bürgerinnen und Bürgern gilt: Nur wenn der Staat die Grundrechte, zu denen auch das Grundrecht auf informationelle Selbstbestimmung – kurz: das Datenschutz-Grundrecht – gehört, achtet und Eingriffe sorgsam abwägt, sie im besten Sinne verhältnismäßig vornimmt, wird es ihm gelingen, Akzeptanz für die situativ notwendigen Eingriffe zu erhalten. Ganz ähnlich ist es im Verhältnis zwischen Unternehmen und Bürgerinnen und Bürgern. Zurecht legen die Menschen in vielen Bereichen großen Wert darauf, dass auch Unternehmen mit ihren Daten ordentlich, also letztlich datenschutzgerecht umgehen. So gesehen ist Datenschutz kein Hindernis, sondern Qualitätsmerkmal, ja Garant einer modernen und zukunftsfähigen Gesellschaft. Dies gilt es nicht zuletzt auch bei allen Überlegungen zur Neustrukturierung der Datenschutzaufsicht, wie sie beispielsweise im Koalitionsvertrag auf Bundesebene anklingen, im Blick zu behalten.

Die Niedersächsische Datenschutzaufsicht ist für Bürgerinnen und Bürger, Behörden, Einrichtungen und Unternehmen erster Ansprechpartner in Sachen Datenschutz. So konnten und können wir mit einem starken, kooperativen Datenschutz in Niedersachsen viel erreichen und so manche innovative Datennutzung begleiten. Wir verstehen es als unsere Aufgabe, nicht in erster Linie Probleme aufzuzeigen, sondern vor allem durch Beratung praxisnahe Lösungen zu fördern. Das wollen wir auch in Zukunft tun.

Dies ist ein hoher Anspruch und es gibt hier auch nach wie vor viel zu tun. In meinem ersten Jahr als Landesbeauftragter für den Datenschutz habe ich zahlreiche Gespräche geführt, mit Bürgerinnen und Bürgern, mit Unternehmensverbänden, Behörden, Gewerkschaften und vielen mehr. Besonders oft ging es dabei um Künstliche Intelligenz (KI).

Das Tempo, mit dem KI in unseren Alltag vordringt, ist rasant. Der Europäische Gesetzgeber hat im vergangenen Jahr die KI-Verordnung verabschiedet. Sie ist in Teilen bereits anwendbar, schafft an vielen Stellen Klarheiten und setzt Regeln.

Um diesen Herausforderungen zu begegnen, haben wir im vergangenen Jahr eine Stabsstelle für Künstliche Intelligenz in unserer Behörde eingerichtet. In den von uns initiierten KI-Expertengesprächen haben wir Akteure aus der niedersächsischen Wirtschaft, Verwaltung, Gesellschaft und Forschung zusammengebracht. Ziel war es auch hier, Antworten zu finden auf offene Fragen zu KI und Datenschutz – etwa für den Umgang mit personenbezogenen Daten in Trainingsdaten, im Output von KI-Systemen und mit den Betroffenenrechten. Mehr dazu lesen Sie im Schlaglicht auf Seite 29.

Besonders freue ich mich, dass wir aktiv an einem praxisorientierten KI-Projekt in Niedersachsen teilnehmen: dem KI-Reallabor CRAI in Osnabrück. Dieses Reallabor soll vertrauenswürdige KI für den Mittelstand entwickeln. Wir begleiten das Reallabor aktiv, um kontinuierlich praxisnahe Erkenntnisse für das Zusammenspiel von Datenschutz und KI zu gewinnen.

Neben KI rückt ein weiteres Thema zunehmend in den Fokus: der Umgang mit Gesundheitsdaten im digitalen Zeitalter. Einerseits bietet die Digitalisierung in diesem Bereich enorme Chancen für Wissenschaft und Forschung – und auch für Patientinnen und Patienten. Andererseits bestehen hohe

Risiken, wenn sensible Gesundheitsdaten nicht ausreichend geschützt sind. Auch hier gilt: Innovation braucht den Datenschutz.

Bescheiden fällt die Bilanz aber bei einigen wichtigen Gesetzesvorhaben aus, allen voran beim Beschäftigtendatenschutz. Leider ist es dem Bundesgesetzgeber in der vergangenen Legislaturperiode wieder nicht gelungen, ein modernes Gesetz zu verabschieden, das den besonderen Gegebenheiten im Arbeitsverhältnis angemessen Rechnung trägt. Weil uns das wichtig ist, setzen wir uns dennoch weiter dafür ein, dass Beschäftigte nicht durch überbordende Kontrolle zum gläsernen Mitarbeiter gemacht werden. Regelungen dazu sollte sich der neu gewählte Bundestag vornehmen und ich kann die Niedersächsische Landesregierung nur ermuntern, etwa durch einen Antrag im Bundesrat, die Stimme zu Gunsten eines modernen, bürokratiearmen und zugleich effizienten Beschäftigtendatenschutzgesetzes zu erheben.

Noch viele andere spannende Themen haben uns im zurückliegenden Jahr beschäftigt. Häufig ist es gelungen, unterstützend zu begleiten, manches Mal mussten wir auch als Ordnungsbehörde tätig werden und Verstöße spürbar ahnden. Aber insgesamt ist es – so denke ich – gelungen, für die Belange des Datenschutzes zu sensibilisieren und den Bürgerinnen und Bürgern, Unternehmen und Verbänden zu helfen.

An dieser Stelle möchte ich Danke sagen an meine Kolleginnen und Kollegen, die auch im vergangenen Jahr viele Projekte angeschoben haben und sich mit großer Leidenschaft für den Datenschutz engagieren – egal, ob es um die IT-forensische Untersuchung einer Datenschutzpanne oder die Prüfung einer Beschwerde geht. Gemeinsam setzen wir uns auch in Zukunft für einen starken Datenschutz ein.

Und zum Schluss danken möchte ich auch unseren vielen Partnerinnen und Partnern in Verwaltung, Forschung, Politik, Wirtschaft und Gesellschaft. Der Austausch mit ihnen bereichert unsere Arbeit.

Ich wünsche Ihnen viele interessante Erkenntnisse und eine spannende Lektüre unseres 30. Tätigkeitsberichts.

Ihr Denis Lehmkemper

Empfehlungen des Landesbeauftragten für den Datenschutz Niedersachsen B

Digitale Souveränität – Die Unabhängigkeit der öffentlichen Verwaltung ist wichtiger denn je

Viel zu zaghaft hält die Idee einer digitalen Souveränität Einzug in die politische Agenda. Einer der ersten konkretisierenden Startpunkte war der Beschluss des nationalen IT- Planungsrates vom Frühjahr 2020 zur „Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung, Eckpunkte – Ziel und Handlungsfelder". In der „Strategie zur digitalen Transformation der Verwaltung des Landes Niedersachsen", beschlossen im Oktober 2023, wird dazu festgestellt: „Um die digitale Handlungsfähigkeit sicherzustellen, ist es erforderlich, darauf zu achten, dass eine maximale Flexibilität beim Einsatz von Informationstechnologie erreicht wird. Grundlage bilden dabei offene Standards beim Einsatz von Hardware und Software".

Doch wie steht es um die Umsetzung dieser Anforderungen? Im vergangenen Jahr schloss die niedersächsische Landesverwaltung einen großvolumigen Vertrag mit Microsoft zur cloudbasierten Ausstattung der Büroarbeitsplätze mit Kommunikations- und Kollaborationsfunktionen, zum Beispiel über Microsoft Teams, ab. Die Tatsache, dass die niedersächsische Datenschutzaufsicht nach umfangreichen Nachverhandlungen und unter zahlreichen Auflagen für die betreibenden Stellen den Einsatz für datenschutzrechtlich akzeptabel erklärt hat, soll nicht darüber hinwegtäuschen, dass eine zwar europäische, aber proprietäre Cloud – Stichwort EU Data Boundary – keine wirklich digital souveräne Lösung ist. Das Gegenteil ist der Fall: Die „single vendor strategy" der Landesverwaltung in diesem Bereich birgt die Gefahr, in immer tiefere Abhängigkeiten zu geraten und könnte über sogenannte „lock-in"-Effekte, die unerwünschte Bindung an Hersteller und Dienste noch ausweiten. Gerade dieser Gefahr aber soll durch die beschlossene Strategie der digitalen Transformation eigentlich explizit entgegengewirkt werden.[1]

1 Vgl. Strategie zur digitalen Transformation der Verwaltung des Landes Niedersachsen unter https://niedersachsen.online/dokumente/

Die aktuellen digital- und geopolitischen Entwicklungen, insbesondere der transatlantischen Beziehungen, machen es erforderlich, die Bedeutung digitaler Souveränität Europas, Deutschlands und letztlich Niedersachsens neu zu bewerten. Sich schnell wandelnde Wertvorstellungen und ein vermeintliches oder tatsächliches Vormachtstreben, das an die Stelle von echter Partnerschaft zu treten scheint, werfen ein neues, besorgniserregendes Licht auf die marktbeherrschende Dominanz einiger Big Tech-Konzerne.

Die öffentliche Hand muss gerade vor diesem Hintergrund handlungsfähig bleiben. Durch die Abhängigkeit von einigen wenigen IT-Produkten und -Diensten droht mehr denn je die Einschränkung der Handlungsfreiheiten der öffentlichen Verwaltung durch die faktische Ausübung äußerer politischer und wirtschaftlicher Macht. Darüber kann auch die derzeit geplante Idee einer „deutschen proprietären souveränen Cloudlösung" nur dann hinweghelfen, wenn sie wirksam, nachhaltig und dauerhaft von den bestehenden Abhängigkeiten wegführt. Im Moment scheint es so, als sei eine souveräne und proprietäre deutsche Cloudlösung allenfalls als eine Zwischenlösung auf dem Weg in eine offene, digital souveräne Cloudlösung denkbar.

Ein erfolgreiches Konzept zur Stärkung der digitalen Souveränität muss über alle Ebenen hinweg und von allen relevanten Akteuren gleichermaßen und gemeinsam entwickelt und verwirklicht werden.

Ebenenübergreifende Zusammenarbeit

Die Umsetzung der digitalen Souveränität beginnt auf der politischen Ebene. Die Voraussetzungen für digital souveräne IT-Infrastrukturen müssen zunächst durch die entsprechenden gesetzlichen Rahmenbedingungen geschaffen werden. Dabei ist es auch Teil der politischen Dimension, zu akzeptieren, dass digitale Souveränität nicht zum Nulltarif zu haben sein wird. Eine digital souveräne Lösung wird nicht immer die billigste Option sein. Jedoch kann ein Defizit an digitaler Eigenständigkeit und die damit verbundenen Risiken für die öffentlichen Aufgaben nicht mit den finanziellen Vorteilen geringerer Kosten begründet werden. Es braucht hier eine grundsätzliche und selbstverständliche Anforderung an Technologieanbieter, dass digitale Souveränität die zentrale Bedingung ist. Dies wird auch bedeuten können, dass diese – für den Staat notwendige – Unabhängig-

keit kurzfristig möglicherweise teurer ist, sich jedoch langfristig auszahlen wird.

Einen vielversprechenden Weg birgt die deutsche Verwaltungscloud-Strategie (DVS), die durch Modularität, Kompatibilität und Interoperabilität von Cloud-Lösungen, deren Austausch- und Wiederverwendbarkeit ermöglichen soll. Für die Realisierung solch eines föderalen Cloud-Verbundes werden in der DVS herstellerunabhängige, modulare Architekturen sowie ebenenübergreifende offene Standards und Schnittstellen[2] für Entwicklung, Inbetriebnahme und Betrieb von Cloud-Anwendungen in engen fachlichen Austausch mit bestehenden Entwicklungen und Aktivitäten definiert. Hier müssen sich die CIOs[3] von Bund und Ländern sowie die IT-Verantwortlichen der Kommunen und die öffentlichen IT-Dienstleister aktiv einbringen, um neben den technologischen Herausforderungen auch die erforderlichen Skaleneffekte für tragfähige und gleichzeitig wirtschaftliche Lösungen zu erstellen.

Somit ist die digitale Souveränität eine Herkulesaufgabe, bei der der Gesetzgeber, die Landesregierung, die Verwaltung und die Digitalwirtschaft in eine gemeinsame Richtung gehen müssen. Dabei sollte der Datenschutz als wichtige Voraussetzung für Freiheit und Grundrechtsschutz in einer pluralistischen und demokratischen Gesellschaft betrachtet werden, der nur in einer digital souveränen Infrastruktur nachhaltig sichergestellt werden kann.

Gelingt das Vorhaben aber, kann es Vorbild sein auch für die Wirtschaft und große Verbandsstrukturen – und trägt in jedem Fall zur Stärkung der Sicherheit und Souveränität unseres Landes bei, weit über die eigentlichen IT-Anwendungen hinaus.

2 Beispielsweise im Bereich der Containerisierung.

3 Chief Information Officer: Verantwortlicher für Strategie und Implementierung von Informationstechnologie in einer Organisation bzw. einem Unternehmen.

C Das Wichtigste in Kürze

Auch das Jahr 2024 war erneut von intensiven Diskussionen um Datenschutzaspekte bei der Nutzung von Künstlicher Intelligenz geprägt. Die rasant steigende Leistungsfähigkeit von KI-Systemen und ihr breiter Einsatz in verschiedenen Anwendungsfeldern bietet große Chancen, stellt aber auch den Datenschutz vor neue Herausforderungen. Ein weiteres wichtiges Thema war die Videoüberwachung, insbesondere durch Privatpersonen, aber auch durch Livestreams, die in einem Fall sogar Aufnahmen von einem FKK-Strand hochauflösend ins Internet übertrugen.

Unsere Behörde hat sich im Berichtszeitraum intensiv mit Künstlicher Intelligenz (KI) beschäftigt. Im August 2024 trat die europäische KI-Verordnung (KI-VO) in Kraft. Da die Datenschutz-Grundverordnung (DSGVO) nach den Festlegungen der KI-Verordnung unberührt bleibt, stellt sich nicht die Frage der Anwendung der DSGVO auf KI-Systeme. Es bleibt aber eine Herausforderung, die Regeln der DSGVO bei KI-Systemen wirksam umzusetzen. Bei Privaten wie auch bei öffentlichen Akteuren bestand hierzu ein erheblicher Beratungsbedarf durch unsere Behörde.

Um diesen Beratungsanfragen kompetent zu begegnen, haben wir eine Stabsstelle zum Thema KI eingerichtet. Zudem haben wir Fachleute aus Wirtschaft, Verwaltung, Forschung und Gesellschaft zu einem insgesamt dreimal tagenden Expertenkreis einberufen. In diesem Fachgremium diskutierten wir zentrale Fragen zur Einhaltung der Datenschutzgrundsätze beim Training von KI-Modellen, zu Bias-Mechanismen und der Qualität von KI-Outputs allgemein.

Erneuter Beschwerdeschwerpunkt Videoüberwachung

Im aktuellen Berichtszeitraum stieg die Zahl der Beschwerden im zweiten Jahr in Folge erneut an. In 2024 erreichten uns über 2.300 Beschwerden und damit rd. 7 % mehr als im Vorjahr (sowie rd. 20 % Steigerung gegenüber 2022). Viele der Beschwerden richteten sich gegen die unberechtigte Veröffentlichung von personenbezogenen Daten in Social Media-Plattfor-

men, gegen Datenschutzverstöße im Bereich des Direktmarketings und im Beschäftigtenverhältnis. Auffällig viele Beschwerden bezogen sich erneut auf den Bereich der Videoüberwachung. Dies betraf sowohl die Videoüberwachung durch Privatpersonen, aber auch touristische Webcams, die teils mehr aufzeichneten und ins Internet streamten, als datenschutzrechtlich zulässig war. So erreichten uns Hinweise auf Kameras, die dauerhaft Aufnahmen von privaten Wohngebäuden, Marktplätzen und sogar einem FKK-Strand in das Internet übertrugen. Aufgrund mehrerer Beschwerden überprüften wir zudem wieder gezielt Fitnessstudios und mussten dort in einigen Fällen erneut gravierende Datenschutzverstöße im Bereich der Videoüberwachung durch nicht-öffentliche Stellen feststellen.

Digitalisierung im Gesundheitswesen

Ein weiteres Schwerpunktthema war die Digitalisierung des Gesundheitswesens. So haben wir intensiv die Vorbereitungen zur Einführung der elektronischen Patientenakte (ePA) begleitet und hierzu FAQ zu rechtlichen Fragen, wie etwa der Widerspruchsmöglichkeit für Versicherte veröffentlicht.

Als wichtigen Schritt für mehr Vertraulichkeit bei der Kommunikation im Medizinwesen kann die seit Juli 2024 verpflichtende Nutzung des KIM-Dienstes („Kommunikation im Medizinwesen“) gewertet werden. Die datenschutzrechtlich problematische Übertragung von Dokumenten wie Arztbriefen, Befunden oder Heilplänen via Fax und unverschlüsselter E-Mail gehört damit endgültig der Vergangenheit an. Der KIM-Dienst ermöglicht nunmehr einen sicheren, da hardwareseitig Ende-zu-Ende verschlüsselten und elektronisch signierten Kommunikationsweg.

Verarbeitung von Fahrzeugdaten – Herausforderungen für den Datenschutz

Als zuständige Datenschutzbehörde für die Volkswagen AG haben wir 2024 ein Verfahren zur Erhebung, Übermittlung und Weiterverarbeitung von Sensordaten aus Fahrzeugen von Volkswagen begleitet. Datenpakete aus diesem Verfahren, die zur Verbesserung der Fahrassistenz- und Fahrsicherheitssysteme genutzt werden, können personenbezogene Daten enthalten. Daher informierte VW uns frühzeitig über die neuen Prozesse, um die datenschutzrechtlichen Rahmenbedingungen abzustimmen.

Digitalisierung in der Verwaltung

Ein hoher Beratungsbedarf bestand auch in diesem Berichtszeitraum wiederum bei Behörden und öffentliche Stellen bei Datenschutzfragen zu Digitalisierungsvorhaben. Schwerpunkte waren hier das novellierte Online-Zugangsgesetz (OZG 2.0) und die hiermit eng verzahnte Registermodernisierung – beides wichtige Bausteine auf dem Weg der Digitalisierung in der Verwaltung.

Eng begleitet haben wir auch das Niedersächsische Ministerium für Inneres und Sport bei seinen Vertragsverhandlungen mit Microsoft zur Nutzung der Plattform Teams für die Landesverwaltung. Dabei ging es um die DSGVO-konforme Abbildung der Auftragsverarbeitung von MS Teams durch Microsoft in der Cloud. Die Vertragsverhandlungen zwischen dem Innenministerium und Microsoft wurden im April 2024 abgeschlossen. Wir konnten feststellen, dass diese Verhandlungen unter der Maßgabe der Einhaltung entsprechender Vorgaben zu einem datenschutzrechtlich akzeptablen Ergebnis geführt haben. Es gibt also nach wie vor keinen generellen datenschutzrechtlichen Freifahrtschein für den Einsatz von MS 365-Produkten wie Teams, wohl aber einen Weg zu deutlich mehr Rechtssicherheit für die verantwortlichen Stellen.

Datenschutz beim Einsatz von Tablets an Schulen

In Niedersachsen erfolgt die Finanzierung von Tablets an Schulen nach wie vor hauptsächlich durch Eltern, was jedoch datenschutzrechtliche Fragen aufwirft, da Kinder diese privaten Geräte dann auch privat nutzen: Eltern sorgen sich über die Möglichkeit eines umfassenden Zugriffs schulischer Administratoren auf die personenbezogenen Daten auf den Geräten. Zudem sind weitere technische und sicherheitsrelevante Fragen noch immer ungelöst. Ziel der nunmehr zwischen uns und dem Niedersächsischen Kultusministerium verabredeten Vorgehensweise muss es sein, Datenschutz und digitale Bildung miteinander in Einklang zu bringen.

Medienkompetenz an Schulen

Können Schülerinnen und Schüler zwischen wahren und falschen Inhalten unterscheiden? Wie können sie ihren Medienkonsum reflektiert steu-

ern und sicher mit ihren personenbezogenen Daten im Netz wie auch der analogen Welt umgehen? Medien- und Datenschutzkompetenz sind im digitalen Zeitalter entscheidende Schlüsselqualifikationen. Obwohl junge Menschen als Digital Natives scheinbar routiniert mit digitalen Medien umgehen, fehlt es mitunter an einem fundierten Verständnis möglicher Risiken. Die niedersächsische Datenschutzaufsicht legt seit 2024 einen besonderen Fokus auf Datenschutz- und Medienkompetenz für Kinder und Jugendliche, um den sicheren Umgang mit den eigenen Daten zu fördern und Cybergefahren dadurch zu begegnen.

Start des Überwachungszentrums für norddeutsche Länder

Ein bedeutendes Projekt war der Start des neuen Rechen- und Dienstleistungszentrums zur Telekommunikationsüberwachung (RDZ-TKÜ) der norddeutschen Küstenländer. Nach zehnjähriger Planungsphase wurde im Dezember 2024 der Teil-Betrieb aufgenommen. Unsere Behörde war während der gesamten Entwicklung beratend involviert.

Der Produktivstart erfolgte Ende 2024, bis Mitte 2025 sollen alle beteiligten Länder angebunden sein, wodurch das veraltete System abgelöst wird. In unserer beratenden Rolle werden wir die Datenschutzkonformität in diesem sensiblen Bereich weiterhin begleiten.

Ausführlichere Informationen zu diesen Themen lesen Sie in den entsprechenden Beiträgen des Tätigkeitsberichts.

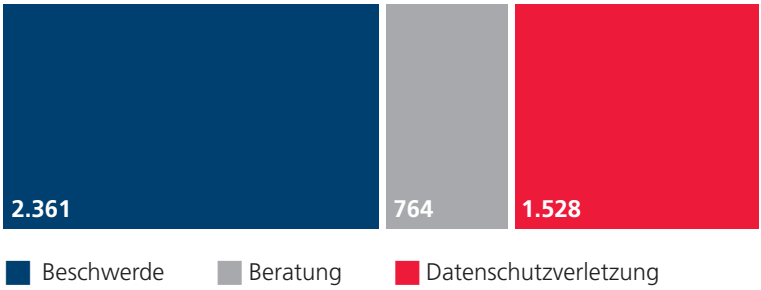
D Zahlen und Fakten

D.1 Blick in die Zahlen: Beschwerden, Datenpannen und Bußgelder

Auch im Jahr 2024 erreichten uns erneut mehr Datenschutzverletzungen und Beschwerden im Vergleich zum vorangegangenen Berichtsjahr. So stieg die Zahl der Beschwerden um rund 7 Prozent, die Zahl der uns gemeldeten Datenschutzverletzungen sogar um gut 17 Prozent.

Als Datenschutzaufsichtsbehörde sind wir erster Anlaufpunkt für verantwortliche Stellen und Datenschutzbeauftragte zu Fragestellungen des Datenschutzrechts. Darüber hinaus setzen wir die Datenschutzgesetzgebung durch Abhilfe- und Vollzugsmaßnahmen durch, immer mit dem Ziel, die Rechte und Freiheiten natürlicher Personen zu schützen.

A1 – Beschwerden, Beratungsanfragen und Datenschutzverletzungen 2024



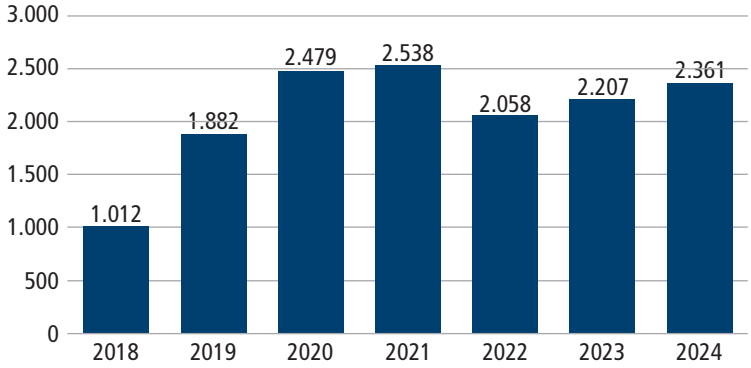
Beschwerden

Im Jahr 2024 gingen bei uns in Summe 2.361 Beschwerden von Bürgerinnen und Bürgern ein. Dies entspricht einem Anstieg um gut 7 Prozent zum vorangegangenen Berichtsjahr. Erneut gab es zahlreiche Beschwerden zu Videoüberwachung, vor allem durch Privatpersonen, also beispielsweise aufgrund von großflächig aufzeichnenden Kameras in der Nachbarschaft. Mehrere Beschwerden erreichten uns auch zu verspätet oder unvollständig

erteilten Auskünften über die jeweils gespeicherten personenbezogenen Daten.[1]

Weiterer häufiger Beschwerdegrund: unerwünschte Kontaktaufnahmen – in der Regel zu Werbezwecken. Dabei wurden uns überwiegend nicht erwünschte E-Mails gemeldet, aber auch Werbeanschreiben per Post, beispielsweise aus dem Bereich des Dialogmarketings. Da hier vielfach kein (Geschäfts-)Kontakt mit der werbenden Stelle bestand, vermuteten die Beschwerdeführenden in solchen Fällen – meist zurecht – einen Verstoß gegen den Datenschutz.

A2 – Zahl der Beschwerden 2018 bis 2024



Abermals erreichten uns leider auch eine Vielzahl von Beschwerden zur unberechtigten Veröffentlichung von personenbezogenen Daten im Internet, vorrangig in den sozialen Medien. Da dies einen erheblichen Eingriff in die Persönlichkeitsrechte der Betroffenen darstellt, hat unsere Behörde hierzu in der Regel Verfahren eröffnet. Ebenfalls wandten sich erneut Beschäftigte an uns, weil sie sich an umfassender Kameraüberwachung von Verkaufs- und Aufenthaltsflächen störten, die sie und andere Mitarbeitende unablässig aufzeichneten.

Datenschutzverletzungen

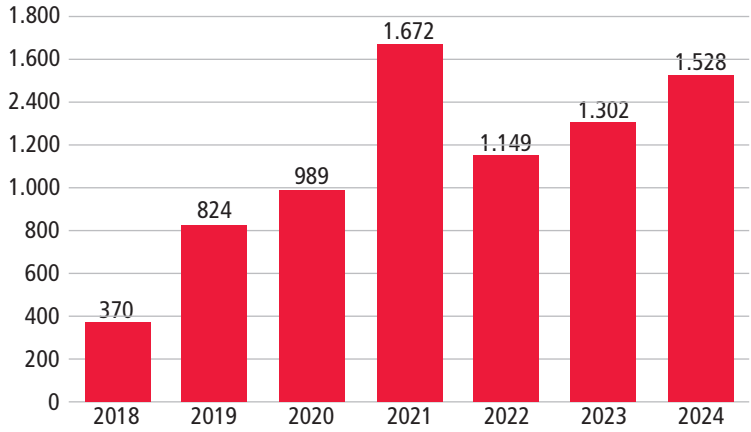
Bei einer Verletzung des Schutzes personenbezogener Daten gibt die Datenschutz-Grundverordnung (DSGVO) vor, dass der Verantwortliche für die

1 Entsprechend des Auskunftsrechts nach Artikel 15 DSGVO.

Datenverarbeitung dies an die zuständige Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden meldet, nachdem ihm die Verletzung bekannt wurde.[2] Dies ist allerdings nur notwendig, wenn die Verletzung voraussichtlich zu einem (nicht nur geringen) Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Auch im Berichtsjahr 2024 haben wir einen Anstieg der Meldungen von Datenschutzverletzungen festgestellt, um gut 17 Prozent im Vergleich zum Vorjahr auf insgesamt 1.528 Meldungen.

A3 – Gemeldete Datenschutzverletzungen 2018 bis 2024



Seit Anwendungsbeginn der DSGVO im Jahr 2018 zeigt sich in den Fallzahlen ein kontinuierlicher Anstieg der gemeldeten Datenschutzverletzungen. Ein Ausreißer im Jahr 2021 erklärt sich mit einer Sicherheitslücke in einer weit verbreiteten Software, zu der uns damals eine Vielzahl an Meldungen von verschiedenen Unternehmen erreichte.[3]

Der kontinuierliche Anstieg legt mehrere Ursachen nahe: Zum einen führt die beständig zunehmende Digitalisierung vieler Lebensbereiche zu einer höheren Wahrscheinlichkeit, von einer Datenpanne oder einer unberechtigten Datenverarbeitung betroffen zu sein.

2 Art. 33 DSGVO.
3 Siehe Tätigkeitsbericht 2021: Seite 168.

Zum anderen wird sechs Jahre nach Anwendbarkeit der DSGVO einem zunehmenden Teil der Verantwortlichen der Umgang mit ihren datenschutzrechtlichen Pflichten geläufiger sein, so dass der Meldepflicht von Datenschutzverletzungen konsequenter nachgekommen wird.

Und drittens haben in diesem Zeitraum auch Cyberangriffe durch Kriminelle auf Unternehmen, öffentliche Stellen und auch Privatpersonen zugenommen, die bei Erfolg häufig mit Datenabflüssen und damit oft Datenschutzverletzungen einhergehen.

Verhängte Geldbußen des LfD

Im Jahr 2024 hat die niedersächsische Datenschutzaufsicht Geldbußen insgesamt in Höhe von 1,04 Millionen Euro erlassen.[4] Dies waren 56 Erstbescheide in Bußgeldsachen, die sich teilweise aber auch auf Fälle aus dem vorangegangenen Jahr bezogen, da eine Bußgeldentscheidung nicht immer in dem Jahr ergeht, in welchem die Sache bei der Behörde eingegangen ist.

Die Erstbescheide zu Geldbußen aus dem Jahr 2024 bezogen sich vor allem auf Datenschutzverletzungen durch Verantwortliche aus den Bereichen Gesundheitswesen, Finanzdienstleistungen, Gastgewerbe und Einzelhandel.

4 Siehe Kapitel H zu abgeschlossenen Bußgeldverfahren.

D.2 Beteiligung an Gesetzgebungsverfahren: Gegenstand und Zeitpunkt entscheidend

Auch 2024 haben wir uns an einer Vielzahl von Gesetzgebungsverfahren beteiligt. Wie läuft so ein typisches Gesetzgebungsverfahren eigentlich ab? Zu welchem Zeitpunkt sollte oder muss die Beteiligung unseres Hauses erfolgen?

Klare und eng umrissene Gesetzesregelungen zur Verarbeitung von personenbezogenen Daten, beispielsweise zu einer möglichen Übermittlung, sichern nicht nur den Datenschutz für die Betroffenen ab. Sie gewährleisten auch Rechtssicherheit für diejenigen, die das Gesetz anwenden werden. Beispielsweise bei Datenübermittlungen sind daher gesetzlich klar erkennbare zulässige Empfänger und eindeutig definierte Voraussetzungen die Grundlage für nachvollziehbare und praktikabel anzuwendende Gesetze.

Eine Beteiligung unseres Hauses an Gesetzgebungsvorhaben der Landesregierung, besonders wenn Datenschutzaspekte berührt sind, ist nicht nur Teil des vorgesehenen Gesetzgebungsprozesses[1], sondern stellt auch eine Erleichterung für die im Vorfeld beteiligten Ministerien dar. Dahinter steht das Prinzip, dass wir die jeweiligen federführenden Fachreferate mit dem gezielten Blick für hinreichend konkrete Regelungen zur Datenverarbeitung unterstützen können. Die Beteiligung zu diesem Zeitpunkt kommt immer der Anwendbarkeit des Gesetzes zugute.

Gesetzesentwürfe des Landes werden im Regelfall von der Landesregierung in den Landtag eingebracht.[2] Das Verfahren, das ein Gesetzesentwurf innerhalb der Landesregierung und der Ministerien auf diesem Weg durchläuft, ist in der Gemeinsamen Geschäftsordnung der Landesregierung und der Ministerien in Niedersachsen (GGO) festgelegt. Der mehrstufige Prozess enthält folgende Schritte:

1 Art. 57 Abs. 1 Buchst. c DSGVO und §§ 9, 24, 31 Gemeinsame Geschäftsordnung der Landesregierung und der Ministerien in Niedersachsen (GGO).

2 Gemäß Art. 42 Abs. 3 Niedersächsische Verfassung können Gesetzesentwürfe darüber hinaus aus der Mitte des Landtags oder durch Volksinitiativen beziehungsweise Volksbegehren eingebracht werden.

Zunächst erstellt das federführende Ministerium einen sogenannten Referentenentwurf. Im Rahmen der Ressortbeteiligung soll die Datenschutzaufsicht als oberste Landesbehörde bereits formlos eingebunden werden, wenn Datenschutzaspekte betroffen sind.[3]

Anschließend erfolgt die erste Kabinettsbefassung, bei der der Regierungsentwurf von der Landesregierung zur Verbandsbeteiligung freigegeben wird. Hier ist nun unser Haus auch förmlich zu beteiligen, insbesondere wenn Datenschutz spezifisch betroffen ist.[4]

Sofern die Stellungnahmen der Verbandsbeteiligung zu Änderungen am Gesetzesentwurf führen, welche Auswirkungen auf den Datenschutz haben, ist im Rahmen einer erneuten Ressortbeteiligung auch unser Haus nochmals zu beteiligen.

Abschließend erfolgt die sogenannte zweite Kabinettsbefassung, die sich also auf den zweiten Regierungsentwurf des Gesetzes bezieht. Die Kabinettsvorlage muss hierbei das Ergebnis der Anhörung unseres Hauses enthalten, sofern das Gesetz das Recht auf informationelle Selbstbestimmung berührt.[5] Dieser zweite Regierungsentwurf wird nun an den Landtag überwiesen.

Vor allem wenn eine geplante Gesetzesregelung sich spezifisch auf Datenschutzbelange bezieht, ist eine frühzeitige Beteiligung unseres Hauses auf der sogenannten Referentenebene sinnvoll. Im Berichtsjahr wurden wir beispielsweise frühzeitig bei einem Gesetzgebungsvorhaben im Gesundheitsbereich eingebunden und konnten hierdurch in diesem frühen Stadium unsere Anmerkungen einbringen.

3 § 24 GGO.
4 § 31 GGO.
5 § 9 Absatz 1 Nummer 5 Buchstabe c GGO.

Im Jahr 2024 haben wir zu folgenden Rechtssetzungsvorhaben Stellung bezogen:

Gesetze des Landes

Gesetz über die Landwirtschaftskammer Niedersachsen (LwKG)
Gesetz zum Zweiten Staatsvertrag zur Änderung des IT-Staatsvertrags
Gesetz zur Änderung des Niedersächsischen Gesetzes zur Ausbildung der Juristinnen und Juristen (NJAG)
Niedersächsisches Beamtengesetz (NBG)
Niedersächsisches Bildungszeitgesetz (NBildZG)
Niedersächsisches Brandschutzgesetz (NBrandSchG)[6]
Niedersächsisches Datenschutzgesetz (NDSG)
Niedersächsisches Disziplinargesetz (NDiszG)
Niedersächsisches Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke (NPsychKG)
Niedersächsisches Gesetz zur Ausbildung der Juristinnen und Juristen (NJAG)
Niedersächsisches Katastrophenschutzgesetz (NKatSG)[7]
Niedersächsisches Schiedsämtergesetz (NSchÄG)
Niedersächsisches Schlichtungsgesetz (NSchlG)
Niedersächsisches Verfassungsschutzgesetz (NVerfSchG)

Verordnungen, Richtlinien, Erlasse und sonstige Regelungen des Landes

Lehrverpflichtungsverordnung (LVVO)
Niedersächsische Beurteilungsverordnung (Nds. BeurtVO)

6 Siehe ausführlich Kapitel G.1.4.
7 Siehe ausführlich Kapitel G.1.4.

Niedersächsische Reisekostenverordnung (NRKVO)
Niedersächsische Verordnung über die Einführung der elektronischen Aktenführung im Bußgeldverfahren bei den Bußgeldbehörden im Land Niedersachsen (NEBußAktEV)
Niedersächsische Verordnung über die maschinelle Führung und die elektronische Einreichung der Tabellen nach § 175 Abs. 1 der Insolvenzordnung (Nds. InsOeTabVO)
Niedersächsische Verordnung über die technischen und organisatorischen Rahmenbedingungen für die elektronische Aktenführung im Bußgeldverfahren (NBußAktFV)
Niedersächsische Verordnung zur elektronischen Aktenführung bei den Gerichten (Nds. eAktGerVO)

Gesetze und Verordnungen des Bundes oder anderer Länder

Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG)[8]
Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)
Registerzensusgesetz (RegZensG)
Sozialgesetzbuch (SGB) - Achtes Buch (VIII)
Vertrag über die Errichtung, den Betrieb und die Weiterentwicklung des Nationalen Once-Only-Technical-Systems (NOOTS) – Vertrag zur Ausführung von Art. 91c Abs. 1, Abs. 2 GG – NOOTS-Staatsvertrag[9]

8 Siehe ausführlich Kapitel I.5.
9 Siehe ausführlich Kapitel G.6.2.

Fazit

Eine frühzeitige Einbindung der Datenschutzaufsichtsbehörde kommt allen Beteiligten zugute: Die Fachreferate der Ministerien erhalten frühzeitig Planungssicherheit in dem oft knappen Zeitplan. Für diejenigen, die das Recht zukünftig anwenden, entsteht Rechtssicherheit durch klare, handhabbare Regelungen – und die Betroffenen erhalten einen wirkungsvollen Schutz ihrer personenbezogenen Daten.

E Schlaglicht: KI-Expertengespräche

KI-Expertengespräche: Datenschutz beim Training und Output von KI gewährleisten

Der KI-Expertenkreis des LfD Niedersachsen hat in drei Gesprächsterminen wesentliche datenschutzrechtliche Aspekte bei der Entwicklung und dem Einsatz von Künstlicher Intelligenz diskutiert. Aus diesen Gesprächen konnte unsere Behörde wichtige Erkenntnisse für ein datenschutzkonformes Training sowie einen datenschutzkonformen Einsatz von KI-Anwendungen gewinnen. Der nachstehende Bericht fasst die Aussagen und Ergebnisse der Gesprächsrunden zusammen. Die Auswertung und abschließende Bewertung durch uns erfolgte nach dem Berichtszeitraum.

Die KI-Verordnung erklärt die Datenschutz-Grundverordnung (DSGVO) vollumfänglich neben der KI-Verordnung für anwendbar. Folgerichtig sind daher abgesehen von einigen sehr wenige Ausnahmen in der KI-Verordnung keine spezifischen Datenschutzvorschriften enthalten. Das führt zu ganz neuen Herausforderungen.

Die Datenschutzaufsichtsbehörden überprüfen daher die Datenschutzkonformität anhand der Vorgaben der DSGVO. Als Exekutivorgan steht ihnen zwar durch die Auslegungskompetenz ein gewisser Spielraum zu, dieser stößt allerdings bei KI-Anwendungen an seine Grenzen. Es wird deutlich, wie schwer es ist, allein durch Auslegung der DSGVO dem Thema KI gerecht zu werden.

Zudem ist die datenschutzrechtliche Durchsetzung gegenüber außereuropäischen KI-Anbietern kaum möglich – selbst, wenn eine Zuständigkeit der deutschen Aufsichtsbehörden gegeben ist. Um einerseits Entwicklung und Einsatz von KI-Anwendungen in Deutschland zu ermöglichen und so die Zukunftsfähigkeit des Wirtschaftsstandorts nicht zu gefährden, und andererseits dem Datenschutz zur Geltung zu verhelfen, sind konstruktive Lösungsansätze erforderlich.

KI-Expertengespräche: Ziele und Vorgehensweise

Ziel des von unserer Behörde einberufenen Expertenkreises war es, Rahmenbedingungen für den datenschutzkonformen Einsatz von KI in der Wirtschaft wie auch in der niedersächsischen Verwaltung zu auszuloten. An den Expertengesprächen nahmen Vertreter führender Institutionen aus der niedersächsischen Wirtschaft und Wissenschaft, der öffentlichen Verwaltung und Datenschutzexperten aus dem gesellschaftlichen Umfeld teil. Wir haben diese interdisziplinäre Zusammensetzung gewählt, um die Datenschutzfragen von KI-Systemen aus unterschiedlichen Perspektiven betrachten zu können.[1]

Vor allem die Wissenschaftler aus dem technischen Bereich konnten wichtige Ansätze für eine Transformation der datenschutzrechtlichen Anforderungen in technische Maßnahmen beitragen. Bei den Experten aus Verwaltung und Wirtschaft standen dagegen die konkreten Bedarfe für einen KI-Einsatz in der Praxis und diesbezügliche Ansätze für die Gewährleistung des Datenschutzes im Vordergrund.

Die drei Expertengespräche waren den folgenden Kernthemen gewidmet:

1. Rechtmäßigkeit des Trainings von KI-Modellen
2. Gewährleistung der Datenschutzgrundsätze, insbesondere der Transparenz, Fairness, Datenminimierung und Speicherbegrenzung in KI-Systemen
3. Grundsatz der Richtigkeit personenbezogenen Outputs und Bias-Mechanismen bei KI-Systemen

Diese Kernthemen betreffen potenziell alle KI-Systeme, bei deren Entwicklung oder Nutzung personenbezogene Daten verarbeitet werden. Entsprechend waren KI-Systeme, bei denen keine Verarbeitung personenbezogener Daten erfolgt, nicht Gegenstand der Expertengespräche.

Wenngleich wir die ganze Vielfalt an KI-Modellen und KI-Systemen betrachtet haben, lag der Schwerpunkt der Erörterungen häufig auf den Large Language Models (LLMs), die derzeit ihren großen Durchbruch erleben. Das Wissen über konkrete Entwicklungsschritte, Funktionen und Funktionsweisen basiert selbstverständlich auf bekannten Produkten.

1 Mehr zu den Expertengesprächen auf unserer Webseite unter https://www.lfd.niedersachsen.de/234172.html und https://www.lfd.niedersachsen.de/238007.html (Pressemitteilungen).

Vor allen von den Experten aus der Forschung und den Unternehmen wurde jedoch hervorgehoben, dass deren Interessenschwerpunkte nicht ausschließlich bei Chatbots und LLMs liege. Künstliche Intelligenz weise noch enorme Entwicklungspotenziale auf, die gegenwärtig noch nicht abgeschätzt werden könnten. Dies betrifft sowohl KI-Modelle mit allgemeinem Verwendungszweck, wie es die LLMs sind, als auch KI-Systeme, die den Einsatz von KI-Modellen in einem spezifischen und konkreten Anwendungsbereich ermöglichen. Die bisherigen Erkenntnisse insbesondere aus der Entwicklung von LLM sollten demnach zugrunde gelegt werden, um zukünftige KI-Entwicklungen durch datenschutzrechtliche Vorgaben zu beeinflussen.

Bei einer typischen Datenschutzprüfung wird die Verarbeitung personenbezogener Daten in einem Verfahren in seine Teilschritte zerlegt und die jeweiligen Teilschritte datenschutzrechtlich bewertet. Dies können beispielsweise Teilvorgänge wie die Erhebung, Speicherung, Sortierung oder auch die Übermittlung sein.

Die Datenschutzaufsichtsbehörden nehmen auch bei KI-Systemen eine differenzierte Prüfung vor und unterscheiden in die Verarbeitungstätigkeiten beim Training von KI-Modellen, dem KI-Modell als solchen und der Nutzung eines KI-Systems. Beispielsweise wird ein LLM entwickelt, indem ein neuronales Netz mit sehr vielen Datensätzen trainiert wird. Das neuronale Netz eines LLMs enthält selbst auch Daten, die personenbezogen sein können. Schließlich werden bei der Nutzung eines KI-Systems, zum Beispiel einer KI basierten Übersetzungssoftware insbesondere Ein- und Ausgabedaten verarbeitet. Diese können aufgrund des durch den Nutzer vorgegebenen Kontextes datenschutzrechtlich relevant sein.

Der Expertenkreis hat diesen Ansatz einer phasenweisen Betrachtung von KI-Modellen und KI-Systemen auch aus der technischen Perspektive als zielführend bestätigt. Entsprechend wurde bei den drei Expertengesprächen jeweils eine andere Verarbeitungstätigkeit in der chronologischen Abfolge Entwicklung, Bereitstellung und Nutzung von KI-Modellen bzw. KI-Anwendungen in den Fokus gerückt. In den Expertengesprächen konnten so bezogen auf eine konkrete Verarbeitungstätigkeit im KI-Lebenszyklus Ansätze für deren datenschutzfreundlichere Ausgestaltung gefunden werden.

Rechtmäßigkeit des Trainings von KI-Modellen

Das Training von KI-Modellen erfordert in sehr großem Umfang Trainingsdatensätze. Sobald in diesen Trainingsdatensätzen personenbezogene Daten enthalten sind, sind die rechtlichen Anforderungen der DSGVO zu berücksichtigen. Die KI-Verordnung enthält diesbezüglich lediglich punktuell ergänzende Vorgaben. Insbesondere sieht sie aber keine „erleichternden" Sonderregelungen zu den Rechtsgrundlagen der Datenschutz-Grundverordnung vor.

Beim Training von KI-Modellen – insbesondere von generativen Modellen – werden in der Regel mindestens zwei Trainingsphasen unterschieden. Zunächst wird das KI-Modell als solches trainiert oder anders gesagt „erschaffen". Vereinfacht umfasst diese Phase die Vorbereitung eines optimierten Trainingsdatensatzes, die Auswahl der Lernmethode wie zum Beispiel Deep Learning und die Durchführung des Trainings nach dem Prinzip Trial and Error.

Soll ein KI-Modell für einen bestimmten Anwendungsbereich eingesetzt werden, erfolgt regelmäßig ein sogenanntes Fine-Tuning. In dieser Trainingsphase wird das vortrainierte Modell für spezifische Aufgaben nachtrainiert und verfeinert. Datenschutzrechtlich können sich hier unterschiedliche Konstellationen der Verantwortlichkeit ergeben, je nachdem ob alle Phasen von einer Stelle durchgeführt werden oder unterschiedliche Akteure agieren.

Generative KI-Modelle werden ihrer Definition nach für sehr breite Anwendungsbereiche entwickelt, wie zum Beispiel die großen Sprachmodelle. Die Entwickler des Systems selbst können das Modell für ein konkrete KI-System einsetzen und vorab ein Fine-Tuning vornehmen. Für den Einsatz in Behörden und Unternehmen und je nach konkreten Einsatzzweck wird regelmäßig zudem ein Fine-Tuning durch die nutzenden Stellen erfolgen.

Die Rechtmäßigkeit des Trainings von KI-Modellen mit personenbezogenen Daten ist vor allem in der Diskussion, weil für die Entwicklung der großen generativen KI-Modelle die Trainingsdaten vornehmlich aus dem Web stammen. Die Daten werden durch Webscraping gesammelt und von spezialisierten Webscrapern als Datenbank zur allgemeinen Verfügbarkeit bereitgestellt. KI-Modelle können selbstverständlich auch mit anderen Trai-

ningsdatensätzen entwickelt werden, wie zum Beispiel den Datenbanken von Wetterdiensten, Fahrzeugdaten oder Forschungsdatenbanken.

Insbesondere wenn kein KI-Modell für einen allgemeinen, sondern einen sehr spezifischen Anwendungsbereich entwickelt werden soll, wird es hohe Anforderungen an die Qualität der Trainingsdatensätze geben, die die unspezifischen Trainingsdaten aus dem Web in der Regel nicht aufweisen. Sollten diese strukturierten Datenbanken personenbezogene Daten enthalten, wird eine Anonymisierung der Datensätze häufig mit verhältnismäßig geringem Aufwand umsetzbar sein.

In dem Expertengespräch wurde auch der Ansatz künstlich erzeugter Trainingsdaten, sogenannte synthetische Daten, diskutiert. Im Ergebnis kann – wenig überraschend – keine allgemeine Aussage darüber getroffen werden, ob synthetische Daten einen adäquaten Ersatz für Realdaten beim Training von KI-Modellen darstellen. Es wurde aber festgestellt, dass synthetische Daten grundsätzlich für das Training von KI-Modellen geeignet sein können. Die folgenden Kriterien beeinflussen die Eignung der synthetischen Daten:

- Anwendungsbereich des konkreten KI-Modells, zum Beispiel werden bei Bilderkennungsverfahren synthetische Daten genutzt, während sie im Anwendungsbereich der medizinischen Forschung nicht nutzbar seien,
- Herstellungsprozess der synthetischen Daten, insbesondere wenn sie selbst mit KI-Systemen erzeugt werden,
- ausschließliche oder ergänzende Nutzung von synthetischen Daten sowie
- der Einsatz beim initialen Training oder beim Fine-Tuning.

Stammen die Trainingsdaten aus dem Web, ist dem Entwickler des KI-Modells nicht bekannt, welche personenbezogenen Daten sich in den Datensätzen verbergen, wer die Betroffenen sind sowie wann, zu welchen Zweck und von wem die Daten im Web veröffentlicht worden sind.

All diese Informationen wären aber erforderlich, um die Voraussetzungen der gesetzlichen Rechtsgrundlagen in der DSGVO überprüfen zu können. In vielen Fällen ist zudem unklar, ob für das Training des KI-Modells überhaupt personenbezogene Daten erforderlich sind, wie zum Beispiel für eine KI-basierte Übersetzungsanwendung.

Bei den Trainingsdatensätzen aus dem Web besteht die Herausforderung, diese von personenbezogenen Daten zu bereinigen. Vor dem Training der großen LLMs sind Maßnahmen getroffen worden, um den Umfang personenbezogener Daten in den verwendeten Trainingsdaten aus dem Web zu reduzieren. Beispielsweise wurden Webseiten, die als Verzeichnis oder Sammlung personenbezogener Daten konzipiert sind (zum Beispiel checkpeople.com oder myheritage.com) identifiziert und entfernt sowie private E-Mail-Adressen auf Webseiten unkenntlich gemacht. Dies sind zwar für sich genommen sinnvolle Beispiele, dennoch ist offensichtlich, dass die getroffenen Maßnahmen nur im geringen Umfang dazu führen, dass personenbezogene Daten nicht für das Training des KI-Modells verwendet worden sind.[2]

Im KI-Expertengespräch wurde die Auffassung vertreten, dass insbesondere aus der technischen Perspektive diesbezüglich deutlich mehr Maßnahmen möglich sind. Allerdings würden solche Maßnahmen einen hohen Aufwand erfordern und sind kostenintensiv. Dazu käme, dass durch Politik, Gesellschaft und letztlich auch den Datenschutzaufsichtsbehörden insbesondere gegenüber den Anbietern großer Sprachmodelle aus Drittstaaten nicht genügend Handlungsdruck erzeugt werde, ein datenschutzkonformes Training durchzuführen. Es bestand zudem Einigkeit, dass erstens keine vollständige Anonymisierung der sehr großen Trainingsdatensätze erreicht werden könne und zweitens bei der Nutzung von KI-Modellen ein erhebliches Risiko der Deanonymisierung bestehe.

Unabhängig davon, welche Optimierungsstrategie letztlich verfolgt wird, ist ein datenschutzrechtlicher Regelungsbedarf festzustellen. Es wird KI-Modelle geben, die ohne ein Training mit massenhaften personenbezogenen Daten nicht auskommen. Welche datenschutzrechtlichen und datenschutzpolitischen Folgerungen sich daraus ergeben, bewerten wir gerade intern und werden uns dazu zu einem späteren Zeitpunkt äußern.

2 Die Problematik, dass auch besondere Kategorien personenbezogener Daten in den Trainingsdatensätzen enthalten sind und für deren rechtmäßige Verarbeitung eine Rechtsgrundlage gemäß Art. 9 Abs. 2 DSGVO gegeben sein müsste, wurde in dem Expertengespräch bewusst ausgeklammert.

Gewährleistung der Datenschutzgrundsätze in KI-Systemen

Es bestehen grundsätzliche Konflikte zwischen KI-Systemen und der Gewährleistung der in der DSGVO normierten Datenschutzgrundsätze.[3] Besonders augenfällig ist die Widersprüchlichkeit zwischen KI-Systemen und dem Grundsatz der Datenminimierung. Danach müssen personenbezogene Daten dem konkreten Zweck angemessen und erheblich sowie auf das für den konkreten Zweck einer Verarbeitung notwendige Maß beschränkt sein.

Im ersten Expertengespräch wurde zudem festgestellt, dass die datenschutzrechtlichen Grundsätze der Transparenz bei KI-Systemen eine besondere Herausforderung darstellen. Gemäß Art. 5 Absatz 1 Buchstabe a DSGVO sind personenbezogene Daten [auf rechtmäßige Weise,] nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise zu verarbeiten.

Nachvollziehbarkeit ist im Datenschutzrecht nicht allein durch die Erfüllung der Informationspflichten und Auskunftsansprüche zu gewährleisten. Sie erfordert darüber hinaus vertiefte Kenntnisse beim Verantwortlichen über die Systemgestaltung. Transparenz umfasst zumindest bei automatisierten Entscheidungen auch aussagekräftige Informationen über die „involvierte Logik" der Datenverarbeitung, „sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person". Diese Facette der Transparenz wird datenschutzrechtlich als Erklärbarkeit bezeichnet.

Die Ergebnisse der Diskussion zur Umsetzung des Grundsatzes der Datenminimierung war in Teilen deckungsgleich zu der Diskussion des ersten KI-Expertengesprächs zur Rechtmäßigkeit des KI-Trainings mit personenbezogenen Daten. Insbesondere für das Training großer KI-Modelle sind mehrere hundert Gigabyte an Daten erforderlich.

Je nach Zielsetzung von KI-Modell und Anwendungsdomäne sind in diesen Daten personenbezogene Daten enthalten oder nicht. Der Grundsatz der Datenminimierung fordert nur eine Reduzierung der personenbezogenen Daten. Diese kann grundsätzlich mit den gleichen Mitteln erreicht werden wie bei anderen IT-Systemen; im Fall von KI-Systemen vor allem durch eine

3 Gemäß Art. 5 Abs. 1 DSGVO.

Anonymisierung. Der Input von personenbezogenen Daten ist auf das erforderliche Maß zu reduzieren. Der Output von personenbezogenen Daten eines KI-Systems kann nur bedingt unmittelbar beeinflusst werden. Bei LLMs werden bereits teilweise Prompts (Eingaben oder Anfragen des Nutzers), die sich auf konkrete Personen beziehen, nicht beantwortet. Das KI-Modell kann zum Beispiel Namen erkennen und entsprechend reagieren. In der Diskussion stand auch die Möglichkeit, über Filtersysteme den Daten-Output zu beeinflussen. Grundsätzlich könnte so auch der Output personenbezogener Daten reduziert oder verhindert werden. Die Zuverlässigkeit der Filtersysteme ist aber noch verbesserungsbedürftig. Es besteht sogar die Vermutung, dass gerade die Verbesserung von Filtersystemen einem ständigen Optimierungsprozess unterliegen wird, und auf diese Weise auch der Datenschutz ständig verbessert werden kann.

In dem Expertengespräch zur Transparenz wurde deutlich, dass sich die Aussagen nicht immer auf den datenschutzrechtlichen Transparenzgrundsatz beschränkten. Dieser bezieht sich auf die Nachvollziehbarkeit der Verarbeitung personenbezogener Daten. Von den Experten wurde ausdrücklich auf den Unterschied zwischen Transparenz und Erklärbarkeit aus der technischen Perspektive hingewiesen. Demnach beziehe sich die Transparenz vornehmlich auf den Aufbau eines KI-Modells in Bezug auf das „Innenleben" – wie zum Beispiel die Anzahl der Schichten, der verwendeten Parameter, Token und der verwendeten Trainingsdaten. Erklärbarkeit meine dagegen, dass die Logik für den konkreten Output eines KI-Modells nachvollziehbar ist. Die Erklärbarkeit ist bei KI-Modellen, die auch als Black Box bezeichnet werden, im Unterschied zu herkömmlicher Software nicht gegeben. Transparenz erfordert eher allgemeine und abstrakte Systeminformationen. Erklärbarkeit bezieht sich demgegenüber auf konkrete Verarbeitungsvorgänge eines Systems und erfordert technisches Detailwissen. Demnach unterscheiden sich das datenschutzrechtliche und das technische Begriffsverständnis von Transparenz und Erklärbarkeit: datenschutzrechtliche Transparenz und Erklärbarkeit im Kontext automatisierter Entscheidungen entsprechen zusammengenommen dem technischen Verständnis von Transparenz.

Die Zielsetzung des datenschutzrechtlichen Transparenzgrundsatzes legt nahe, dass „nur" Transparenz, aber keine technische Erklärbarkeit in Bezug auf die Verarbeitung personenbezogener Daten gefordert wird. Betrof-

fenen müssen grundsätzlich insbesondere Kenntnis darüber haben, dass personenbezogene Daten für das Training eines bestimmten KI-Modells verwendet worden sind, welche Zielsetzung und welche Anwendungsbereiche dieses KI-Modell hat und personenbezogene Daten als Output ausgegeben werden können. Auch Informationen zu den im KI-Modellen festgelegten KI-Parametern kann für Betroffene relevant sein. Diese beeinflussen den Output von KI-Modellen. Zum Beispiel bestimmt der KI-Parameter Temperatur die Zufälligkeit der von der KI generierten Antworten.[4] Bei manchen KI-Systemen lassen sich die KI-Parameter von dem Nutzer einstellen; bei anderen werden die Parameter durch die Prompts vom Nutzer eher unbewusst angesprochen.

Des Weiteren bestand unter den Experten Einigkeit, dass der Grundsatz der Transparenz auch bei KI-Systemen stets aus der „Empfängersicht" zu betrachten sei. Mit Empfängern können allerdings sowohl Betreiber als auch Nutzer eines KI-Modells gemeint sein. Soweit diese für den Einsatz des KI-Modells datenschutzrechtlich verantwortlich sind, sind sie gegenüber Betroffenen selbst zur Transparenz verpflichtet. Das bedeutet, sie müssen grundsätzlich vom Entwickler des KI-Modells alle erforderlichen Informationen erhalten, um erstens beurteilen zu können, ob bei der Nutzung des KI-Modells oder KI-Systems die Anforderungen der Datenschutz-Grundverordnung eingehalten werden können. Zweitens müssen sie die Betroffenen informieren können. „Empfänger" sind daher auch die Betroffenen selbst, denen die Transparenz zur Durchsetzung ihrer Datenschutzrechte verhelfen soll. Im KI-Lebenszyklus gibt es daher aus der Datenschutzperspektive unterschiedliche „Empfänger", denen in unterschiedlichem Umfang Informationen über das KI-Modell zur Verfügung stehen müssen.

Schließlich wurde noch festgestellt, dass das Problem der Transparenz und Erklärbarkeit zwar bei Large Language Modellen bestehen würde, nicht aber bei allen KI-Modellen. So seien zum Beispiel neuro-symbolische Systeme sehr gut nachvollziehbar.

4 Eine hohe Temperatur führt dazu, dass das LLM auch unwahrscheinlichere Antwortmöglichkeiten einbezieht.

Grundsatz der Richtigkeit und Bias-Mechanismen

Das dritte und letzte Expertengespräch war weiteren Grundsätzen des Datenschutzrechts und einem Gesamtresümee gewidmet.

Der datenschutzrechtliche Grundsatz der Richtigkeit wurde in dem Expertengespräch ausschließlich in Bezug auf den Output von KI-Modellen und KI-Systemen diskutiert. Dabei haben wir zwei unterschiedliche Facetten betrachtet. Erstens: Wie kann proaktiv der Output falscher personenbezogener Daten verhindert werden? Zweitens: Wie kann reaktiv die Ausgabe falscher personenbezogener Daten für die Zukunft korrigiert werden? Nach dem gegenwärtigen Kenntnisstand kann der Output falscher personenbezogener Daten durch die Implementierung von auf Tests basierenden Filtern reduziert und teilweise auch korrigiert werden.

Bei großen generativen KI-Modellen wird diese Methode weniger erfolgreich sein, als bei kleineren KI-Modellen für spezifische Anwendungsbereiche. Letztlich kamen die Experten zu dem Ergebnis, dass trotz weiteren Maßnahmen die Richtigkeit des Outputs von den Entwicklern nicht garantiert werden kann. Ergänzend wurde darauf verwiesen, dass der menschlichen Nachkontrolle eine hohe Bedeutung zukomme.

Ein weiterer technischer Ansatz insgesamt zur Reduzierung des Outputs personenbezogener Daten und damit auch zur Minimierung des Risikos des Outputs falscher personenbezogener Daten sind Methoden der differential privacy. Dabei wird, vereinfacht gesagt, der Output gezielt um ein Rauschen im Sinne der Veränderung der Daten ergänzt, um eine höhere Abstrahierung und damit eine geringere Wahrscheinlichkeit der Personenbeziehbarkeit herbeizuführen. Nach Einschätzung der KI-Experten sei diese Methode allerdings sehr aufwendig und damit kostspielig. Bisher werde sie allenfalls im akademischen Bereich in Bezug auf KI-Modelle erprobt und es sei nach gegenwärtigem Kenntnisstand in den nächsten Jahren nicht mit einem verbreiteten Einsatz zu rechnen. Gleichwohl wurde diesbezüglich Potenzial für zukünftigen Verbesserungen des Datenschutzes bei KI-Modellen anerkannt.

Das neuronale Netz eines KI-Modells kann nachträglich kaum korrigiert werden. Die Ausgabe falscher personenbezogener Daten kann bei KI-Modellen nicht auf „falsche" im Modell gespeicherte Daten zurückgeführt werden. Technisch gibt es aber Ansätze der sogenannten erklärbaren KI.

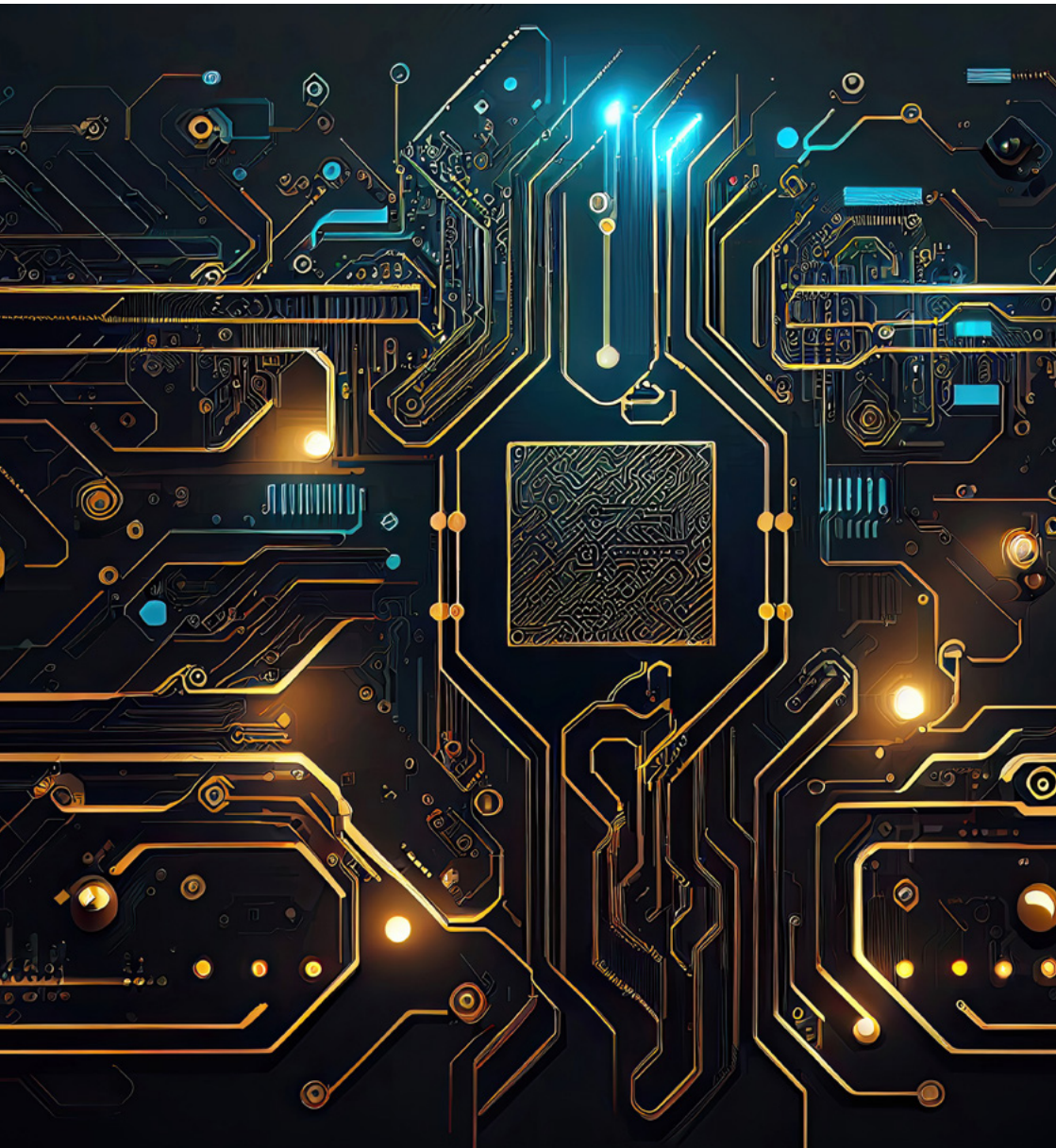
Dadurch soll die Nachvollziehbarkeit von Output-Daten erhöht werden. Ist bekannt, warum ein falsches Datum ausgegeben wird, können zumindest nachgeschaltete Filter die Anzeige solcher Daten beim Nutzer unterdrücken. Des Weiteren können KI-Modelle darauf trainiert werden, bei Wissensfragen im Zweifel nicht zu antworten.

Fazit

Die Expertengespräche zur Künstlichen Intelligenz waren der Versuch einer neuen Zusammenarbeit mit externen öffentlichen und nicht-öffentlichen Stellen. Wie auch der LfD Niedersachsen beschäftigten sich diese eingeladenen Experten intensiv mit dem neuen Thema der künstlichen Intelligenz – aus ihrer jeweils eigenen Perspektive. Insbesondere die eingebrachte technische Expertise und die daraus resultierenden Denkansätze, was technisch möglich wäre, sind sehr hilfreich für die KI-spezifische Konkretisierung datenschutzrechtlicher Anforderungen.

Der LfD Niedersachsen hat zudem einen guten Einblick in die Einsatzszenarien und die damit verbundenen Überlegungen der eingeladenen Institutionen erlangen können. Das neue Austauschformat wurde von allen Seiten begrüßt und als Erfolg gewertet.

F Schlaglicht: Beratung und Fortbildung durch den LfD



Beratung und Fortbildung durch die Datenschutzaufsicht Niedersachsen

In unserem Datenschutzinstitut schulen wir die Datenschutzbeauftragten der öffentlichen Stellen in Niedersachsen. Darüber hinaus haben sich zahlreiche Austauschformate mit Wirtschaftsverbänden, Kommunen, Vereinen und anderen Interessenvertretungen etabliert. Unser Ziel: Durch Prävention Datenschutzverstöße vermeiden, anstatt sie später ahnden zu müssen.

Die Datenschutzbehörden haben in erster Linie eine Aufsichts- und Durchsetzungsfunktion. Eine Beratungspflicht sieht die Datenschutz-Grundverordnung (DSGVO) vor allem gegenüber dem niedersächsischen Gesetzgeber vor.[1] Darüber hinaus unterstützt die Datenschutzaufsicht Niedersachsen regelmäßig Verantwortliche in öffentlichen Stellen und Wirtschaft mit Beratungs- und Fortbildungsangeboten.

Denn zum einen sollen die Datenschutzbehörden gemäß der DSGVO Verantwortliche und Auftragsverarbeiter für ihre datenschutzrechtlichen Pflichten und Aufgaben sensibilisieren.[2] Zum anderen zeigt die Erfahrung, dass wir mit solchen Beratungsangeboten präventiv Datenschutzverstöße vermeiden. Nicht zuletzt stärken proaktive Beratungsangebote das Vertrauen in die Datenschutzbehörden, fördern die Zusammenarbeit und damit einen starken Datenschutz in Niedersachsen.

Neben den zahlreichen Beschwerden und Hinweisen auf Datenschutzverstöße erreichen uns jährlich Hunderte von individuellen Beratungsanfragen. Da diese hohe Zahl an Beratungsanliegen mit den Ressourcen einer Landesdatenschutzbehörde kaum zu leisten ist, konzentrieren wir uns bei der Beratung auf die gebündelte Ansprache von Multiplikatoren und bieten gezielt Fortbildungen und Veranstaltungen für bestimmte Bereiche an, in denen ein besonderer Informationsbedarf besteht.

Hieraus sind verschiedene regelmäßige Austauschgespräche und Veranstaltungen entstanden, bei denen wir zu Datenschutzthemen informieren

1 Siehe dazu Kapitel D.2.
2 Art. 57 Abs. 1 Buchst. d DSGVO.

und Fragen beantworten. Beispielsweise treffen wir uns mit Unternehmensverbänden und Kammern. Zudem nehmen wir an den Erfahrungsaustauschkreisen der niedersächsischen Datenschutzbeauftragten teil. Etabliert haben sich auch die Netzwerktreffen der behördlichen Datenschutzbeauftragten, zum Beispiel der obersten Landesbehörden. Hinzu kommen der Runde Tisch im Gesundheitswesen[3] und diverse andere Termine etwa im Schul- und Hochschulbereich, an denen wir teilnehmen.

In drei Bereichen hat unsere Behörde im vergangenen Jahr Schwerpunkte gesetzt: Fortbildungen für Datenschutzbeauftragte im öffentlichen Bereich, Infoveranstaltungen für Vereine und die Unterstützung der niedersächsischen Kommunen.

Schulungen des Datenschutzinstituts Niedersachsen

Das Datenschutzinstitut Niedersachsen (DsIN) ist die zentrale Anlaufstelle für Datenschutzschulungen im öffentlichen Dienst des Landes. Es unterstützt Beschäftigte öffentlicher Stellen dabei, Kenntnisse im Datenschutz zu vertiefen. Im Jahr 2024 haben wir in diversen Kursen insbesondere behördliche Datenschutzbeauftragte geschult, die in ihren Institutionen als zentrale Ansprechpersonen für die Mitarbeitenden, aber auch für unsere Behörde fungieren. Mit einem vielseitigen Schulungsprogramm vermittelt das DsIN praxisnahes Wissen und trägt dazu bei, Datenschutzstandards in Verwaltungen und Schulen zu stärken.

Die angebotenen Schulungen decken sowohl rechtliche als auch technische Aspekte des Datenschutzes ab. Dazu gehörten 2024 die Kurse:

- Grundlagen des Datenschutzrechts für öffentliche Stellen
- Grundlagen des methodisch technisch-organisatorischen Datenschutzes
- Technisch-organisatorische Maßnahmen in der Praxis
- Sozialdatenschutz
- Datenschutz in Schulen
- Beschäftigtendatenschutz für Personalvertretungen

Besonders im schulischen Bereich stellen sich vielfältige Herausforderungen: Schulen müssen nicht nur den Schutz personenbezogener Daten von

3 Siehe Kapitel G.5.1.

Schülerinnen und Schülern gewährleisten, sondern auch den Einsatz digitaler Lern- und Lehrmittel datenschutzkonform gestalten. Die Schulungen des DsIN helfen dabei, Unsicherheiten im schulischen Alltag zu klären.

Datenschutz im Verein

Regelmäßig erreichen uns auch Anfragen und Beschwerden aus Vereinen. Neben klassischen Datenschutzfragen zur Mitgliederverwaltung und Datenlöschung werden uns auch immer wieder Pannen wie fehlerhafte E-Mail-Verteiler gemeldet. Besonders häufig treten Unsicherheiten bei der Speicherung und Löschung personenbezogener Daten auf.

Angesichts dieses hohen Beratungsbedarfs unterstützt unsere Behörde die Vereine seit einigen Jahren mit verschiedenen Angeboten. Die Vereinshotline ermöglicht die direkte Klärung datenschutzrechtlicher Fragen, während die kostenlose Online-Schulung „Datenschutz im Verein" Informationen zu praxisnahen Fällen in Vereinen vermittelt und konkret auf die Fragen der Teilnehmenden eingeht. Aufgrund der großen Nachfrage haben wir in diesem Jahr die Anzahl der Veranstaltungstermine deutlich erhöht und damit über 100 Ehrenamtliche aus niedersächsischen Vereinen schulen können.

Ergänzend dazu haben wir eine Handreichung veröffentlicht, die die wichtigsten datenschutzrechtlichen Anforderungen für Vereine kompakt zusammenfasst. Diese Handreichung sowie weitere Informationen finden Sie auf unserer Website unter https://lfd.niedersachsen.de/vereine.

Zusammenarbeit mit den Kommunen

Unsere Behörde versteht sich als aktiver Partner der niedersächsischen Landkreise, Städte und Gemeinden, um sie bei der Umsetzung datenschutzrechtlicher Anforderungen zu unterstützen. Dabei verfolgen wir zusammen mit den kommunalen Akteuren das Ziel, bereits im Vorfeld von Datenschutzvorfällen zu helfen und so einen effektiven Schutz personenbezogener Daten zu gewährleisten.

Auch hier haben sich regelmäßige Treffen mit den Datenschutzbeauftragten der Kommunen etabliert. Diese Gespräche sind ein wichtiges Forum, in dem die Behörde auf spezifische Fragen der Kommunen eingehen kann.

Viele Fragen gab es im Jahr 2024 in diesen Runden zum datenschutzkonformen Einsatz von Microsoft Teams und zu den Informations- und Dokumentationspflichten.

Regelmäßig erreichen uns auch Fragen zur ordnungsgemäßen Veröffentlichung von Dokumenten. Hier befinden sich die Kommunen in einer besonderen Situation, da sie einerseits aus Transparenzgründen Stellungnahmen und Ähnliches veröffentlichen und andererseits dabei regelmäßig mit personenbezogenen Daten umgehen.

Eine Rechtsgrundlage für die Veröffentlichung personenbezogener Daten im Internet gibt es nur in besonderen Ausnahmefällen. Liegt keine wirksame Einwilligung vor, müssen solche Daten daher in der Regel vor der Veröffentlichung in den Dokumenten geschwärzt oder auf andere Weise entfernt werden. Ein häufiger Fehler dabei: Der schwarze Balken wird lediglich als zusätzliche Grafik über den Text gelegt und das Dokument dann als PDF gespeichert – sodass die Balken später mit einem Editor wieder entfernt werden können.

Auf unserer Website[4] finden Kommunen außerdem eine umfangreiche Sammlung von Antworten auf häufig gestellte Fragen und weiteres hilfreiches Infomaterial.

Fazit

Durch unsere Beratungs- und Schulungsangebote unterstützen wir Verantwortliche öffentlicher und privater Stellen bei ihren datenschutzrechtlichen Pflichten. Aufgrund der erhaltenen Rückmeldungen trägt der enge Austausch mit Kommunen, Unternehmen und Vereinen dazu bei, praktikable Lösungen zu entwickeln, proaktiv zu sensibilisieren statt reaktiv zu ahnden und dadurch den Schutz personenbezogener Daten in Niedersachsen nachhaltig zu stärken.

4 https://lfd.niedersachsen.de/kommunen

G Aktuelle Themen

Videoüberwachung

G.1.1 Touristische Webcams: Livestream von FKK bis Marktplatz

Touristische Webcams sind inzwischen weit verbreitet. In vielen Fällen erfassen die Betreiber durch die Webcams jedoch mehr, als zulässig ist. Mitunter werden Marktplätze und sogar FKK-Strände einschließlich der Besucherinnen und Besucher hochauflösend in das Internet gestreamt.

Im Jahr 2024 erreichten uns vermehrt Beschwerden und Hinweise zu möglichen Datenschutzverstößen, die touristische Webcams in ganz Niedersachsen betrafen. Im Rahmen einer Stichprobe haben wir zudem festgestellt, dass bei einer Vielzahl solcher Webcams die Verantwortlichen nicht genug auf den Datenschutz geachtet haben.

Touristische Webcams werden sowohl durch nicht-öffentliche Stellen wie private Vermieter von Ferienwohnungen oder Hotelbetreibern als auch von öffentlichen Stellen wie Kommunen betrieben. Dabei sind stets die datenschutzrechtlichen Vorschriften[1] zu beachten.

Für Betroffene besteht durch den Einsatz von Webcams ein besonderes Risiko für deren Persönlichkeitsrechte. Dies gilt vor allem dann, wenn die Aufnahmen oder Bilder der Webcam aus öffentlich zugänglichen Bereichen in Echtzeit und frei zugänglich im Web übertragen werden. Dritte können die digitalen Aufnahmen dann weltweit abrufen, kopieren und unbegrenzt speichern.

Der Einsatz einer Übersichtskamera und insbesondere einer Webcam – gegebenenfalls auch mit einer dauerhaft laufenden Bildübertragung – ist nur

1 Für den nicht-öffentlichen Bereich ist dies Art. 6 Abs. 1 Buchst. f DSGVO und für den öffentlichen Bereich § 14 Abs. 1 S. 1 NDSG.

zulässig, wenn die Aufnahmen keinen Bezug zu bestimmten Personen ermöglichen. Personen dürfen grundsätzlich nicht so abgebildet werden, dass sie identifizierbar sind. Das bedeutet, dass Personen, aber auch Kraftfahrzeuge nur schemenhaft erkennbar und (Wohn-)Gebäude oder Geschäfte nicht erfasst sein dürfen. Dies kann beispielsweise mit einer entsprechenden Kamerapositionierung, fehlender Zoom-Möglichkeit oder einer Verpixelung von Teilbereichen erreicht werden.[2]

Die Aufnahmen einer Übersichtskamera dürfen keinen Bezug zu bestimmten Personen ermöglichen.

Livestream eines FKK-Strandes

In einem Fall wurden wir auf einen frei im Internet zugänglichen Livestream aufmerksam gemacht. Der Verantwortliche erfasste einen Strandabschnitt durch eine schwenkbare Webcam. Diese verfügte zudem über eine Zoom-Funktion. Die Webcam sollte touristischen Zwecken dienen. Zudem konnte die Tide über die Webcam verfolgt werden. Allerdings waren auch Personen erkennbar.

Besonders gravierend war an dieser Webcam, dass der erfasste Strandabschnitt ein FKK-Strand war. Hierdurch waren Personen in ihrem Intimbereich betroffen. Zudem wurden die betroffenen Personen nicht auf die Videoüberwachung hingewiesen. Die im FKK-Strandabschnitt befindlichen Personen wurden also ohne deren Wissen für jedermann frei zugänglich im Web veröffentlicht.

Der Verantwortliche zeigte sich kooperativ und verpixelte im Zuge des Verwaltungsverfahrens den betreffenden Strandabschnitt. Das Verwaltungsverfahren konnte daraufhin beendet werden. Wegen der hohen Eingriffsintensität schloss sich ein Bußgeldverfahren an.

Videoüberwachung von Strand und Pool

In einem anderen Fall wurden wir selbst auf zwei Webcams aufmerksam. Hintergrund waren eigene Recherchen, nachdem eine Beschwerde über

2 Siehe DSK, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", Link: https://www.lfd.niedersachsen.de/download/158457/ (PDF)

eine Videoüberwachung in einem Sauna- und Spa-Bereich eingereicht wurde.

Neben der Videoüberwachung im Sauna- und Spa-Bereich stellten wir fest, dass auf der Webseite des Unternehmens auch die Aufnahmen von zwei Webcams eingebunden waren. Eine der Webcams zeigte den vorgelagerten Strandabschnitt, die andere Webcam den innenliegenden Poolbereich.

Der Verantwortliche war im laufenden Verwaltungsverfahren zunächst nicht gewillt, seine Videoüberwachung datenschutzkonform auszugestalten oder einzustellen – weder bezogen auf die Videoüberwachung im Sauna- und Spa-Bereich noch auf die Einstellungen der Webcams. Erst als wir den Verantwortlichen förmlich angewiesen hatten[3], eine datenschutzkonforme Einstellung der Videoüberwachungskameras vorzunehmen, beendete der Verantwortliche die rechtswidrigen Datenverarbeitungen. Die Videoüberwachung im Sauna- und Spa-Bereich sowie die Webcam im Poolbereich deaktivierte der Verantwortliche. Zudem schwenkte er die auf den Strandabschnitt gerichtete Kamera, sodass die Strandpromenade selbst nicht mehr erfasst war.

Sensibilisierung statt Verbote

Ausgehend von den geschilderten Einzelfällen und der im Jahr 2024 erhöhten Anzahl von Beschwerden und Hinweisen zu touristischen Webcams haben wir ein Hinweisschreiben[4] verfasst, um die Öffentlichkeit zu sensibilisieren und aufzuklären. Dieses Schreiben lassen wir der jeweils örtlich zuständigen Gemeinde zukommen, um über die rechtlichen Rahmenbedingungen zum datenschutzkonformen Einsatz von Webcams aufzuklären. Wir hoffen, dass uns die Gemeinden dabei unterstützen und als Institutionen vor Ort unsere Hinweise den Betreiberinnen und Betreibern von Webcams in geeigneter Weise bekanntmachen.

3 Art. 58 Abs. 2 Buchst. d DSGVO.
4 Art. 57 Abs. 1 Buchst. b DSGVO.

Fazit

Der Einsatz touristischer Webcams steht in einem Spannungsverhältnis zum Datenschutz. Um die Verantwortlichen zu sensibilisieren und einen datenschutzkonformen Einsatz von touristischen Webcams zu ermöglichen, weisen wir die Verantwortlichen unter Einbeziehung der Kommunen vor Ort auf die Rechtslage hin, werden aber auch weiterhin bei uns eingehenden Beschwerden nachgehen und nicht datenschutzkonforme Konstellationen beseitigen lassen.

G.1.2 Prüfungen von Fitnessstudios: Vor-Ort-Kontrollen und Bußgelder

Bei einer Prüfung von Fitnessstudios stellten wir 2023 einige – zum Teil schwerwiegende – datenschutzrechtliche Verstöße fest. Im Jahr 2024 setzten wir die Prüfung fort, leiteten in drei Fällen Bußgeldverfahren ein und untersuchten zwei weitere Studios vor Ort.

Bereits im Jahr 2023 hatten wir aufgrund vieler Beschwerden im Bereich von Fitnessstudios begonnen, zehn stichprobenartig ausgewählte Fitnessstudio-Unternehmen mit insgesamt 17 Filialen in Niedersachsen zu überprüfen.[1] Vorrangig untersuchten wir die Rechtmäßigkeit der eigentlichen Videoüberwachung. Ergänzend kontrollierten wir die Einhaltung der Informationspflichten und weiterer formaler Verpflichtungen. Diese Untersuchungen konnten wir 2024 abschließen.

Von den zehn ausgewählten Unternehmen betrieben sechs Fitnessstudios in neun Filialen eine Überwachung mittels Videokameras. Da die Verstöße zum Teil nur gering waren, stellten wir drei Verfahren ein und wiesen die Unternehmen lediglich auf die Voraussetzungen einer datenschutzkonformen Videoüberwachung hin. In drei Unternehmen stellten wir schwerwiegende Datenschutzverstöße fest.[2] In diesen Fällen schloss sich ein Bußgeldverfahren an.[3]

Verstöße gegen die Rechtmäßigkeit der Datenverarbeitung

Drei Unternehmen überwachten unzulässigerweise die Trainingsflächen, die Sitzbereiche der Kundinnen und Kunden sowie Beschäftigtenbereiche. Zwei dieser Unternehmen filmten darüber hinaus datenschutzwidrig Bereiche außerhalb des eigenen Grundstücks.

Bei der durchgehenden Videoüberwachung im Fitnessstudio während der gesamten Öffnungszeiten auf allen Trainingsflächen handelt es sich um einen gravierenden Eingriff in die Grundrechte aller Trainierenden. Diese

1 Siehe Tätigkeitsbericht 2023, G.1.1.
2 Entsprechend Art. 58 Abs. 2 DSGVO.
3 Siehe Kapitel H zu abgeschlossenen Bußgeldverfahren.

sind in ihrem Grundrecht auf informationelle Selbstbestimmung[4] in ganz erheblicher Weise berührt. Insbesondere besteht für die Betroffenen keine räumliche oder zeitliche Ausweichmöglichkeit im Rahmen der Inanspruchnahme der vertraglichen Leistungen.

Die Beschäftigten haben zudem grundsätzlich einen Anspruch darauf, bei Ausübung ihrer beruflichen Tätigkeit keiner ständigen Arbeits- und Leistungskontrolle seitens des Arbeitgebers zu unterliegen.

Verstöße gegen Informationspflichten und formale Vorschriften

Fünf Unternehmen erfüllten die Informationspflichten[5] nicht vollständig. Wir konnten allerdings positiv feststellen, dass alle Unternehmen, die eine Videoüberwachung betrieben, zumindest auch auf den Umstand der Videoüberwachung hinwiesen.

Zudem verstießen die Unternehmen zum Teil gegen weitere formale Vorschriften wie die Pflicht zum Führen eines Verzeichnisses von Verarbeitungstätigkeiten[6] und der Meldung des betrieblichen Datenschutzbeauftragten bei der Aufsichtsbehörde.[7]

Vor-Ort-Kontrollen bei Fitnessstudios

Im Jahr 2024 prüften wir außerhalb der anlasslosen Prüfung zudem zwei weitere Fitnessstudios vor Ort. In einem Fall standen wir einem Unternehmen beratend zur Seite. Wir erläuterten dem Verantwortlichen die Voraussetzungen einer datenschutzkonformen Videoüberwachung anhand der Gegebenheiten vor Ort. Dabei wiesen wir auf rechtliche Grenzen hin, zeigten aber auch auf, was datenschutzrechtlich zulässig wäre.

In einem anderen Fall suchten wir das Fitnessstudio aufgrund einer konkreten Beschwerde auf. Einen datenschutzwidrigen Zustand hinsichtlich der Erfassungsbereiche der Kamera konnten wir jedoch nicht feststellen.

4 Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 GG.
5 Art. 12 in Verbindung mit Art. 13 DSGVO.
6 Art. 30 DSGVO.
7 Art. 37 Abs. 7 DSGVO.

Bei den Unternehmen, die wir bereits im schriftlichen Verfahren kontrolliert hatten, verzichteten wir auf Vor-Ort-Prüfungen. Die Unternehmen hatten die festgestellten datenschutzrechtlichen Verstöße bereits im Rahmen des schriftlichen Verwaltungsverfahren abgestellt.

Fazit

Videoüberwachungsanlagen in Fitnessstudios werden nur selten datenschutzkonform betrieben.

Immer mehr Unternehmen installieren in den von ihnen betriebenen Fitnessstudios Videoüberwachungsanlagen. Diese werden jedoch nur selten datenschutzkonform betrieben. Häufig werden insbesondere Trainingsflächen, Beschäftigten- und Sitzbereiche großflächig und dauerhaft überwacht. Bei konkreten Hinweisen oder Beschwerden werden wir auch weiterhin Prüfverfahren durchführen und die Einhaltung der datenschutzrechtlichen Vorschriften durchsetzen.

Privater Einsatz von Drohnen datenschutzrechtlich häufig problematisch G.1.3

Der Einsatz von Drohnen stellt vielfache Anforderungen an den Betreiber, auch in rechtlicher Hinsicht. Schließlich ist neben anderen Rechtsgebieten gleichsam das Datenschutzrecht zu beachten.

Der freizeitmäßige Einsatz von Drohnen mit Videokameras durch Privatpersonen begegnet jedenfalls innerhalb von Ortslagen mit Wohnbebauung neben luftverkehrs- und zivilrechtlichen auch datenschutzrechtlichen Bedenken. Anwohner, die eine Drohne in ihrer Nähe bemerken, empfinden dies häufig als ein überraschendes Eindringen in ihre Privatsphäre, weil sie auf diese Weise von Unbekannten in ihrer jeweiligen Situation wahrgenommen werden können. Dementsprechend erreichen uns Beschwerden über den Einsatz von Drohnen.

Schon Aufnahmen von Häusern mittels Drohne sind datenschutzrechtlich heikel (Symbolbild).

Selbst wenn der Betreiber mit seiner Drohne tatsächlich keine Videos aufnimmt, rechnen viele Betroffene damit und befürchten, dass Aufnahmen von ihnen und Informationen über sie den ausschließlich persönlichen oder

familiären Rahmen verlassen und anderweitig beispielsweise gewerblich verwertet oder sogar in sozialen Medien verbreitet werden könnten.

Rechtsgrundlage erforderlich

Das Übertragen und Aufzeichnen von Bildern einer Drohnenkamera bedarf als Datenverarbeitung einer Rechtsgrundlage aus der Datenschutz-Grundverordnung. In Betracht kommen außer der Einholung einer Einwilligung nur der Erlaubnistatbestand der Wahrnehmung überwiegender berechtigter Interessen an der Nutzung des Fluggeräts.[1]

Das setzt beim Einsatz der Drohne über bewohntem Gebiet aber zwingend voraus, dass der Betreiber oder die Betreiberin belegen kann, sorgfältig und nachvollziehbar abgewogen zu haben, ob die Interessen der Betroffenen an dem Schutz ihrer Privatsphäre nicht höher zu bewerten sind als das Nutzungsinteresse an der Drohne und ob eine etwaige Datenverarbeitung auch wirklich erforderlich ist.

Ein überwiegendes berechtigtes Interesse ist beispielsweise zu bejahen beim Einsatz einer Drohne durch einen Dachdecker, um die Schäden an einem Dach näher zu verifizieren, auch wenn dabei Teile des Nachbargrundstücks gefilmt werden.

Informationspflicht erfüllen

Ferner muss der jeweils Verantwortliche sich überlegen, wie er den Informationspflichten[2] gegenüber den betroffenen, also den gefilmten Personen über seine Identität und die tatsächlichen Gegebenheiten genügen kann.

An diesen Voraussetzungen fehlt es nach unseren Beobachtungen regelmäßig. Deshalb geht man sehr häufig beim Einsatz von Drohnen mit Videokameras das Risiko ein, gegen Datenschutzbestimmungen zu verstoßen.

Weitere Informationen zu diesem Thema sind in dem von der Datenschutzkonferenz 2019 veröffentlichten „Positionspapier zur Nutzung von Kame-

1 Vgl. Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO.
2 Vgl. Art. 12 und 13 DSGVO.

radrohnen durch nicht-öffentliche Stellen“[3] festgehalten, das nach wie vor Gültigkeit hat.

Fazit

Das Filmen mittels einer Drohne ist (auch) datenschutzrechtlich heikel und bedarf im Vorfeld einer gründlichen datenschutzrechtlichen Analyse, wenn beispielsweise dritte Personen, aber auch Häuser Dritter aufgenommen werden.

3 Kurzlink: https://t1p.de/dsk-drohnen (PDF).

G.1.4 Rechtsgrundlagen für den Drohneneinsatz geschaffen: Dennoch weiterer Regelungsbedarf

Im Niedersächsischen Brand- und Katastrophenschutzgesetz wurden die Rechtsgrundlagen für den Einsatz von unbemannten Luftfahrtsystemen (Drohnen) geschaffen. Auch in anderen Bereichen besteht Regelungsbedarf.

Immer häufiger werden durch öffentliche Akteure in unterschiedlichen Einsatzszenarien unbemannte Luftfahrtsysteme verwendet. Diese kommen in der Regel als Videoflugdrohnen zum Einsatz. Aus datenschutzrechtlicher Sicht weist der Einsatz derartiger Drohnen eine erhöhte Eingriffsintensität auf. Aufgrund der Art des Einsatzes als fliegendes Objekt kann ein Gefühl stetiger potenzieller Überwachung entstehen. Zudem handelt es sich angesichts der möglichen Reichweite des Einsatzes und der Beweglichkeit der Drohne um einen Eingriff mit erheblicher Streubreite – die Einsatzumgebung kann miterfasst werden.

Drohnen beim Brand- und Katastrophenschutz

Der Gesetzgebungsprozess zum Niedersächsischen Brandschutzgesetz (NBrandSchG) und zum Niedersächsischen Katastrophenschutzgesetz (NKatSG) wurde ursprünglich von der CDU-Fraktion mit einem Gesetzentwurf im Oktober 2023 initiiert und seitens der Landesregierung mit einem Vorschlag des Ministeriums für Inneres und Sport aus Juni 2024 aufgegriffen. Im Rahmen der Beteiligung unseres Hauses begrüßten wir die geplanten Rechtsgrundlagen für den Einsatz von Drohnen bereits in einer schriftlichen Stellungnahme. Zudem hoben wir das Vorhaben innerhalb der mündlichen Anhörung im Ausschuss für Inneres und Sport des Niedersächsischen Landtags am 19. September 2024 ausdrücklich als insgesamt positiv hervor.

Hinsichtlich des NBrandSchG sahen wir Optimierungsbedarf etwa hinsichtlich des Katalogs von Einsatzszenarien. Dieser erschien uns zu offen formuliert. Wir empfahlen eine abschließende Bestimmung für feste, eindeu-

tige Zwecke. Weiter haben wir darauf gedrungen, die Gefahrenbegriffe im Einklang zu den Gefahrenbegriffen im Niedersächsischen Polizei- und Ordnungsbehördengesetz (NPOG) zu verwenden.[1] Dies betraf vor allem die besonders eingriffsintensive Datenerhebung aus Wohnungen. Einheitliche Begrifflichkeiten würden hier Sicherheit bei der späteren Anwendung des NBrandSchG verschaffen.

Beim Einsatz als fliegendes Objekt kann ein Gefühl stetiger potenzieller Überwachung entstehen.

Zusätzlich bedurfte es aus unserer Sicht einer Nachbesserung beim Umgang mit den Informationspflichten und einer verbindlicheren Regelung zur Kenntlichmachung der Flugsysteme. Dabei war die vorgesehene Aufnahme einer Pflicht zur Kenntlichmachung von Drohnen für sich genommen positiv zu bewerten. Es sollte jedoch durch die dabei verwendeten Formulierungen sichergestellt sein, dass diese Vorgabe in der Praxis nicht wieder aufgeweicht wird.

Die Regelung im NKatSG ist nahezu wortgleich zu derjenigen im NBrandSchG. Sie bezieht sich allerdings – statt auf Einsätze zur Brandbekämpfung und Hilfeleistung wie im NBrandSchG – auf die Bekämpfung einer Katastrophe oder eines außergewöhnlichen Ereignisses.

Rechtsgrundlagen auch für Verfassungsschutz und Polizei

Aktuell sieht auch der Entwurf des Niedersächsischen Verfassungsschutzgesetzes (NVerfSchG) vor, zukünftig den Einsatz von Drohnen zuzulassen. Das bisherige ausdrückliche Verbot[2] soll aufgehoben werden.[3] Eine spezifische Rechtsgrundlage für den Drohneneinsatz ist im Gesetzentwurf bislang jedoch nicht vorgesehen. Daher haben wir – unter Verweis auf das NBrandSchG und NKatSG – im Oktober 2024 ebenfalls eine solche Rechtsgrundlage für das NVerfSchG in unserer Stellungnahme gegenüber dem Niedersächsischen Ministerium für Inneres und Sport gefordert. Das Kabinett hat den Gesetzentwurf – ohne eine entsprechende Regelung – im November 2024 angenommen.[4]

1 Siehe § 2 NPOG.
2 Siehe § 14 Absatz 1 Satz 4 NVerfSchG.
3 Niedersächsischer Landtag, Drucksache 19/5930, Art. 1 Nr. 4 b).
4 https://www.stk.niedersachsen.de/237506.html

Bei der Polizei sind Drohnen teilweise schon im Einsatz.[5] Auch hier mangelt es jedoch aus unserer Sicht an einer Rechtsgrundlage im NPOG. Die durch den Drohneneinsatz erhöhte Eingriffsintensität bedarf auch hier einer speziellen Rechtsgrundlage.

Ausblick

Die Rechtsgrundlagen im NBrandSchG und NKatSG für den Drohneneinsatz sind am 12. November 2024 in Kraft getreten.[6] Die obigen Empfehlungen unseres Hauses wurden darin leider nicht mehr umgesetzt. Nichtsdestotrotz werden von unserer Seite die aus datenschutzrechtlicher Sicht bestehenden Änderungsbedarfe weiterhin benannt und eingefordert.

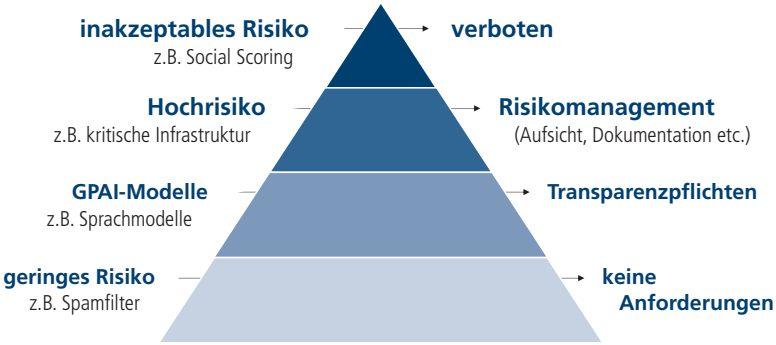
Zugleich erhalten wir im Hinblick auf das NVerfSchG im weiteren Gesetzgebungsprozess die Forderung einer spezifischen Rechtsgrundlage für den Drohneneinsatz aufrecht. Ebenso verhält es sich mit dem NPOG. Auch hier dringen wir auf den Gesetzgeber, zeitnah eine entsprechende Rechtsgrundlage zu schaffen.

5 https://www.mi.niedersachsen.de/227558.html
6 Siehe § 35d NBrandSchG und § 32b NKatSG.

Künstliche Intelligenz

Künstliche Intelligenz im Zusammenspiel mit dem Datenschutz G.2.1

Am 1. August 2024 trat die europäische KI-Verordnung in Kraft. Der deutsche Gesetzgeber ist nun aufgefordert ein nationales Umsetzungsgesetz zu erlassen. Datenschutzaufsichtsbehörden, Unternehmen und öffentliche Stellen müssen sich nun mit dem Zusammenspiel von KI-Verordnung und Datenschutz-Grundverordnung auseinandersetzen. Bestehende und künftige KI-Modelle und -Systeme werden datenschutzrechtlich bewertet.



Risikostufen von KI-Systemen nach der KI-Verordnung

Die europäische KI-Verordnung (KI-VO) gibt den Rechtsrahmen für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen Künstlicher Intelligenz (KI-Systeme) in der Europäischen Uni-

on vor.[1] Der europäische Gesetzgeber hat sich für eine risikoorientierte, zeitlich abgestufte Geltung der Vorschriften entschieden. Bereits ab dem 1. Februar 2025 gelten die Kapitel I und II der KI-Verordnung und damit die Verbote bestimmter Praktiken der Künstlichen Intelligenz. Die weiteren Vorschriften werden nach und nach jeweils ab dem 2. August 2025, 2026 und 2027 Geltung erlangen.

Die KI-Verordnung ist im Kern regulierendes Technikrecht, das Aspekte der Marktüberwachung, der Produktsicherung, der Haftung, aber auch des Datenschutzes umfasst. Sie gibt eine recht komplexe KI-Governance-Struktur vor: In Europa wird es mit dem KI-Ausschuss und dem KI-Büro neue, zuständige Organe geben. Die EU-Mitgliedstaaten müssen insbesondere eine notifizierende Behörde und eine oder mehrere Marktüberwachungsbehörden benennen. Der deutsche Gesetzgeber hat 2024 trotz des bestehenden Zeitdrucks zwar keinen Entwurf für ein nationales Umsetzungsgesetz zur KI-Verordnung vorgelegt. Es wurden allerdings Überlegungen zum Rahmen für einen Entwurf und ein Regelungskonzept veröffentlicht. Aus Letzterem geht insbesondere hervor, dass der Gesetzgeber den Datenschutzaufsichtsbehörden keine Zuständigkeiten im Rahmen der KI-Verordnung zuweisen will.

Die KI-Verordnung enthält zwar selbst nur sehr wenige Datenschutzvorschriften[2], allerdings stellt Artikel 2 Absatz 7 der KI-VO klar, dass die Datenschutz-Grundverordnung unberührt bleibt. Da davon auszugehen ist, dass viele KI-Systeme personenbezogene Daten verarbeiten werden – häufig wohl sogar in sehr großem Umfang –, sind die Datenschutzaufsichtsbehörden für diesen Bereich zuständig. Es besteht daher ein Abstimmungsbedarf zwischen den zukünftig in Deutschland für die Marktüberwachung zuständigen Stellen mit den Datenschutzaufsichtsbehörden.

Alle Adressaten der KI-Verordnung haben nach unserem Eindruck das Jahr 2024 intensiv genutzt, sich mit den Regelungen und Konsequenzen des neuen Rechtsrahmens vertraut zu machen. Vor diesem Hintergrund erreichten die niedersächsische Datenschutzaufsicht zunehmend Beratungsanfragen – meist bezogen auf die Inbetriebnahme von KI-Systemen in Behörden, Unternehmen und sonstigen Organisationen. Es ist im Berichtsjahr

1 Weitere allgemeine Informationen zur KI-Verordnung sind hier abrufbar: https://www.lfd.niedersachsen.de/ki

2 Insbesondere Art. 10 DSGVO Daten und Daten-Governance bei Hochrisiko-KI-Systemen.

auch eine erste Beschwerde gegen den Einsatz eines KI-Systems bei uns eingegangen.

In Anbetracht der rasanten Entwicklung und Verbreitung von KI-Systemen hat die niedersächsische Datenschutzaufsicht im September 2024 eine Stabsstelle Künstliche Intelligenz eingerichtet.[3] Ziel der neuen Organisationseinheit ist es, die zunehmende Verbreitung und Nutzung von KI-Technologien datenschutzrechtlich zu begleiten. Die Stabsstelle fungiert als Kompetenzzentrum für alle Fragen rund um den Einsatz von KI und arbeitet eng mit anderen Behörden, der Wissenschaft sowie privaten und öffentlichen Stellen zusammen. Im Berichtsjahr ist hier beispielsweise die Durchführung der KI-Expertengespräche beim LfD Niedersachsen zu nennen.[4]

Fazit

Wir haben 2024 mit der Einrichtung der Stabsstelle KI beim LfD Niedersachsen die Voraussetzungen geschaffen, um für das umfassende und voraussichtlich auch die nächsten Jahre sehr präsente Thema Künstliche Intelligenz gut aufgestellt zu sein. Ziel ist es, eigenes Know-how aufzubauen, an datenschutzkonformen Entwicklungspfaden von KI-Systemen mitzuwirken und dem Datenschutz auch in Bezug auf die hochdynamischen technischen Entwicklungen im KI-Umfeld zur Geltung zu verhelfen und so Innovationen in diesem Bereich konstruktiv zu begleiten.

3 Siehe https://www.lfd.niedersachsen.de/236012.html.

4 Siehe hierzu Kapitel E.

G.2.2 Datenschutzbehörde Niedersachsen beteiligt sich an KI-Reallabor in Osnabrück

Unsere Behörde begleitet als Projektpartner das im Jahr 2024 gestartete Forschungsprojekt CRAI. Im Rahmen des Projekts entsteht in Niedersachsen ein Reallabor, in dem praxisnahe Lösungen für den Einsatz vertrauenswürdiger, auf Künstlicher Intelligenz basierter Geschäftsmodelle in mittelständischen Unternehmen entwickelt werden.

Das Forschungsprojekt CRAI (kurz für „Center of Research and Development of Trustworthy AI Applications for Midsized Companies") ist in Osnabrück angesiedelt und soll den Mittelstand mit einem Reallabor bei der Umsetzung von Projekten rund um Künstliche Intelligenz (KI) unterstützen.

Das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) ist maßgeblich beteiligt.

Ein Reallabor ist ein Testraum, in dem die Teilnehmerinnen und Teilnehmer innovative Technologien oder Geschäftsmodelle möglichst realitätsnah entwickeln und erproben können. Ein solches Reallabor wird sowohl zeitlich, wie auch sachlich begrenzt eingerichtet. Ein wichtiger Aspekt bei der Entwicklungsarbeit ist dabei die Möglichkeit, rechtliche Spielräume zu nutzen und gegebenenfalls Erkenntnisse für die Weiterentwicklung des Rechtsrahmens zu gewinnen („regulatorisches Lernen").

Das Forschungsprojekt CRAI wird vom Bundesministerium für Digitales und Verkehr und vom Niedersächsischen Ministerium für Wirtschaft, Ver-

kehr, Bauen und Digitalisierung gefördert. Beteiligt sind verschiedene Partner aus Forschung, Wirtschaft und Verwaltung, neben unserer Behörde unter anderem das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI), die Universität Osnabrück sowie das Klinikum Osnabrück.

Die Konferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder hat bereits 2019 in der Hambacher Erklärung zur Künstlichen Intelligenz konstatiert, dass KI eine substanzielle Herausforderung für die Wahrung des Grundrechts auf informationelle Selbstbestimmung darstellt. Die Datenschutzvorschriften sind grundsätzlich technikneutral und gelten daher zwar für neue Techniken, Anwendungsfälle und Geschäftsmodelle, sie bedürfen aber einer KI-bezogenen Konkretisierung. Obwohl KI auf sehr umfassenden Datenverarbeitungsprozessen basiert, fehlt es bisher – sowohl für Reallabore als auch für innovative KI basierte Geschäftsmodelle, die in diesen erprobt werden sollen – an konkreten Anforderungen für deren datenschutzkonforme Ausgestaltung.

Fazit

Die Beteiligung am Projekt CRAI birgt große Chancen für alle Beteiligten. Unsere Datenschutzbehörde erhofft sich Einblicke in die Praxis beim konkreten Entwickeln und Umsetzen von KI-Projekten, bei denen der Datenschutz von Anfang an mitgedacht wird. Damit wird das KI-Reallabor von Anfang an unter Berücksichtigung der rechtlichen Anforderungen ausgestaltet. Dies stellt einen wichtigen Schritt dar, um sicherzustellen, dass die spätere Entwicklung und Anwendung vertrauenswürdiger KI-basierter Geschäftsmodelle rechtskonform umgesetzt und in die Praxis überführt werden können.

Darüber hinaus können aus den Ergebnissen und Erfahrungen der Testphase Vorschläge erarbeitet werden, wie der bestehende Rechtsrahmen anzuwenden ist, beziehungsweise angepasst werden könnte. Dies schließt auch die Möglichkeit mit ein, über neue Regelungen nachzudenken und diese in die rechtspolitische wie gesellschaftliche Diskussion einzubringen.

Digitale Medien

G.3.1 Zuständigkeit klargestellt: Schutz vor überflüssigen Cookies verbessert

Eine Beschwerde, die sich gegen den Einsatz speziell eines Cookies durch die Webseite einer Bank richtete, konnte aus unserer Sicht zufriedenstellend gelöst werden. Hierfür war jedoch zunächst die Zuständigkeit der Datenschutzaufsichten für die Durchsetzung des TDDDG zu klären. Zudem erfreulich: Die in Niedersachsen erreichte Lösung kommt nun auch deutschlandweit zum Einsatz.

Webseiten sind zumeist mit Einwilligungsbannern ausgestattet, in denen sich die Besucher mit dem Einsatz von Cookies einverstanden erklären oder ihre Zustimmung erteilen sollen. Aus rechtlicher Perspektive werden sie also darum gebeten, eine wirksame Einwilligung zu erteilen.

In der Beschwerdepraxis müssen wir leider immer wieder feststellen, dass die eingeholten Einwilligungen der Nutzenden unwirksam sind, weil sie nicht den Anforderungen der Datenschutz-Grundverordnung (DSGVO) genügen. Oftmals versuchen die Betreiber der Webseite, die Nutzerinnen und Nutzer durch manipulierende Gestaltungen der Abfragemaske zur Einwilligung zu bewegen (sogenanntes „Nudging“[1]).

Doch warum ist eine Einwilligung überhaupt erforderlich? Die Regelungen dazu finden sich zum einen in der DSGVO, die dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten dient. Zum anderen stehen sie auch im Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), das im Besonderen den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten regelt und ebenfalls Datenschutzvorschriften enthält.

1 Siehe hierzu auch Tätigkeitsbericht 2023, Kapitel G.6.2.

Sofern Cookies personenbezogene Daten enthalten, sind bei der Verarbeitung dieser Daten die Regelungen der DSGVO zu beachten. Eine Einwilligung ist im Zusammenhang mit personalisierter Werbung notwendig. Tracking-Cookies sind Kernbestandteil solcher Werbung, bei der Nutzerinnen und Nutzer oftmals über verschiedene Webseiten hinweg verfolgt („getrackt") und ein umfangreicher Datenbestand („Profilbildung") aufgebaut wird.

Für den initialen Schritt, also das Speichern des Cookies auf dem Endgerät, greifen die Regelungen des TDDDG. Paragraf 25 dieses Gesetzes soll die Integrität des Endgeräts, also die Privatsphäre der Nutzenden, etwa eines Computers oder eines Smartphones sicherstellen. Eine Webseite darf danach grundsätzlich keine Informationen im Endgerät speichern oder Zugriff auf Informationen nehmen, also insbesondere Cookies setzen oder solche auslesen. Den Nutzenden soll so eine umfassende Kontrolle über ihre Endgeräte zugebilligt werden. Zulässig sind diese Vorgänge nur, wenn zuvor eine Einwilligung erteilt wurde oder eine der eng definierten Ausnahmebestimmung erfüllt ist.

Datenschutzaufsichten sind zuständig

Es ist ein großer Gewinn für die Durchsetzung des TDDDG, dass die Datenschutzaufsichten auch für die Durchsetzung dieser Regeln für zuständig erklärt wurden. Anfang 2024 wurde die Zuständigkeit hierfür, die konkreten Befugnisse sowie die möglichen Sanktionen umfassend im Niedersächsischen Datenschutzgesetz (NDSG) verankert.[2]

Das Beispiel des folgenden Falles zeigt, dass wir dadurch in der Lage sind, die eng verflochtenen Regelungsgegenstände der DSGVO und des TDDDG in Bezug auf Cookies auf Webseiten „aus einer Hand" zu bewerten und Beschwerden wirkungsvoll abhelfen zu können.

In dem angesprochenen Verfahren wendete sich der Beschwerdeführer speziell gegen einen Cookie, der auf der Webseite einer niedersächsischen Sparkasse eingesetzt wurde. Dieser enthielt eine eindeutige Identifikationsnummer (ID), die ein Tracking des Nutzers zu Werbezwecken technisch ermöglicht hätte. Nach den Ausführungen des verantwortlichen Betreibers der Webseite fand jedoch kein Tracking statt, sodass eine Einwilligung nach der DSGVO nicht erforderlich war. Weiter wurde ausgeführt, der

2 § 20a NDSG.

Cookie diene der Sicherheit des Online-Bankings. Standardmäßig müsse ein Login mithilfe einer Freigabe-App bestätigt werden. Nutzende könnten jedoch alternativ die Funktion der Geräteerkennung aktivieren. Der Cookie würde lediglich genutzt, um das Gerät wiederzuerkennen. Daher konnte sich die Verantwortliche auf die erwähnte Ausnahme[3] berufen, die das Speichern von Informationen erlaubt, wenn diese – verkürzt gesagt – „unbedingt erforderlich" ist.

Im IT-Labor des Landesbeauftragten für den Datenschutz Niedersachsen wurden diese Angaben gründlich überprüft. Es wurde festgestellt, dass der Cookie stets für alle Besucher der Webseite gesetzt wurde, nicht nur für Kundinnen und Kunden der Bank, die die Funktion der Geräteerkennung für das Online-Banking aktiviert hatten. Der Cookie war für einen Großteil der Webseitenbesucher daher nicht „unbedingt erforderlich".

Im Rahmen des Prüfverfahrens entschloss sich die Bank den Login-Prozess anzupassen. Die eindeutige ID wird seitdem erst dann gespeichert, wenn der Nutzer die Funktion der Geräteerkennung aktiviert hat. Aus unserer Sicht war das Verfahren ein besonderer Erfolg: Die Anpassungen wurden nicht nur auf der beschwerdegegenständlichen Webseite implementiert, sondern deutschlandweit in die Systeme anderer Sparkassen, die sich überwiegend nicht in unserem Zuständigkeitsbereich befinden. So haben wir eine erhebliche Reichweite dieser datenschutzfreundlichen Lösung erreicht.

Fazit

Bei dem Betrieb von Webseiten ist einerseits die DSGVO und andererseits die datenschutzrechtliche Vorgabe des TDDDG[4] zu beachten. Diese Bestimmung setzt nicht voraus, dass die DSGVO anzuwenden ist. Wichtig ist es, jeden eingebundenen oder bereitgestellten Dienst einzeln zu würdigen, um nicht nur die rechtlichen, sondern auch die technischen Belange berücksichtigen zu können. Ausführliche Informationen hierzu enthält die im November 2024 aktualisierte Orientierungshilfe der Datenschutzkonferenz.[5]

3 Nach § 25 Abs. 2 Nr. 2 TDDDG.

4 § 25 TDDDG.

5 Siehe DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste) Version 1.2, Stand November 2024, Kurzlink: https://t1p.de/vhupm (PDF).

Weg frei für die neuen Einwilligungsverwaltungsdienste G.3.2

In der letzten Sitzung des Jahres hat der Bundesrat der vom Bundestag vorgelegten Verordnung über Dienste zur Einwilligungsverwaltung zugestimmt. Damit sind die rechtlichen Rahmenbedingungen für Einwilligungsverwaltungsdienste in Deutschland festgelegt. Der Einsatz dieser Dienste soll dazu führen, die von vielen Nutzern als störend empfundenen Einwilligungsbanner auf Webseiten deutlich zu reduzieren und zu vereinfachen.

Die Einwilligungsverwaltungsverordnung (EinwV) gemäß § 26 Absatz 2 TTDSG wird voraussichtlich am 1. April 2025 in Kraft treten.[1] Ab diesem Zeitpunkt können sogenannte Dienste zur Einwilligungsverwaltung auf dem Markt angeboten werden. Einsatzgebiet dieser Dienste sind Webseiten und Apps, auf denen die Anbieter Einwilligungen der Nutzer in der Regel über entsprechende Banner insbesondere für den Einsatz von Cookies und andere Tracking-Techniken abgefragt werden. Viele Nutzer empfinden die regelrechte „Bannerflut" im Web als störend und zeitfressend.

Die neue Verordnung sieht anerkannte Dienste zur Einwilligungsverwaltung als anwenderfreundliche Alternative zu den Einwilligungsbannern vor, um diese deutlich zu reduzieren. Dies bedeutet allerdings nicht, dass Nutzer im Dienst zur Einwilligungsverwaltung quasi einmal ihre Einwilligungen erteilen, die dann für eine Vielzahl von Webseiten gelten. Entsprechend der Bezeichnung dient der neue Dienst nicht der Erteilung, sondern nur der Verwaltung von Einwilligungen, die der Nutzer beim Aufruf einer Webseite in einem Einwilligungsbanner erteilt hat. Sobald in dem Dienst in Bezug auf eine konkrete Webseite der Status der Einwilligung – erteilt oder nicht erteilt – gespeichert ist und der Nutzer dieselbe Webseite noch einmal besucht, wird der Status automatisch an den Betreiber der Webseite übermittelt. Der Einwilligungsbanner erscheint dann nicht mehr.

1 Siehe dazu auch Tätigkeitsbericht 2023, I.4, sowie Pressemitteilung des LfD Niedersachsen vom 27. Dezember 2024, https://www.lfd.niedersachsen.de/238383.html

Nutzen der Verordnung zweifelhaft

Wir gehen davon aus, dass die EinwV nicht zu einer wesentlichen Reduzierung der Einwilligungsbanner führen wird.

Zunächst ist zweifelhaft, ob sich Dienste zur Einwilligungsverwaltung überhaupt etablieren werden. Ein anerkannter Dienst zur Einwilligungsverwaltung muss in einem entsprechenden Antrag bei der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit umfassende Anforderungen nachweisen.[2] Insbesondere muss er darlegen, dass er kein wirtschaftliches Eigeninteresse an der Einwilligung der Endnutzer und an den verwalteten Daten hat. Darüber hinaus muss er rechtlich und organisatorisch unabhängig von Unternehmen sein, die ein solches Interesse haben können. Damit dürften etliche potenzielle Dienstleister der Internetbranche und der Branche des digitalen Marketings ausgeschlossen sein. Zudem ist das Einbinden von Diensten der Einwilligungsverwaltung für die Betreiber von Webseiten freiwillig, ohne dass ein Mehrwert offensichtlich ist.

Schließlich werden weiterhin Einwilligungen auf den besuchten Webseiten abgefragt werden. Dies ist zunächst dem beschriebenen Ablauf geschuldet, wonach die Erteilung und Ablehnung von Einwilligungen über die einzelnen Webseiten erfolgt. Die bekannten datenschutzrechtlichen Defizite von Einwilligungsbannern, wie etwa das Nudging oder die fehlende „alles ablehnen" Schaltfläche werden sich demnach voraussichtlich fortsetzen. Zudem bezieht sich die EinwV nur auf einen Teil der auf Webseiten erteilten Einwilligungen. Sie umfasst Einwilligungen gemäß Paragraf 25 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) – nicht aber Einwilligungen gemäß der Datenschutz-Grundverordnung.

Fazit

Die Datenschutzaufsicht Niedersachsen setzt sich bereits seit Jahren aktiv dafür ein, die Flut von Einwilligungsbannern auf Webseiten und in Apps zu reduzieren sowie auf datenschutzkonforme Einwilligungsbanner hinzuwirken.[3] Dazu müssen Webseitenbetreiber ihre Webseiten konsequent daten-

2 Siehe §§ 11 f. EinwilligungsV.

3 Siehe dazu auch Tätigkeitsbericht 2023, G.2.2, Prüfung von Medienwebseiten, sowie Orientierungshilfe zu digitalen Diensten, November 2024, https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf

schutzfreundlicher gestalten, zum Beispiel, indem sie auf Drittdienste und Cookies insbesondere für exzessives und für den Nutzer nicht vorhersehbares, digitales Marketing verzichten. Außerdem würden Einwilligungsbanner bei einer datenschutzkonformen Gestaltung kaum stören. Neben der häufig zu findenden Schaltfläche „Einwilligen" müssen sie eine entsprechende Schaltfläche zum „Ablehnen" jeglicher Einwilligungen aufweisen. Dienste zur Einwilligungsverwaltung können allenfalls einen Mehrwert darstellen, wenn diese Grundvoraussetzungen datenschutzkonformer Webseiten eingehalten werden.

Wirtschaft

G.4.1 Vor-Ort-Kontrollen der Immobilienwirtschaft: Mängel bei der Datenverarbeitung

Vermieter und Immobilienverwalter erfassen routinemäßig eine Vielzahl personenbezogener Daten zur Abwicklung von Vermietungsprozessen. Seit 2022 werfen wir einen genaueren Blick auf Unternehmen der Immobilienbranche und ihre Datenverarbeitung, im Jahr 2024 haben wir einige davon vor Ort geprüft.

Um die Einhaltung der Datenschutz-Grundverordnung (DSGVO) im Umgang mit Mieterdaten in der Immobilienbranche zu überprüfen, haben wir vier Immobilienmakler und Wohnungsunternehmen nach Ankündigung vor Ort besucht. Dabei interessierte uns, ob sie den Datenschutz ausreichend beachten. Denn wir gehen davon aus, dass sich Mieter und insbesondere Mietinteressenten bei möglichen Datenschutzverstößen eher nicht zur Wehr setzen, weil sie bei der aktuell angespannten Lage des Wohnungsmarkts Nachteile für sich befürchten.

Bei der Kontrolle haben wir stichprobenartig datenschutzrechtliche Aspekte bei der Wohnraumvermietung untersucht, bei denen wir mögliche Versäumnisse, Unachtsamkeiten oder Verstöße gegen Datenschutzprinzipien, wie Datensparsamkeit von Unternehmen der Immobilienbranche vermuteten. Die Kontrollen fokussierten sich auf die Verarbeitung personenbezogener Daten von Mietinteressierten. Dabei haben wir sämtliche Phasen des Vermietungsprozesses beleuchtet: von der ersten Kontaktaufnahme und der Vereinbarung eines Besichtigungstermins, über den Abschluss eines Mietvertrags oder der Absage an nicht ausgewählte Interessierte, bis hin zur Verwaltung bestehender Mietverhältnisse.

Im Rahmen der durchgeführten Vor-Ort-Kontrollen haben wir eine Reihe von datenschutzrechtlichen Verstößen aufgedeckt. Bei vielen Verstößen

sagten uns die Verantwortlichen deren sofortige Beseitigung zu. Kein Verstoß war allerdings derart gravierend, dass wir ein Bußgeldverfahren einleiten mussten.

Archivierung von Personalausweiskopien und Gehaltsnachweisen

Drei der überprüften Unternehmen verarbeiteten personenbezogene Daten von Mietinteressierten teilweise in unzulässiger Weise. Konkret wurden Kopien von Ausweisdokumenten oder Gehaltsabrechnungen gefordert beziehungsweise erstellt und gespeichert, obwohl dies im jeweiligen Stadium des Vermittlungsprozesses nicht gerechtfertigt war.

Ausweisdokumente dienen ausschließlich der Identitätsfeststellung. Dies kann bereits durch einfaches Einsehen des Dokuments und eine dokumentierte Bestätigung des Abgleichs erfolgen. Es muss also keine Kopie gefertigt und gespeichert werden. Eine Archivierung ist weder für die Vertragsanbahnung[1] noch im Rahmen einer Interessenabwägung[2] erforderlich. Ebenso fehlt in der Regel eine rechtliche Verpflichtung[3] im Kontext von Vermietungen. Daher ist das Kopieren und Archivieren von Ausweisdokumenten – auch in geschwärzter Form – durch Vermieter, Vermieterinnen oder Hausverwaltungen unzulässig.

Das Gleiche gilt für Gehaltsnachweise. Es genügt, diese vorzulegen und die Übereinstimmung mit den Angaben in der Mieterselbstauskunft zu überprüfen. Für den Nachweis der Fähigkeit, die Wohnungskosten finanziell zu tragen, sind Kopien oder deren Archivierung nicht erforderlich und daher unzulässig.

Unzulässige Fragen, kein Verzeichnis über Verarbeitungstätigkeiten

Drei der geprüften Unternehmen setzten zudem Formulare für die Mieterselbstauskunft ein, die die datenschutzrechtlichen Vorgaben nicht erfüllten. So wurden beispielsweise Kontaktinformationen von aktuellen oder früheren Vermietern oder Vermieterinnen erfragt sowie einzelne Beträge nebst

1 Art. 6 Abs. 1 Buchst. b DSGVO.
2 Art. 6 Abs. 1 Buchst. f DSGVO.
3 Art. 6 Abs. 1 Buchst. c DSGVO.

Zahlungszwecke, die vom Nettoeinkommen abgezogen werden, obwohl diese Informationen für die Entscheidung über den Abschluss eines Mietvertrags nicht notwendig sind.

Zwei der überprüften Unternehmen führten kein Verzeichnis der Verarbeitungstätigkeiten.[4] Jeder Verantwortliche ist jedoch verpflichtet, ein solches Verzeichnis zu führen. Es bildet die Basis jeglicher technisch-organisatorischer Maßnahmen des Verantwortlichen, um den Datenschutz und damit auch die IT-Sicherheit in seinem Unternehmen sicherzustellen.

Ergebnis und Fazit

Die durchgeführten Prüfungen hatten eine beratende und aufklärende Funktion sowie eine sanktionierende Funktion, falls Verstöße festgestellt wurden. In Bezug auf zwei Unternehmen, bei denen datenschutzrechtliche Mängel aufgedeckt wurden, wurde ein feststellender Bescheid erlassen. Bei den anderen beiden Unternehmen haben wir keine groben Beanstandungen hinsichtlich der Datenverarbeitung festgestellt.

Wie schon unsere Prüfung im Vorjahr[5] haben die durchgeführten Kontrollen gezeigt, dass in den geprüften Unternehmen teilweise erhebliche Datenschutzmängel im Umgang mit Mieterdaten bestehen. Besonders die verschiedenen Phasen der Datenverarbeitung im Rahmen des Vermietungsprozesses erfordern eine fortlaufende Überprüfung durch den Verantwortlichen, um zu gewährleisten, dass die Erhebung von Daten zu dem jeweiligen Zeitpunkt und für den jeweiligen Zweck gerechtfertigt ist. Zudem müssen über die Verarbeitungsvorgänge Verzeichnisse geführt werden.

Wir behalten uns weiterhin vor, auch in Zukunft unregelmäßige Prüfungen im Bereich der Immobilienwirtschaft durchzuführen.

4 Art. 30 DSGVO

5 Siehe Tätigkeitsbericht 2023, G.3.2.

Datenschutz beim Abschluss von Leasingverträgen G.4.2

Aufgrund zahlreicher Beschwerden zu Leasingverträgen haben wir uns bei einem Unternehmen dieser Branche das Procedere rund um den Datenschutz näher angeschaut. Erfreulicherweise hatte unsere Behörde dabei nur wenig zu beanstanden.

Nach mehreren bei uns eingegangenen Beschwerden zum Datenschutz beim Leasing haben wir uns 2024 dieser Branche intensiver gewidmet. Gegenstand der Beschwerden waren das Auskunftsrecht[1] sowie der Umfang der Datenverarbeitung im Zuge des Vertragsschlusses. Die beschwerdeführenden Personen hatten vor allem Zweifel, ob das Unternehmen wirklich eine ungeschwärzte Verdienstbescheinigung anfordern darf und ob dieses auf ihre Anfragen zur Verarbeitung personenbezogener Daten ordnungsgemäß Auskunft erteilt hatte.

Aufgrund der Beschwerden haben wir ein Leasingunternehmen aufgesucht, dort Einblick in Datenverarbeitung genommen, uns die Prozesse eingehend erläutern lassen, unsere Feststellungen mitgeteilt und uns über deren Umsetzung intensiv mit dem Unternehmen ausgetauscht.

Verdienstbescheinigung

Wir sind mit dem Unternehmen die einzelnen Punkte der Leasingverträge durchgegangen und haben geprüft, ob die dort angeforderten personenbezogenen Daten wirklich notwendig sind. Vor allem hat uns interessiert, warum die Vorlage einer ungeschwärzten Verdienstbescheinigung notwendig sein sollte. Dabei schilderte uns das Unternehmen verschiedene Fälle, in denen Vertragspartner mittels einer manipulierten Verdienstmitteilung versucht hatten, einen hochwertigen Gegenstand zu leasen, obwohl sie damit wirtschaftlich überfordert gewesen wären. Ein Abschluss in diesen Fällen wäre aus Sicht des Unternehmens nicht nur für sie, sondern auch für ihre Vertragspartner nachteilig gewesen. Wir erhielten zudem Einblick in verschiedene Leasinganträge, bei denen die Verdienstbeschei-

1 Vgl. Art. 15 DSGVO.

nigung manipuliert gewesen ist. Das überzeugte uns, das in diesen Fällen die ungeschwärzte Verdienstmitteilung erforderlich ist.

Das Vorlegen einer solchen Bescheinigung ist insoweit auch ein Beitrag zur Betrugsprävention, um Vermögensschäden zu vermeiden. Aufgrund der verschiedenen Abhängigkeiten zwischen den Angaben auf einer Verdienstbescheinigung sowie für die Überprüfung der Richtigkeit der Angaben kommt vorliegend auch keine teilweise Schwärzung in Betracht. Aus unserer Sicht fordert das Unternehmen in diesem Szenario personenbezogene Daten an, die für den Vertragsschluss und in dessen Folge für die Vertragserfüllung notwendig sind.

Ungeschwärzte Verdienstmitteilungen können erforderlich sein.

Vertragsunterlagen per Mail

Bei der Untersuchung fiel uns auf, dass die Vertragsbedingungen einen Passus zur E-Mail-Kommunikation enthielten. Der Leasingnehmer konnte in die unverschlüsselte Übermittlung einwilligen, wenn eine E-Mail mit Transportverschlüsselung unmöglich war.

Wir sind unter Bezugnahme auf den entsprechenden Beschluss der Datenschutzkonferenz[2] der Auffassung, dass in technisch-organisatorische Maßnahmen nicht eingewilligt werden kann. Hier gibt die Regelung zur Sicherheit der Verarbeitung[3] die Richtung vor, sie bestimmen sich also nach dem Stand der Technik, der Implementierungskosten, Art und Umfang der Verarbeitung sowie weiteren gesetzlichen Voraussetzungen. Deshalb kann auf die von kommerziellen E-Mail-Providern regelmäßig zur Verfügung gestellte Transportverschlüsselung nicht verzichtet werden.

Da das Unternehmen im Zug der Antragsbearbeitung einen TLS-Check der angegebenen E-Mail-Adresse des Kunden durchführt und bei negativem Ergebnis die Unterlagen per Post versendet, besteht auch von dieser Seite kein Erfordernis für die entsprechende Passage in den Vertragsunterlagen. Das Unternehmen verwendet diesen Passus dementsprechend zukünftig nicht mehr.

2 Beschluss der DSK, 24. November 2021, abrufbar unter dem Kurzlink https://t1p.de/dsk-toms (PDF).

3 Vgl. Art. 32 DSGVO.

Auskunftsersuchen und Rollenkonzepte

Aufgrund der entsprechenden Beschwerden prüften wir auch den Umgang des Unternehmens mit Auskunftsersuchen. Dabei versendet das Unternehmen die Antwort grundsätzlich auf demselben Weg, wie die Anfrage an das Unternehmen gerichtet worden ist – in der Regel elektronisch.

Je nach Sensibilität der zu beauskunftenden Daten verschlüsselt das Unternehmen elektronische Antworten und teilt der betroffenen Person über ein anderes Kommunikationsmittel das Passwort mit. Nach unserer Einschätzung ist das implementierte Verfahren datenschutzrechtlich nicht zu beanstanden.

Auch mit dem Rechte- und Rollenkonzept waren wir zufrieden. Dabei muss ein Leasingunternehmen mit komplexen Abläufen und dem Zusammenspiel verschiedener Programme umgehen, die für die Bearbeitung und Verwaltung der Leasinganträge beziehungsweise -verträge zum Einsatz kommen. Die Zuteilung der einzelnen Berechtigungen lässt sich in solchen Systemen nur in einer vielschichtigen Matrix darstellen.

Fazit

Die datenschutzrechtliche Prüfung ist in mehrfacher Hinsicht erfolgreich gewesen. So haben wir einen Einblick in die Prozesse beim Bearbeiten und Verwalten von Leasingverträgen erhalten, was uns bei der Bewertung und Einordnung künftiger Beschwerden hilft. Zugleich konnten wir uns davon überzeugen, dass im konkreten Fall die Datenschutz-Grundverordnung (DSGVO) umgesetzt wird.

Auf der anderen Seite hat das Unternehmen einen Eindruck von der Arbeitsweise unserer Behörde erhalten. Beides dient nach unserer Überzeugung dem gemeinsamen Verständnis vom Datenschutz und fördert die einheitliche Anwendung der DSGVO.

G.4.3 Personalisierte Werbung enthält sensible Gesundheitsdaten

Mehrere Personen beschwerten sich bei uns über personalisiert abgefasste Werbebriefe eines Unternehmens. Darin warb es für Pflegeprodukte und Hilfsmittel für die Versorgung Pflegebedürftiger – und wusste offenbar bestens über die Pflegestufen von Familienmitgliedern Bescheid.

In den Werbeschreiben wies das Unternehmen darauf hin, dass bei einem Familienmitglied eine bestimmte Pflegestufe vorläge. Sofern Bedarf bestünde, würde das Unternehmen auf Bestellung regelmäßig sogenannte Pflegeboxen mit entsprechenden Materialien liefern und warb weiterhin damit, die Kostenerstattungsansprüche gegenüber den dafür eintrittspflichtigen Pflegekassen direkt geltend zu machen.

Nachfragen der Betroffenen, woher die Adressdaten und vor allem die speziellen Kenntnisse über die familiären Verhältnisse und die Pflegebedürftigkeit von Angehörigen stammten, beantwortete das Unternehmen teils gar nicht, teils unvollständig oder nur ausweichend. Auch nach wiederholten Aufforderungen kam das Unternehmen der Pflicht zur umfassenden und vollständigen Auskunftserteilung[1] nicht nach.

Der Fall zeigt, wie sich die DSGVO positiv für die betroffenen Bürger auswirkt.

Unsere Untersuchung ergab, dass das Unternehmen in Kooperation mit verschiedenen Adresshändlern fortlaufend Daten von im In- und Ausland tätigen Gewinnspielveranstaltern bezog, welche die in ihrem Webauftritt einzugebenden Daten für die Teilnahmeanmeldungen auch für Werbezwecke vermarkteten. Unternehmen, die in diesem Zusammenhang als Sponsoren für die Preisgewinne auftraten, erhielten die Adressdaten und konnten auch, wie hier geschehen, zusätzliche Fragestellungen für eigene Zwecke initiieren.

1 Vgl. Art. 15 DSGVO.

Verstoß gegen Rechenschaftspflicht

Das in Niedersachsen ansässige Unternehmen konnte seinerseits keine zweifelsfreien Nachweise über die – von den Betroffenen mit Nachdruck bestrittenen – Einwilligungen in die Datenerhebung und die weitere Nutzung für Werbezwecke beibringen. Es ist damit seiner Rechenschaftspflicht[2] nicht nachgekommen. Die Verarbeitung der personenbezogenen Daten durch das Unternehmen ist folglich rechtswidrig gewesen.

Wir wiesen das Unternehmen deshalb zur umfassenden Erfüllung der Auskunftsersuchen einschließlich Benennung der Datenquellen an, um die Betroffenen über die Datenverarbeitung vollständig zu informieren. Damit werden sie in die Lage versetzt, ihre Rechte auch bei den Adresshändlern geltend zu machen. Für die Zukunft haben wir dem Unternehmen zudem untersagt, sich ohne eindeutige und zweifelsfreie Nachweise über erteilte Einwilligungen Adressdaten und Angaben über gesundheitliche Verhältnisse bei den Betroffenen zu verschaffen und zu Werbezwecken zu nutzen. Zudem hat unsere Behörde ein Bußgeldverfahren eingeleitet.

Fazit

Der Fall zeigt, wie sich die Datenschutz-Grundverordnung (DSGVO) und der darin festgelegte Grundsatz der Rechenschaftspflicht positiv für die betroffenen Bürgerinnen und Bürger auswirkt. Nicht wir mussten dem Unternehmen die Verletzung der Vorschriften nachweisen (wie in einem Verwaltungsverfahren), sondern umgekehrt das Unternehmen die Einhaltung der DSGVO. Auch deshalb ist es für die Unternehmen wichtig, die Rechenschaftspflicht zu erfüllen.

2 Vgl. Art. 5 Abs. 2 DSGVO.

G.4.4 Immense finanzielle Schäden durch manipulierte E-Mails

Wenn Online-Kriminelle in IT-Systeme beziehungsweise Computer eindringen, können sie sensible Daten nicht nur mitlesen und abgreifen, sondern auch manipulieren. In einem uns gemeldeten Fall erbeuteten Angreifer auf diesem Weg 147.000 Euro, indem sie die Kontonummer auf einer elektronischen Rechnung austauschten.

Im vergangenen Jahr meldeten sich bei unserer Behörde diverse Betroffene, bei denen es zu einer Manipulation von elektronisch versandten Rechnungen gekommen war. In diesen Fällen liegt der Verdacht nahe, dass entweder auf Versender- oder auf Empfängerseite das IT-System, insbesondere der E-Mail-Server, gehackt oder anderweitig kompromittiert wurde. Dadurch erhält ein Dritter Zugriff auf die E-Mails und kann sie beliebig verändern beziehungsweise den E-Mail-Account von Mitarbeitern (heimlich) benutzen. So lässt der angreifende Dritte die Parteien in dem Glauben, dass sie direkt miteinander kommunizieren, während er tatsächlich alle ausgetauschten Informationen ausspähen, speichern und manipulieren kann.

Fehlüberweisung in Höhe von 147.000 Euro

Alle uns gemeldeten Angriffe hatten gemein, dass die E-Mail-Kommunikation angegriffen wurde. Nachdem die Angreifenden in die IT-Systeme eingedrungen sind, haben sie die empfangenen beziehungsweise zu versendenden E-Mails manipuliert. In allen Fällen änderten sie die bei Rechnungen enthaltenen Zahlungsinformationen. Ziel war es, den Rechnungsempfänger zu einer Fehlüberweisung auf die Konten der Angreifer zu bringen – offenbar in vielen Fällen mit Erfolg. So überwies zum Beispiel der Kunde eines Unternehmens, das sich an uns wendete, aufgrund einer manipulierten Rechnung die Rechnungssumme in Höhe von 147.000 Euro auf ein Konto der Kriminellen.

Die Angreifer manipulieren jedoch nicht nur Mails an und von externen Personen. Ein weiteres beliebtes Vorgehen ist es, die unternehmensinterne Kommunikation für ihre kriminellen Zwecke zu nutzen. Ein Unterneh-

men meldete uns beispielsweise, dass die Kommunikation zwischen der Geschäftsleitung und der Buchhaltung von der Attacke betroffen war. In Zahlungsanweisungen der Geschäftsleitung waren die Bankdaten der Konten der Angreifenden eingesetzt. In diesen Fällen ist davon auszugehen, dass sich die Angreifer Zugang zum E-Mail-System des Unternehmens verschafft hatten, das Unternehmen also gehackt worden war.

Es sind also mit sehr hoher Wahrscheinlichkeit Dritte in das IT-System eingedrungen und konnten die vorhandenen Sicherheitsmaßnahmen umgehen. In einem nächsten Schritt übernehmen die Kriminellen dann möglicherweise das IT-System des Unternehmens komplett oder verschlüsseln wertvolle Daten. Unternehmen, die derartige Auffälligkeiten bemerken, sollten deshalb sofort ihr IT-System intensiv überprüfen und ihre Kommunikationspartner davon unterrichten, damit diese ihrerseits ihre IT-Systeme untersuchen. Denn häufig ist unklar, ob die Manipulation auf der Absender- oder der Empfängerseite erfolgt.

Die Konsequenzen können verheerend sein, wenn Angreifende unbemerkt agieren.

Angriffe verhindern

Die Prävention eines Angriffs erfolgt im Wesentlichen auf technischer Ebene, erfordert aber auch Wachsamkeit der Unternehmensmitarbeiter. Firewalls und Virenscanner mit sicherheitsadäquater Konfiguration sollten standardmäßig im Einsatz sein, unsichere Verbindungen sind tabu.[1] Auch ein entsprechendes Patchmanagement ist unerlässlich, die verwendete Software sollte also regelmäßig und zeitnah Updates erhalten, um bekannte Schwachstellen in den Produkten zu beheben.

Schließlich können Nutzerkonten durch den Einsatz von Mehrfaktorauthentifizierung vor Angriffen besser geschützt werden. Beschäftigte sollten regelmäßig in Schulungen zu Phishing-Mails und anderen Angriffsstrategien sensibilisiert werden.

Die an uns herangetragenen Fälle verdeutlichen außerdem, dass man die Daten neuer Zahlungsempfänger vor der ersten Überweisung stets verifizieren sollte – zum Beispiel durch einen Anruf.

1 Allgemeine IT-Sicherheitstipps des BSI verfügbar unter https://t1p.de/bsi-basistipps (Kurzlink), für kleine Unternehmen unter https://t1p.de/bsi-kmutipps (Kurzlink).

Fazit

Zielgerichtete Angriffe auf die E-Mail-Korrespondenz sind eine ernsthafte Bedrohung für Verantwortliche, sowohl auf der Absender- als auch auf der Empfängerseite von E-Mails. Die Konsequenzen können verheerend sein, wenn Angreifende in der Lage sind, unbemerkt zu agieren. Schwerwiegende Datenlecks und finanzielle Schäden für die Kommunikationspartner sind mögliche Folgen.

Die besten Schutzmaßnahmen dagegen sind die aufgezeigten technischen und organisatorischen Maßnahmen, schnelles Handeln in Verdachtsfällen sowie wachsame, regelmäßig geschulte Mitarbeiter.

Proaktive Schwachstellenanalyse durch das IT-Labor der Datenschutzaufsicht Niedersachsen G.4.5

Erfolgreiche Hackerangriffe auf Unternehmen verursachen hohe wirtschaftliche Schäden und führen dazu, dass personenbezogene Daten in die falschen Hände geraten. Wer Sicherheitsupdates nicht zeitnah installiert, macht es den Angreifern besonders einfach. Wir haben daher 40 Unternehmen identifiziert, die nicht aktualisierte Microsoft Exchange Server betreiben und haben diese zum Schließen der Sicherheitslücken aufgefordert.

Zu den grundlegenden Maßnahmen der IT-Sicherheit gehört ein Patch- und Änderungsmanagement.[1] Softwareanbieter reagieren fortlaufend auf bekanntgewordene Sicherheitslücken und stellen Softwareupdates bereit, die die Lücken schließen.

Wenn Unternehmen diese Softwareupdates nicht oder erst nach geraumer Zeit installieren, fällt es Angreifern nicht schwer, die Kontrolle über einen nicht gepatchten Server zu übernehmen, dort Schadsoftware zu platzieren und anschließend höchstwahrscheinlich weitere Teile des Unternehmensnetzwerkes zu übernehmen. Solche Angriffe erfolgen zunehmend automatisiert und betreffen daher immer mehr Unternehmen, und zwar unabhängig von ihrer Größe. Selbst nach Schließung der Sicherheitslücke ist es möglich, dass auf den Systemen bereits Schadsoftware versteckt wurde, die einen späteren Angriff ermöglicht – sogenannte Backdoor-Programme.

Ein Patchmanagement ist essenzieller Bestandteil eines jeden IT-Sicherheitskonzepts.

Außer den möglicherweise existenzbedrohenden Folgen für das betroffene Unternehmen sind natürlich auch die personenbezogenen Daten von Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeitern erheblich gefährdet. Angreifer begnügen sich nicht mehr damit, Daten zu verschlüs-

1 Das Bundesamt für Sicherheit in der Informationstechnik stellt auf seiner Webseite einen entsprechenden IT-Grundschutz-Baustein bereit, siehe Kurzlink: https://t1p.de/bsi-patch (PDF).

seln, um Ihre Forderungen durchzusetzen. Sie erhöhen den Druck, indem sie Daten extrahieren und mit deren Veröffentlichung drohen.

Identifizierung von niedersächsischen Unternehmen

In zwei gemeinsamen Projekten haben unser zuständiges juristisches Fachreferat und das IT-Labor unserer Behörde 40 Unternehmen in Niedersachsen identifiziert, bei denen eine kritische Sicherheitslücke in der Software Microsoft Exchange Server vorhanden war. Auf diesen Systemen werden in der Regel personenbezogene Daten verarbeitet, sodass entsprechende Sicherheitslücken die Vertraulichkeit, Verfügbarkeit und Integrität dieser Daten gefährden. Zudem wäre es je nach Einbindung in das Unternehmensnetzwerk und Absicherung des betroffenen Servers jederzeit möglich, dass sich die Angreifer wie oben skizziert weiter im Unternehmensnetzwerk ausbreiten.

Das IT-Labor hat mit der Hilfe von Internet-Wide-Scanning-Datenbanken nach Servern niedersächsischer Unternehmen mit veraltetem Softwarestand gesucht und die Treffer anschließend selbst verifiziert.

Aufforderung zur Schließung der Sicherheitslücken

Nachdem die Unternehmen identifiziert waren, haben wir Prüfverfahren eröffnet und die Unternehmen aufgefordert, die Sicherheitslücken zu schließen. Wir kündigten zudem an, von unseren aufsichtsrechtlichen Befugnissen Gebrauch zu machen und die Schließung der Sicherheitslücken anzuordnen,[2] falls nicht kurzfristig ein Update erfolgt. Wer personenbezogene Daten verarbeitet, muss eine angemessene Sicherheit der Verarbeitung sicherstellen und nachweisen können. Der Betrieb eines Microsoft Exchange Servers mit einer kritischen Sicherheitslücke erfüllt diese Anforderung nicht. Es handelt sich um einen Verstoß gegen die Datenschutz-Grundverordnung.[3]

Die Unternehmen zeigten sich kooperativ und ganz überwiegend auch dankbar. Die Meldungen, dass die Lücken geschlossen wurden, erreichten uns sehr zeitnah und konnten vom IT-Labor bestätigt werden. Die Erteilung

2 Auf Grundlage von Art. 58 Abs. 2 Buchst. d DSGVO.
3 Art. 32 DSGVO.

einer Anweisung war in keinem Fall notwendig. Wir haben die Verfahren mit Verwarnungen[4] beendet.

Fazit

Ein Patch- und Änderungsmanagement ist essenzieller Bestandteil eines jeden IT-Sicherheitskonzepts. Besorgniserregend ist, dass hierfür in vielen Unternehmen das erforderliche Bewusstsein fehlt oder die Umsetzung an anderen Gründen wie fehlenden Ressourcen scheitert. Umso wichtiger ist es, als Aufsichtsbehörde durch entsprechende Prüfungen auf Verbesserungen hinzuwirken.

4 Art. 58 Abs. 2 Buchst. a DSGVO.

G.4.6 Neuartige Datenverarbeitung in Kundenfahrzeugen der Marke Volkswagen

Automobilhersteller entwickeln neue Fahrzeugfunktionen oder verbessern diese. Um Trainingsdaten aus dem echten Verkehr zu gewinnen, nutzen sie oftmals spezielle Fahrzeuge.[1] Eine neuartige Vorgehensweise, die auch bei VW zum Einsatz kommen soll, zieht dabei auch Daten aus Kundenfahrzeugen heran.

Die Datenschutzaufsicht Niedersachsen steht gemeinsam mit den Datenschutz-Aufsichtsbehörden Baden-Württembergs und Bayerns im engen Austausch mit der Volkswagen AG und ihren deutschen Tochtermarken über die Einführung neuer Verfahren zur Verarbeitung von Fahrzeugdaten zur Verbesserung und Fortentwicklung der Fahrassistenz- und Fahrsicherheitssysteme.

Die Unternehmen hatten die jeweils zuständige Datenschutzaufsicht kontaktiert, um über die neuartige Datenverarbeitung zu informieren und datenschutzrechtliche Rahmenbedingungen zu besprechen.

Unternehmen hatten die zuständige Datenschutzaufsicht kontaktiert.

Die Volkswagen AG beabsichtigt, künftig kurze Sequenzen von Sensor- und Bilddaten der Umgebung aus Kundenfahrzeugen zu nutzen, um Fahrerassistenzsysteme und automatisierte Fahrfunktionen als zentrale Technologien für die Verbesserung der Verkehrssicherheit schneller und kontinuierlicher weiterentwickeln zu können. Beginnend in 2025 will das Unternehmen in einigen Fahrzeugserien anhand vorher festgelegter, eng definierter Szenarien das Ausleiten solcher Sequenzen auslösen und die Daten zur Produktverbesserung verarbeiten.

Solche Szenarien können laut Volkswagen zum Beispiel der Einsatz des Notbremsassistenten oder plötzliche Ausweichmanöver durch den Fahrer sein. Eine dauerhafte Datenübertragung zu diesem Zweck fände demgegenüber nicht statt. Zudem wird die Zustimmung der Fahrzeugnutzer und -nutzerinnen vorausgesetzt, denn die Privatsphäre der Fahrzeugsys-

1 Zu diesen Entwicklungsfahrten siehe Tätigkeitsbericht 2023, I.6.

teme des Halters wird durch das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz geschützt.[2] Mehr Informationen zur Technik und den in Betracht kommenden Fahrzeugmodellen hat die Volkswagen AG auf ihrer Webseite veröffentlicht.[3]

Die zuständigen Datenschutzbehörden haben diese technische Innovation eng begleitet. Gemeinsames Ziel ist es, die Verantwortlichen frühzeitig für datenschutzrechtliche Risiken und geeignete Maßnahmen zur Gewährleistung der Betroffenenrechte zu sensibilisieren und zur Einhaltung datenschutzrechtlicher Anforderungen anzuhalten. Die Aufsichtsbehörden stimmen überein, dass die neuen Verfahren bei zielgerichtetem Einsatz dazu geeignet sein können, die Fahrassistenzsysteme weiter zu verbessern und damit auch die Verkehrssicherheit zu erhöhen.

Fazit

Unsere Behörde hat ein Prüfverfahren begonnen, das derzeit noch andauert. Eine abschließende datenschutzrechtliche Bewertung konnte bis Ende 2024 noch nicht abgeben werden.

Die angesprochene Verarbeitung steht nach bisherigen Erkenntnissen nicht im Zusammenhang mit einer Verletzung des Schutzes personenbezogener Daten bei der Volkswagen AG, über die Ende 2024 medial berichtet wurde. Der Aufklärung dieser Datenschutzverletzung widmet sich unsere Behörde mit großer Sorgfalt.

2 Siehe dazu in diesem Tätigkeitsbericht G.3.1.

3 https://www.volkswagen.de/de/mehr/rechtliches/datenausleitung-zur-verbesserung-der-assistenzsysteme.html

G.4.7 Prüfung zum Auskunftsrecht: Niedersächsische Unternehmen schneiden gut ab

Die niedersächsische Datenschutzaufsicht überprüfte im Jahr 2024 im Rahmen einer koordinierten anlasslosen Kontrolle die Prozesse zum Auskunftsrecht. Während wir in Niedersachsen keine nennenswerten Defizite feststellen konnten, konstatierte der Europäische Datenschutzausschuss noch Herausforderungen für die vollständige Umsetzung des Auskunftsrechts.

Der Landesbeauftragte für den Datenschutz Niedersachsen beteiligte sich im Frühjahr 2024 an einer koordinierten Prüfung verschiedener europäischer Aufsichtsbehörden zur Implementierung des Auskunftsrechts durch Verantwortliche. Diese Prüfung erfolgte im Rahmen des Coordinated Enforcement Frameworks durch den Europäischen Datenschutzausschuss (EDSA). In Niedersachsen schrieben wir 15 Unternehmen aus unterschiedlichen Branchen an und forderten sie auf, einen strukturierten Fragebogen zu beantworten. Ziel der Prüfung war es, herauszufinden, ob und inwieweit die Unternehmen fest implementierte Prozesse zur Gewährleistung des Auskunftsrechts vorweisen können. Darüber hinaus interessierte uns, ob und inwiefern es allgemein praktische Hürden für Verantwortliche bei der Bearbeitung von Auskunftsanträgen gibt.

Dem Ergebnis unserer Kontrolle zufolge war den geprüften Unternehmen erfreulicherweise grundsätzlich bekannt, welche Anforderungen das Auskunftsrecht[1] an den Umgang mit Auskunftsanfragen stellt. Im Lauf der Prüfung konnten wir keine nennenswerten Mängel hinsichtlich des Umgangs mit Auskunftsanfragen feststellen. Im Übrigen ergab unsere Auswertung der Rückmeldungen, dass die Zahl der Auskunftsersuchen deutlich geringer war als wir im Vorfeld angenommen hatten.

Außer Niedersachsen beteiligten sich in Deutschland auch die Aufsichtsbehörden aus Bayern, Brandenburg, Mecklenburg-Vorpommern, Rheinland-

1 Art. 15 DSGVO.

Pfalz, dem Saarland und Schleswig-Holstein sowie die Bundesbeauftragte für den Datenschutz an der Prüfung. Europaweit nahmen 30 Aufsichtsbehörden an der Prüfung teil. Insgesamt wurden die Antworten von 1.185 Verantwortlichen aus dem nicht-öffentlichen und öffentlichen Bereich geprüft.

Fazit

Im Ergebnis bewerteten zwei Drittel aller beteiligten europäischen Aufsichtsbehörden die jeweiligen Ergebnisse als durchschnittlich bis gut. Die Auswertung der Ergebnisse der Umfrage auf europäischer Ebene zeigte aber auch, dass die für die Verarbeitung Verantwortlichen zum Teil noch nicht hinreichend über den Inhalt der EDSA-Leitlinien 01/2022 zu den Rechten der betroffenen Person – Auskunftsrecht[2] informiert waren und dass insofern noch eine weitere Sensibilisierung notwendig ist. Im Übrigen wurden bei einigen Verantwortlichen vereinzelte Probleme beobachtet. Der EDSA hat diese Probleme in seinem veröffentlichten Prüfbericht aufgelistet und hierzu Empfehlungen ausgesprochen.[3]

2 Kurzlink: https://t1p.de/edsa-guidelines (PDF).
3 Kurzlink: https://t1p.de/cef-2024

G.4.8 Corona-Gesundheitsdaten von Beschäftigten: Alles weg?

Während der Corona-Pandemie haben wir zahlreiche Beschwerden und Fragen von Beschäftigten zur Verarbeitung ihrer personenbezogenen Gesundheitsdaten durch den Arbeitgeber erhalten. Deshalb haben wir geprüft, ob Unternehmen mit den sogenannten 3G-Daten ihrer Beschäftigten richtig umgegangen sind – und sie inzwischen gelöscht haben.

Im Zuge der Corona-Pandemie haben Arbeitgeberinnen und Arbeitgeber auf Grundlage gesetzlicher Regelungen[1] zahlreiche personenbezogene Daten von Beschäftigten einschließlich ihrer Gesundheitsdaten[2] verarbeitet. Zwischenzeitlich sind viele dieser Regelungen als Rechtsgrundlage für die Datenverarbeitung weggefallen. Mit dem Wegfall der Rechtsgrundlage fielen auch die Zwecke für die Datenverarbeitung weg. Für diese Fälle regelt die Datenschutz-Grundverordnung (DSGVO) eine Pflicht der Verantwortlichen, gespeicherte personenbezogene Daten zu löschen.[3]

Im April 2022 forderten wir im Rahmen einer Presseerklärung Verantwortliche dazu auf, die im Zusammenhang mit der Pandemie gespeicherten personenbezogenen Daten zu löschen, soweit der Zweck der Datenverarbeitung weggefallen ist. Gleichzeitig behielten wir uns vor, anlasslose Kontrollen in Unternehmen und anderen Einrichtungen durchzuführen.

Durchführung der Kontrollen

Bereits in den Jahren 2022 und 2023 haben wir Vor-Ort-Kontrollen bei niedersächsischen Unternehmen durchgeführt. Die Auswahl der Unternehmen erfolgte anlasslos, wobei wir uns auf größere Unternehmen beschränkten. Unsere Prüfverfahren konnten wir 2024 abschließen.

1 Liste der infolge der Corona-Pandemie erlassenen deutschen Gesetze und Verordnungen, unter: https://t1p.de/corona-gesetze (Kurzlink)
2 Art. 4 Nr. 1 und 15 DSGVO.
3 Art. 17 Abs. 1 Buchst. a DSGVO.

Im Schwerpunkt konzentrierten wir uns bei den Kontrollen auf die Verarbeitung sogenannter 3G-Daten der Beschäftigten („Geimpft", „Genesen", „Getestet"). Dabei untersuchten wir insbesondere die Ausgestaltung der gesetzlich vorgeschriebenen Zutrittskontrollen[4] und, ob eine Löschung gespeicherter 3G-Daten der Beschäftigten nach Außerkrafttreten der gesetzlichen Pflicht zur Durchführung einer Zutrittskontrolle erfolgt war.

Darüber hinaus prüften wir, inwieweit die Unternehmen für Beschäftigte aus dem Personalbereich, die im Homeoffice tätig sind, ausreichende technische und organisatorischen Maßnahmen zum Schutz der verarbeiteten Daten getroffen haben.[5]

Prüfergebnisse

Im Rahmen unsere Prüfungen stellten wir fest, dass die geprüften Unternehmen die während der Corona-Pandemie durchzuführende Zutrittskontrollen in datenschutzrechtlich nicht zu beanstandender Weise durchgeführt haben.

Auch die ordnungsgemäße Löschung der 3G-Daten konnte unsere Behörde feststellen. Lediglich im Zusammenhang mit Erstattungsanträgen nach dem Infektionsschutzgesetz (IfSG)[6] verarbeiteten Unternehmen noch vereinzelt 3G-Daten der Beschäftigten. Dies war datenschutzrechtlich jedoch nicht zu beanstanden.

3G-Daten wurden ordnungsgemäß gelöscht.

Ebenfalls konnten wir uns davon überzeugen, dass alle geprüften Unternehmen geeignete technische und organisatorische Maßnahmen für die Datenverarbeitung durch Beschäftigte im Homeoffice getroffen haben.

Abschluss der Prüfung

Entsprechend unserer Pressemitteilung aus dem April 2022 und der wesentlichen Zielsetzung unserer Prüfung konnten wir feststellen, dass, soweit die Daten nicht mehr benötigt wurden, die gesetzlich vorgesehene

4 Vgl. § 28b IfSG alte Fassung.
5 Art. 24, 25 und 32 DSGVO.
6 Vgl. § 56 IfSG.

Löschung der 3G-Daten der Beschäftigten durch die geprüften Unternehmen erfolgt ist.

Infolge der sehr positiven Ergebnisse bei den geprüften „großen" Unternehmen entschieden wir uns zur Vermeidung unnötigen Verwaltungsaufwands bei uns und bei den Unternehmen, von weiteren anlasslosen Kontrollen im Kontext der 3G-Datenverarbeitung abzusehen.

Um auch kleine und mittelständischen Unternehmen für das Thema zu sensibilisieren, haben wir nach Abschluss unserer Prüfung Pressearbeit dazu gemacht und dabei insbesondere Branchenmagazine und Mitteilungsblätter der Kammern und Verbände in den Blick genommen.

Umgang mit Beschwerden bei sachgleichen zivilgerichtlichen Verfahren G.4.9

Immer wieder reichen Beschäftigte Datenschutzbeschwerden ein und führen gleichzeitig ein arbeitsgerichtliches Verfahren gegen ihren Arbeitgeber. Oft sind datenschutzrechtliche Fragen mittelbar oder unmittelbar Gegenstand des gerichtlichen Prozesses. Wir haben unsere Vorgehensweise in diesen Fällen umgestellt.

Die Fülle der Aufträge unserer Behörde und die Vielzahl der eingehenden Beschwerden, Datenpannen und Beratungsanfragen verlangt eine ständige Priorisierung beim Bearbeiten von Einzelfällen. Daneben bedarf es regelmäßig der Überprüfung von Verfahrensabläufen, um die Effizienz und Qualität unserer Arbeit zu gewährleisten.

Für Fallkonstellationen, in denen neben dem Beschwerdeverfahren ein gerichtliches Verfahren zwischen der beschwerdeführenden Person und der verantwortlichen Stelle geführt wird, haben wir eine Anpassung unserer Verfahrensweise vorgenommen.

Ist der Streitgegenstand des laufenden Gerichtsverfahrens (teilweise) sachgleich zu unserem Beschwerdeverfahren, setzen wir das Beschwerdeverfahren regelmäßig zunächst aus. Erst nach Abschluss des gerichtlichen Verfahrens nehmen wir das Beschwerdeverfahren wieder auf.

„Erledigung" durch Beendigung des Zivilprozesses

Hintergrund für diese Verfahrensänderung ist, dass wir in der Vergangenheit wiederholt feststellen mussten, dass sich die laufende Beschwerdebearbeitung durch den Abschluss des parallel geführten gerichtlichen Verfahrens überholt hatte.

So erhielten wir etwa nach der Beendigung des gerichtlichen Verfahrens seitens eines Beschwerdeführers die Mitteilung, dass sein Interesse an der weiteren Verfolgung der datenschutzrechtlichen Beschwerde nicht mehr bestehe. In anderen Fällen schlossen die Parteien im Rahmen des Zivilprozesses einen gerichtlichen Vergleich, mit dem die Geltendmachung sol-

cher Ansprüche ausgeschlossen wurde, die zugleich den Gegenstand der datenschutzrechtlichen Beschwerde ausmachten.

Dies hatte jeweils zur Folge, dass wir unsere Beschwerdeverfahren beendeten und die bereits erfolgte Bearbeitung der Verfahren überwiegend gegenstandslos wurde.

Effizientere Beschwerdeverfahren

Mit der Umstellung unserer Verfahrensweise stellen wir nunmehr sicher, dass wir das Beschwerdeverfahren zielgerichtet und ressourcenschonend durchführen. Wie unsere Erfahrungen gezeigt haben, kann die zeitgleiche Bearbeitung von Beschwerde- und Gerichtsverfahren zu einer unnötigen Bindung von Ressourcen führen. Mit der Aussetzung des Verfahrens schaffen wir Raum, um Einzelfälle effizienter zu bearbeiten und unsere Kapazitäten dort einzusetzen, wo sie am dringendsten benötigt werden. Zudem bietet sich die Möglichkeit, zu erwartende rechtliche und tatsächliche Erkenntnisse aus dem gerichtlichen Verfahren für die Bearbeitung des Beschwerdeverfahrens zu nutzen.

Unsere Vorgehensweise erfolgt im Einklang mit den Vorgaben des Verwaltungsverfahrensgesetzes.[1] Danach ist ein Verwaltungsverfahren unter anderem einfach und zweckmäßig durchzuführen. Nach dem Grundsatz eines ressourcenschonenden Einsatzes von Zeit und Personal ist dabei insbesondere eine „Doppelarbeit" durch öffentliche Stellen zu vermeiden.

1 § 10 S. 2 VwVfG in Verbindung mit § 1 Abs. 1 NVwVfG.

Gesundheit und Soziales

Große Fortschritte bei der Digitalisierung des Gesundheitswesens G.5.1

Im Jahr 2024 haben wir uns intensiv mit den sich ändernden rechtlichen, technischen und praktischen Verhältnissen im Gesundheitswesen auseinandergesetzt – von elektronischer Patientenakte über das E-Rezept bis zum Fax-Ersatz KIM. Größere Datenschutzvorfälle sind in Niedersachsen ausgeblieben. Auch im Datenschutz gilt der aus der Medizin bekannte Präventionsgrundsatz: Besser vorbeugen statt später heilen.

Voraussichtlich ab Mitte Februar 2025 wird die elektronische Patientenakte (ePA) flächendeckend und damit auch in Niedersachsen jeder gesetzlich krankenversicherten Person automatisch von der Krankenkasse zur Verfügung gestellt. Vor dem Anlegen der elektronischen Patientenakte erhalten die Versicherten eine umfangreiche Information über die Funktionen und über ihre Rechte bei der Datenverarbeitung. Denn der Umfang der Datenverarbeitung wird maximal erweitert.

Alle behandelnden Ärztinnen und Ärzte müssen zukünftig sämtliche Daten aus der aktuellen Behandlung in die elektronische Patientenakte einstellen. Alle gesetzlich zum lesenden Zugriff befugten Stellen wie Arztpraxen, Krankenhäuser oder Apotheken können die gespeicherten Dokumente zur Kenntnis nehmen. Hinzu kommt, dass alle gespeicherten medizinischen Daten in pseudonymisierter Form an das beim Bundesamt für Arzneimittel angegliederte Forschungsdatenzentrum übermittelt werden.

Elektronische Patientenakte und Datenschutz

Diese Neuerung stellt einen bislang nicht dagewesenen Eingriff in das Recht auf informationelle Selbstbestimmung der Versicherten dar. Der Bundesgesetzgeber hat den Versicherten zumindest das Recht eingeräumt, gegenüber ihrer Krankenkasse dem Anlegen der elektronischen Patientenakte in Gänze zu widersprechen oder den standardmäßig vorgegebenen Vollzugriff für alle Befugten einzuschränken (Opt-Out).

Versicherte, die bereits zuvor auf freiwilliger Basis eine elektronische Patientenakte genutzt haben, müssen eigenständig prüfen, ob bereits vorgenommene Einschränkungen der Sichtbarkeit von Dokumenten korrekt in die neue elektronische Patientenakte übernommen wurden.

Damit wir den erwartbaren Anfragen und Beschwerden gerecht werden können, haben wir uns eingehend mit der elektronischen Patientenakte beschäftigt. In diesem Zusammenhang haben wir uns die einzelnen Funktionen von einer gesetzlichen Krankenkasse zeigen und technische Abläufe im Hintergrund erläutern lassen. Aus den gesammelten Informationen haben wir für die Betroffenen ein FAQ mit den wesentlichen Fragen zum Datenschutz erstellt. Dieses ist über den Link https://lfd.niedersachsen.de/epa erreichbar.

E-Rezept

Das elektronische Rezept wurde bereits im Jahr 2023 großflächig eingeführt, seit dem 1. Januar 2024 ist es Pflicht für alle Beteiligten. Die Umsetzung des E-Rezepts funktionierte aus datenschutzrechtlicher Sicht in Niedersachsen geräuschlos. Bislang sind keine Beschwerden oder Beratungsanfragen bei uns eingegangen.

Wir führen dies auch auf unsere im Jahr 2023 durchgeführte Prüfung von Apotheken[1] zurück, bei welcher am Rande die in der Praxis bestehenden Schwierigkeiten bei der Umsetzung des E-Rezepts angesprochen und behoben wurden. Damals hatten wir unseren Bericht der Apothekerkammer zukommen lassen und diese gebeten, die Mitgliedsapotheken über die Erkenntnisse aus der Prüfung zu unterrichten.

1 Tätigkeitsbericht 2023 (G.4.1).

KIM statt Fax

Der von der Nationalen Agentur für Digitale Medizin (gematik GmbH) im Rahmen der Telematik-Infrastruktur betriebene E-Mail-Dienst für das Gesundheitswesen (KIM) wurde im Rahmen des Digitalgesetzes zum 1. Juli 2024 für alle niedergelassenen Ärztinnen und Ärzte verpflichtend eingeführt. KIM ermöglicht eine von Ende-zu-Ende verschlüsselte Datenübertragung und ersetzt E-Mail und Fax.

Elektronische Arztbriefe datenschutzkonform an andere Leistungserbringer.

Ärztinnen und Ärzte können nun elektronische Arztbriefe datenschutzkonform an andere Leistungserbringer, die an die Telematik-Infrastruktur angeschlossen sind, übermitteln. Wir haben die Heilberufskammern gebeten, ihre Mitglieder darüber in Kenntnis zu setzen, dass zukünftig sämtliche Kommunikation zwischen den an der Telematik-Infrastruktur angebundenen Leistungserbringer im Gesundheitswesen über KIM zu erfolgen hat.

Runder Tisch im Gesundheitswesen

Der 2019 zusammen mit uns ins Leben gerufene „Runde Tisch im Gesundheitswesen" ist eine Austauschplattform für datenschutzrechtliche Themen zwischen der Datenschutzaufsichtsbehörde und den Kammern im Gesundheitswesen sowie der Kassenärztlichen Vereinigung und der Kassenzahnärztlichen Vereinigung. Insbesondere mit Blick auf die Digitalisierung im Gesundheitswesen haben sich die Gespräche als gewinnbringend für alle Akteure gezeigt. In der Sitzung am 19. August 2024 haben wir gemeinsam entschieden, dass dieses Treffen künftig jährlich stattfinden soll.

Ein Kernthema 2024 war der Umgang in der Praxis mit dem bereits im Tätigkeitsbericht 2023 vorgestellten Urteil des Europäischen Gerichtshofes zur ersten kostenlosen Kopie der Patientenakte.[2] Die Heilberufskammern haben ihre Mitglieder auf das Urteil hingewiesen, was offenbar zu einem leichten Rückgang der Beschwerden in diesem Bereich geführt hat. Unmittelbar im Anschluss des Runden Tisches hat die Datenschutzkonferenz die Kammern aufgefordert, die Berufsordnungen entsprechend dem Urteil an-

2 Tätigkeitsbericht 2023, G.4.5.

zupassen. Die Psychotherapeutenkammer hatte dies zu diesem Zeitpunkt bereits getan, die übrigen wollen nachziehen.

Digitalisierungsforum für den Öffentlichen Gesundheitsdienst

In Kooperation mit dem Niedersächsisches Studieninstitut für kommunale Verwaltung e. V. (NSI) wurde am 27. Februar 2024 ein Workshop beim Digitalisierungsforum des Öffentlichen Gesundheitsdienstes Niedersachsen zum Thema „Datenpannen und Notfallmanagement“ durchgeführt.

In dem Workshop haben wir den Teilnehmenden praxisnah den rechtssicheren Umgang mit Datenpannen und die damit verbundenen technisch-organisatorischen Bezüge erläutert. In Zusammenarbeit mit dem NSI konnten wir die erforderlichen Schritte sowohl aus Sicht der Verantwortlichen, als auch aus Sicht der Aufsichtsbehörde nachvollziehbar vermitteln. Sowohl die Teilnehmenden als auch die Referenten haben diese Art Workshop als sehr positiv und gewinnbringend bewertet.

Sicherheitslücke bei Kita-App betrifft auch Niedersachsen

G.5.2

Die auf Kitas und Pflegeeinrichtungen spezialisierte App Stay Informed hatte 2024 mit einem größeren Datenleck zu kämpfen. Aufgrund einer Fehlkonfiguration auf dem Webserver des Anbieters war eine große Menge schützenswerter personenbezogener Daten über das Internet frei abrufbar, betroffen waren auch Nutzerinnen und Nutzer in Niedersachsen. Der App-Anbieter reagierte unverzüglich, schloss das Datenleck und informierte über den Vorfall auf seiner Homepage in Form von FAQs.

Ein anonymer Hinweisgeber informierte die Redaktion des Computerfachmagazins c't Mitte März 2024 über eine Fehlkonfiguration auf einem Webserver der Firma Stay Informed GmbH.[1] Diese Lücke hatte zur Folge, dass personenbezogene Daten frühestens seit dem 20. Oktober 2021 und spätestens seit dem 18. August 2023 über das Internet frei abrufbar waren. Mehr als 11.000 Einrichtungen nutzten die App Stay Informed nach Recherchen der c't zum Zeitpunkt der Veröffentlichung bundesweit, darunter Kindertageseinrichtungen, Horte, Schulen und Pflegeeinrichtungen. Über die App können Kindertagesstätten und Schulen beispielsweise mit den Eltern der Kinder kommunizieren. Die Firma Stay Informed GmbH, die als Auftragsdatenverarbeiter mit Sitz in Freiburg agiert, hat die gemeldete Lücke an dem betroffenen Server nach eigenen Angaben am 18. März 2024 binnen zwei Stunden nach Kenntnis des Vorfalls geschlossen. Ferner hatte sie eine Untersuchung durch interne und externe IT-Fachleute angekündigt. Ziel dieser Untersuchung war es, mögliche weitere Schwachstellen zu finden und Zugriffe auf die Dateien nachzuvollziehen.

Stay Informed hat den Vorfall der für sie zuständigen datenschutzrechtlichen Aufsichtsbehörde gemeldet, dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg. Ferner hat sie die betroffenen Träger und Einrichtungen, für die sie als Auftragsverarbeiter

1 https://heise.de/-9667323

tätig ist, am 26. März 2024 mit Verweis auf ihre FAQ zu diesem Vorfall informiert.[2] Dieses FAQ wurde anschließend regelmäßig aktualisiert

Die datenschutzrechtliche Verantwortung für den Vorfall liegt bei den kommunalen und privaten Trägern beziehungsweise den Schulen, die eine Auftragsvereinbarung zur Nutzung der Kita- und Schul-App mit Stay Informed geschlossen haben. Daher sind 60 Träger von Kindertagesstätten sowie vier Schulen in Niedersachsen ihrer Meldepflicht gemäß Artikel 33 Datenschutz-Grundverordnung nachgekommen und haben uns diesen Vorfall gemeldet.

Nach dem bisherigen Rechercheergebnis des Unternehmens waren von dem Vorfall vier Datentypen betroffen, die auf dem Webserver lagen:

- PDF-Anhänge von Chat-Nachrichten, die die Einrichtungen an Eltern geschickt haben
- Avatare (Profilbilder)
- Digitale Unterschriftengrafiken, die allerdings verschlüsselt wurden
- Aus anderen Systemen von den Einrichtungen exportierte Dateien, deren Import in die App fehlgeschlagen ist.

Die Inhalte der aus anderen Systemen exportierten Dateien unterschieden sich teilweise sehr stark, enthielten aber teilweise vollständige Datensätze mit Namen und Geburtsdaten der Kinder sowie Namen, Anschriften und Telefonnummer der Sorgeberechtigten.

Der Firma Stay informed GmbH lagen keine Erpressungsschreiben vor. Auch sonstige Anhaltspunkte, dass es eine Manipulation an der Software oder an den darin gespeicherten Daten gab, waren nicht ersichtlich. Angesichts dessen bestand voraussichtlich keine Gefahr für die von dem Vorfall betroffenen Personen. Eine abschließende Bewertung des Vorfalls ist erst möglich, sobald die zuständige Aufsicht in Baden-Württemberg den umfangreichen forensische Untersuchungsbericht des Unternehmens ausgewertet hat.

2 https://www.stayinformed.de/informationen-zur-datenpanne

Datenverarbeitung im Rahmen des Masern-Impfnachweises G.5.3

Regelmäßig fragen uns besorgte Eltern, welche Befugnisse beim Nachweis eines Masernimpfschutzes von Kindern in der Kindertagesstätte oder der Grundschule bestehen und welche Datenverarbeitungen zulässig sind. Wir haben dazu auf unserer Website[1] die wichtigsten Datenschutzfragen beantwortet.

Kommt ein Kind in eine Kita, eine Kindertagespflege[2] oder in die Grundschule, wird eine Vielzahl von Daten über das Kind erhoben. Spätestens, wenn auch nach Gesundheitsdaten gefragt wird, stellen sich viele „Personensorgeberechtigte" – in der Regel die Eltern – die Frage, ob dies überhaupt zulässig ist. Auch Kitas und Schulen wenden sich an unsere Behörde, um sich rund um den Datenschutz beim Impfnachweis zu informieren.

Rechtsgrundlage der Datenverarbeitung

Durch das Gesetz für den Schutz vor Masern wurde im März 2020 das Infektionsschutzgesetz (IfSG) um Regelungen zum Nachweis einer bestehenden Schutzimpfung gegen Masern oder einer bestehenden Kontraindikation erweitert.

Demnach müssen alle Kinder, die in einer Gemeinschaftseinrichtung[3] wie beispielsweise einer Kindertagesstätte, bei einer Tagespflegeperson oder in der Grundschule betreut werden, einen ausreichenden Impfschutz gegen Masern oder ab der Vollendung des ersten Lebensjahres eine Immunität gegen Masern aufweisen.[4] Eine Ausnahme gilt nur für die Kinder, die aufgrund einer medizinischen Kontraindikation nicht geimpft werden können.[5]

1 lfd.niedersachsen.de/masern/
2 § 43 Achtes Buch Sozialgesetzbuch (SGB VIII).
3 § 33 IfSG.
4 § 20 Absatz 8 Satz 1 IfSG.
5 § 20 Abs. 8 Satz 4 IfSG.

Wer den Impfnachweis anfordern darf

Eltern fragen oft, weshalb sie einen Nachweis, den sie bereits bei der Kindertagesstätte vorgelegt haben, auch der Grundschule vorlegen müssen. Hier ist zu beachten, dass jede der oben genannten Einrichtungen eine eigenständig verantwortliche Stelle ist. Das bedeutet, dass jede Einrichtung verpflichtet ist, die Prüfung eigenständig vorzunehmen.[6] Die Unterlassung dieser Prüfpflicht ist bußgeldbewährt.[7]

Dies hat zur Folge, dass die Eltern den Impfschutz oder den Grund für eine Kontraindikation grundsätzlich bei jeder Einrichtung nachweisen müssen, es sei denn, eine vorher besuchte Einrichtung oder eine staatliche Stelle bestätigt einen entsprechenden Nachweis gegenüber der neuen Einrichtung.[8]

Wird der Impfnachweis beispielsweise im Rahmen der Schuleingangsuntersuchung vorgelegt, kann das Gesundheitsamt die Information über die Vorlage des Nachweises mit Einwilligung der Eltern an die aufnehmende Grundschule weitergeben. Da das IfSG ausdrücklich nur die Vorlage der entsprechenden Bescheinigung oder des ärztlichen Gutachtens regelt, schließt dies die Anfertigung einer Kopie durch die verantwortliche Stelle aus.[9]

Wenn kein Nachweis vorgelegt wird

Wird der Nachweis nicht vorgelegt oder bestehen bei der Einrichtungsleitung Zweifel an der Echtheit oder inhaltlichen Richtigkeit des Nachweises, hat diese unter Angabe von personenbezogenen Daten des betroffenen Kindes und der Eltern unverzüglich das Gesundheitsamt zu benachrichtigen.[10]

Wird das Gesundheitsamt tätig, kann es die entsprechenden Nachweise direkt von den Eltern anfordern. In diesem Fall sind die Eltern verpflichtet, dem Gesundheitsamt die angeforderten Nachweise vorzulegen.[11]

6 § 20 Abs. 9 IfSG.
7 § 73 Abs. 1 a Nr. 7a IfSG.
8 § 20 Abs. 9 Satz 1 Nr. 3 IfSG.
9 § 20 Abs. 9 Satz 1 IfSG.
10 § 20 Abs. 9a Satz 2 IfSG.
11 § 20 Abs. 12 Satz 1 Nr. 1 IfSG.

Bestehen seitens des Gesundheitsamtes Zweifel an der Echtheit oder inhaltlichen Richtigkeit des vorgelegten Nachweises einer Kontraindikation, so kann es eine ärztliche Untersuchung zur Feststellung anordnen, ob die betroffene Person auf Grund einer medizinischen Kontraindikation nicht gegen Masern geimpft werden kann. Behandelnde Ärztinnen und Ärzte sind zudem zur Auskunft gegenüber dem Gesundheitsamt verpflichtet.[12]

Unter https://lfd.niedersachsen.de/masern/ finden Sie ausführliche Informationen rund um den Datenschutz beim Nachweis der Masernschutzimpfung.

12 § 20 Abs. 12 Satz 2 IfSG.

G.5.4 Zu viele Fragen bei Schuleingangsuntersuchungen

Schuleingangsuntersuchungen sind ein wichtiger Baustein im Leben eines jeden Kindes. Doch wenn das Amt dabei sensible Daten überbordend abfragt, kann dies das Vertrauen der Eltern in die staatliche Untersuchung erschüttern. Aufgrund verschiedener Beschwerden haben wir Gespräche mit dem Niedersächsischen Landesgesundheitsamt geführt und eine datenschutzkonforme Lösung gefunden.

In der Vergangenheit erhielten wir Beschwerden von Eltern zu Schuleingangsuntersuchungen. Diese richteten sich insbesondere gegen eine überbordende Datenerhebung durch die Gesundheitsämter. Die Ämter verpflichteten die Eltern beispielsweise, hochsensible Daten zu ihren Kindern anzugeben, etwa zum Zusammenleben in der Familie, zur Art der Geburt ihres Kindes oder ob Bettnässen vorkomme. In einigen Fällen sollten Eltern sogar die Ärztinnen und Ärzte der Kinder benennen und diese gegenüber dem Amt von der ärztlichen Schweigepflicht entbinden.

Rechtlicher Rahmen der Schuleingangsuntersuchung

Rechtlich dient die Schuleingangsuntersuchung ausschließlich dem Zweck der Feststellung der Schulfähigkeit. Denn mit Vollendung des sechsten Lebensjahres wird ein Kind grundsätzlich schulpflichtig. Im Rahmen der Schuleingangsuntersuchung prüft das örtliche Gesundheitsamt mögliche körperliche, geistige oder soziale Entwicklungsverzögerungen, die den Schulstart erschweren könnten. Das Ergebnis dient als gutachterliche Stellungnahme, die die Grundschule bei der Entscheidung unterstützen soll, ob das Kind eingeschult oder zurückgestellt wird.

Das Niedersächsische Schulgesetz verpflichtet alle Kinder zur Teilnahme an der Schuleingangsuntersuchung.[1] Zudem sind die Kinder und die Eltern zur Erteilung der zwingend erforderlichen Auskünfte während der Untersuchung vor Ort verpflichtet. Eine weitergehende Datenerhebung seitens des

1 § 56 Abs. 1 Satz 1 NSchG.

Gesundheitsamtes bei anderen Stellen ist vom gesetzlichen Auftrag nicht umfasst, sodass es beispielsweise nicht erforderlich ist, eine Entbindung von der Schweigepflicht einzuholen. Der Gesetzgeber hat zudem keine Sanktionsmöglichkeit vorgesehen, wenn die Eltern nicht mitwirken. Kommen Eltern ihrer Auskunftspflicht nicht nach, gilt das Kind als schulfähig.

Zu viele Fragen als Pflichtangaben gekennzeichnet

Zur Vorbereitung auf die Schuleingangsuntersuchung erhalten die Erziehungsberechtigten einige Wochen vor dem Untersuchungstermin einen sogenannten Elternfragebogen mit den für die Untersuchung relevanten Fragen sowie freiwilligen Angaben. Ein Muster dieses Fragebogens wird den Gesundheitsämtern vom Niedersächsischen Landesgesundheitsamt zur Verfügung gestellt.[2]

Unsere datenschutzrechtliche Überprüfung hat ergeben, dass zu viele Fragen als Pflichtangaben gekennzeichnet waren. Zudem haben einige Gesundheitsämter den Eindruck erweckt, der komplette Fragebogen sei im Vorfeld verpflichtend auszufüllen und bei der Untersuchung abzugeben. Dies ist unzutreffend. Der Elternfragebogen dient ausschließlich den Eltern zur Vorbereitung auf die Schuleingangsuntersuchung.

Das Landesgesundheitsamt hat uns gegenüber dargelegt, dass die Gesundheitsämter vor Ort den Sinn und Zweck der Schuleingangsuntersuchung sehr weit auslegen. Außer der reinen Prüfung der Schulfähigkeit liegt der Fokus der Ärztinnen und Ärzte auch in der ganzheitlichen Betrachtung der Entwicklung des Kindes. Sie versuchen eine Prognose für die gesamte Zeit in der Grundschule abzugeben. Und sie geben Hinweise zu etwaigem Förderbedarf oder zur weiteren Untersuchung von Auffälligkeiten durch weiterbehandelnde Ärztinnen und Ärzte. Diese weitergehenden Untersuchungen und Beratungen seien für das Kind sehr wertvoll.

Das Ziel ist nachvollziehbar. Nach derzeitiger Rechtslage dient die Schuleingangsuntersuchung allerdings ausschließlich der Prüfung der Zurückstellung eines Kindes vom Schulbesuch.[3] Daher sind auch nur die hierfür zwingend erforderlichen Fragen von der Mitwirkungspflicht umfasst. Sensible Fragen zu Themen wie Bettnässen oder zur Art der Geburt müssen daher

2 § 5 Abs. 2 Satz 5 NGöGD.
3 § 56 Abs. 1 Satz 1 Nr. 1 NSchG.

als freiwillige Angaben klar gekennzeichnet werden – sofern sie überhaupt zu stellen sind.

Datenschutzkonforme Anpassungen erforderlich

Wir haben dem Landesgesundheitsamt daher empfohlen, den Muster-Fragebogen für die Eltern zu überarbeiten und die Schuleingangsuntersuchung möglichst vollständig auf die freiwillige Mitwirkung der Eltern auszurichten.

Freiwilligkeit ist im Fragebogen stärker herauszustellen.

Eine datenschutzkonforme Schuleingangsuntersuchung ist möglich. Dazu müssen die zwingend erforderlichen und damit verpflichtenden Kernfragen im Fragebogen deutlich gekennzeichnet sein. Darüber hinaus sollte der Hintergrund des Fragebogens sowie der Sinn der freiwilligen Fragen verständlich erklärt werden, damit die Eltern besser nachvollziehen zu können, welche Vorteile für das eigene Kind das Beantworten mit sich bringt.

Mit dem Landesgesundheitsamt hat unsere Behörde vereinbart, dass das dortige Muster des Elternfragebogens datenschutzkonform überarbeitet und den Gesundheitsämtern der Landkreise und kreisfreien Städten mit der Bitte um künftige Berücksichtigung zur Verfügung gestellt wird.

Wir gehen davon aus, dass sich alle Gesundheitsämter an das datenschutzkonforme Muster halten und ihre Anschreiben an die Eltern entsprechend anpassen werden.

Kommunen und Verwaltung

Microsoft Teams in der Landesverwaltung G.6.1

Im April 2024 hat das Niedersächsische Ministerium für Inneres und Sport Vertragsverhandlungen mit Microsoft zur Nutzung der Plattform Teams für die Landesverwaltung abgeschlossen. Wir haben das Innenministerium hierzu vor Beginn der Verhandlungen zu Datenschutzfragen beraten und die Ergebnisse bewertet.

Hintergrund der Verhandlungen war der Wunsch der niedersächsischen Landesverwaltung, das bisher genutzte Videokonferenztool Skype for Business durch das aktuellere Produkt Microsoft Teams zu ersetzen. Teams gehört zur Produktfamilie MS 365. Die datenschutzrechtlichen Regelungen für die Nutzung finden sich in dem Data Protection Addendum (DPA) dieser Software, zu dem sich die Datenschutzkonferenz (DSK) im November 2022 positioniert hat. Dabei hatte sie Mängel festgestellt, die sich sieben wesentlichen Problemfeldern zuordnen lassen.[1]

Wie im Tätigkeitsbericht 2023 berichtet haben wir in einem ersten Schritt zusammen mit sechs anderen Datenschutzbehörden eine Handreichung für die Verantwortlichen erstellt, die an bestimmte von der Datenschutzkonferenz ermittelten Problemfelder anknüpft.[2]

In einem nächsten Schritt haben wir daraus konkretisierende Empfehlungen für die Vertragsgestaltung abgeleitet. Damit konnten wir dem niedersächsischen Innenministerium eine Hilfestellung geben, wie eine akzeptable Datenschutzvereinbarung erreicht werden könnte. An den Ver-

1 DSK, Abschlussbericht zur aktuellen Vereinbarung zur Auftragsverarbeitung für Microsoft 365 vom 2.11.2022: https://lfd.niedersachsen.de/dsk-ms365

2 Handreichung zur Auftragsverarbeitungs-Vereinbarung für Microsoft 365 vom 24. August 2023, https://lfd.niedersachsen.de/225721.html

handlungen selbst war unsere Behörde nicht beteiligt, wir haben allerdings das Ergebnis und die Zwischenergebnisse bewertet.

Aus unserer Sicht besteht mit Blick auf die Ergebnisse noch ein deutliches Potenzial für datenschutzfreundlichere Regelungen.[3] Außerdem haben die Verantwortlichen auf Grundlage der vertraglichen Vereinbarungen weiterhin etliche praktische Umsetzungsfragen zu klären, um einen datenschutzrechtlich einwandfreien Betrieb von MS Team gewährleisten zu können. Wir haben dem Innenministerium dazu umfangreiche Hinweise gegeben. Vorbehaltlich der Beachtung dieser (im Folgenden skizzierten) Hinweise haben wir den Einsatz von Teams auf Basis des Verhandlungsergebnisses für akzeptabel befunden.

Datentransfer in Drittländer

Ein Aspekt, für den es lange keine einfache Lösung zu geben schien, war der mit der Nutzung von Microsoft-Onlinediensten verbundene Transfer personenbezogener Daten in sogenannte Drittländer, darunter die USA. Am 10. Juni 2023 hat die EU-Kommission ein angemessenes Datenschutzniveau bei der Verarbeitung personenbezogener Daten in den USA durch Unternehmen festgestellt, die nach dem EU-US-Data Privacy Framework zertifiziert sind.[4] Zudem wurde zwischen der niedersächsischen Landesverwaltung und Microsoft die Verarbeitung innerhalb der sogenannten EU-Datengrenze (EU Data Boundary) vereinbart.

Wir haben allerdings im Rahmen unserer finalen Bewertung darauf hingewiesen, dass auch bei der Anwendung der EU-Datengrenze in bestimmten Fällen weitere Übermittlungen in Drittländer nicht ausgeschlossen werden könnten und sich die Verantwortlichen damit beschäftigen müssten.

Weitere Pflichten für den Verantwortlichen

Zahlreiche Anfragen an uns, aber auch Veröffentlichungen in den Medien zeigen, dass unsere Bewertung als „akzeptabel" vielfach missverstanden wurde. Oft wird übersehen, dass dieses Bewertungsergebnis mit weiteren

3 Siehe auch „Microsoft Teams in der Landesverwaltung Niedersachsen", https://lfd.niedersachsen.de/231856.html

4 Siehe auch „Datenübermittlung in die USA: EU erlässt neuen Angemessenheitsbeschluss", https://lfd.niedersachsen.de/223847.html

Hinweisen verknüpft ist und sich unsere Prüfung ausschließlich auf die Frage bezog, ob das nachverhandelte DPA den Anforderungen aus Artikel 28 Absatz 3 der Datenschutz-Grundverordnung (DSGVO) genügt. Dieses zu bejahen befreit den Verantwortlichen nicht von seinen Pflichten, die auch bei jeder anderen Verarbeitung für ihn gelten.

Im konkreten Fall muss der Verantwortliche zusätzlich zum geänderten DPA beispielsweise überprüfen, inwieweit die von Microsoft getroffenen technischen und organisatorischen Maßnahmen für den Schutz seiner Daten angemessen sind und inwiefern der Verantwortliche selbst für die Verarbeitung sämtlicher personenbezogener Daten, die Microsoft in seinem Auftrag verarbeitet, eine Rechtsgrundlage hat. Ferner muss der Verantwortliche eine Schwellwertprüfung und eine gegebenenfalls darauffolgende Datenschutzfolgenabschätzung durchführen. Auf diese Schritte bezog sich unsere Beratung jedoch nicht.

Es besteht noch ein deutliches Potenzial für datenschutzfreundlichere Regelungen.

Fazit

Wir freuen uns, dass unsere Beratung infolge einer frühzeitigen Einbindung durch das Innenministerium zu deutlichen Verbesserungen des DPA geführt hat. Allerdings gibt es nach wie vor keinen datenschutzrechtlichen Freifahrtschein für den Einsatz von MS 365-Produkten wie Teams.

G.6.2 Digitalisierung des Staats: Fortschritte bei Onlinezugangsgesetz und Registermodernisierung

Im Jahr 2024 haben wir unsere Beratung zu den beiden maßgeblichen Säulen der Verwaltungsdigitalisierung fortgesetzt – dem Onlinezugangsgesetz und der Registermodernisierung. Einige unserer Vorschläge haben Bund und Länder umgesetzt, allerdings wäre aus Sicht der DSK eine deutlichere Begrenzung des Anwendungsbereichs des NOOTS-Staatsvertrages wünschenswert gewesen.

Als Teil der Kontaktgruppe OZG 2.0 hat unsere Behörde den Gesetzgebungsprozess zum OZG-Änderungsgesetz begleitet und im Jahr 2024 eine entsprechende Orientierungshilfe[1] erstellt. Daneben lag ein wichtiger Schwerpunkt unserer Tätigkeit als Teil der Kontaktgruppe „Registermodernisierung" auf der Beratung des Projekts „Gesamtsteuerung Registermodernisierung". Die Kontaktgruppe befasste sich mit den datenschutzrechtlichen Anforderungen bei der Gestaltung des Bund-Länder-Staatsvertrags über die Errichtung und den Betrieb des National Once-Only-Technical-Systems (NOOTS). Die Regierungschefinnen und -chefs von Bund und Ländern haben den Staatsvertrag im Dezember 2024 beschlossen.[2] Zum Inkrafttreten des Vertrages bedarf es noch der Ratifikation durch eine qualifizierte Mehrheit der Vertragspartner.

Da über das NOOTS Nachweise unter den Behörden ausgetauscht werden und damit personenbezogene Daten fließen sollen, stellte sich insbesondere die Frage der datenschutzrechtlichen Verantwortlichkeit für die Verarbeitung über das NOOTS sowie die Frage der Rechtsgrundlage der Verarbeitung. Die datenschutzrechtliche Verantwortlichkeit haben Bund und Länder durch den Staatsvertrag dem Bundesverwaltungsamt zugewiesen. Die Rechtsgrundlage der Verarbeitung ist in § 7 des Staatsvertrages[3] enthalten.

1 Siehe Kapitel I.5 zur Orientierungshilfe.
2 Kurzlink zur Pressemitteilung: https://t1p.de/register24
3 In Verbindung mit Art. 6 Abs. 1 Buchst. e, Abs. 2 und Abs. 3 S. 1 Buchst. b DSGVO.

Während einige Verbesserungsvorschläge unserer Kontaktgruppe im Rahmen der Erstellung des Vertragsentwurfs berücksichtigt wurden, wurden andere Forderungen nicht umgesetzt. Nicht eingeschränkt wurde beispielsweise der Anwendungsbereich des Staatsvertrages nach dem Vorbild des ID-Nummerngesetzes[4] auf solche Nachweisabrufe, für die das NOOTS ursprünglich vorgesehen war – das heißt insbesondere auf Abrufe für die Erbringung von Leistungen nach dem Onlinezugangsgesetz. Stattdessen ist der Anwendungsbereich des Staatsvertrages weit geblieben. Hier werden wir die weitere Entwicklung umso genauer beobachten.

Fazit

Die Registermodernisierung ist noch lange nicht abgeschlossen und wird von uns auch in den kommenden Jahren begleitet und auf den Prüfstand gestellt werden.

4 Vgl. § 5 Abs. 1 S. 2 IDNrG.

G.6.3 Prüfung von Kommunen: Diskretion im Bürgerbüro

Im Nachgang zu unserer Prüfung im kommunalen Bereich haben wir in einer Stichprobe vier Bürgerbüros vor Ort besucht. Hintergrund war auch, dass uns in der Vergangenheit Beschwerden zu möglichen Datenschutzverletzungen aufgrund der Gestaltung der Räumlichkeiten erreichten.

Viele Kommunen bieten die Möglichkeit, in sogenannten Bürgerbüros unterschiedliche Angelegenheiten zu erledigen. Je nach Zuständigkeitsbereich können Bürgerinnen und Bürger dort ihr Kraftfahrzeug anmelden, Ausweise beantragen und vieles mehr erledigen. Aus der Vielfalt der vorgehaltenen Aufgaben ergibt sich, dass in den Büros mit personenbezogenen Daten von unterschiedlicher Sensibilität hantiert wird. Den Schutz dieser Daten während der Sprechzeiten gilt es für die Kommunen sicherzustellen.

Datenschutz durch organisatorische Maßnahmen

Aus datenschutzrechtlicher Sicht sind bei der Auswahl der Räumlichkeiten insbesondere folgende Punkte zu berücksichtigen:

- Ist ein gesonderter Wartebereich vorhanden?
- Sind die Bildschirme der Beschäftigten vor der Einsicht durch Dritte geschützt?
- Ist ein ausreichender Abstand zwischen den Beratungsplätzen und somit eine Diskretion sichergestellt?
- Können Gespräche bei Bedarf (auf Wunsch) in einem gesonderten Büro geführt werden?

Viele Kommunen sind dazu übergegangen, für Angelegenheiten im Bürgerbüro vorab Termine zu vergeben. Dies dient neben der Verkürzung von Wartezeiten auch dem Datenschutz, da ein überfüllter Warteraum die Diskretion erschwert.

Wir haben Kommunen unterschiedlicher Größe in verschiedenen Regionen Niedersachsens besucht. Die Städte und Gemeinden, die auf Termin-

vergaben verzichten, haben größere Wartezonen, die von den Bearbeitungsbereichen getrennt sind. Des Weiteren war festzustellen, dass die Kommunen beim Neu- beziehungsweise Umbau von Räumlichkeiten die Anforderungen an ein datenschutzfreundliches Umfeld berücksichtigt haben. Der Aufruf erfolgte überwiegend über Aufrufnummern, die entweder bei der Terminvergabe übermittelt oder vor Ort vergeben werden.

Die aus unserer Sicht erforderlichen organisatorischen Maßnahmen haben die geprüften Kommunen getroffen, sodass die Gestaltung der Bürgerbüros aus datenschutzrechtlicher Sicht erfreulicherweise nicht zu beanstanden ist.

G.6.4 Ärger mit persönlich adressierter Wahlwerbung

Im Vorfeld von Wahlen erreichen uns regelmäßig Beschwerden zu persönlich adressierter Wahlwerbung. Die Angeschriebenen fragen sich, wie die Parteien die Anschriften erhalten haben. In einem Fall erhielten nicht wahlberechtigte Kinder und Jugendliche von einer Partei Post.

Im Vorfeld von Wahlen werben Parteien und Kandidaten für sich auf unterschiedlichen Wegen. An Wurfsendungen, die ohne persönliche Adresse in die Briefkästen eingeworfen werden, gibt es aus datenschutzrechtlicher Sicht nichts zu beanstanden.

Doch wie sieht es mit Anschreiben aus, die gezielt persönlich an mögliche Wählerinnen und Wähler adressiert werden? Diese Post richtet sich dann beispielsweise an alle Erstwähler. In solchen Fällen beschweren sich immer wieder Bürgerinnen und Bürger bei der Datenschutzaufsicht und wollen wissen, wie denn die Partei an ihre Adresse gekommen sei.

Rechtsgrundlage der Datenübermittlung

Parteien und Wählergruppen dürfen bei den Meldebörden im Vorfeld von Wahlen gezielt personenbezogene Daten von wahlberechtigten Personen abfragen. Für die Zusammensetzung der angefragten Gruppe muss das Alter maßgebend sein.[1]

Die Behörden dürfen Familienname, Vorname, etwaigen Doktorgrad und die derzeitige Anschrift mitteilen.[2] Die Weitergabe des Geburtsdatums ist dagegen nicht zulässig. Diese Auskünfte dürfen Parteien und Wählergruppen maximal sechs Monate vor einer Wahl anfordern und nur für Wahlwerbung nutzen. Spätestens einen Monat nach der Wahl sind die Daten zu löschen.

1 § 50 Abs. 1 BMG.
2 § 44 Abs. 1 BMG.

Wahlwerbung für Kinder und Jugendliche – Was ist passiert?

Eine Partei hatte im Vorfeld der Europawahl bei einer niedersächsischen Stadtverwaltung Meldedaten für die Gruppe der Erstwählerinnen und Erstwähler angefordert. Das Einwohnermeldeamt übermittelte Daten und die Partei versandte personalisierte Wahlwerbung. Die Briefe erreichten jedoch Kinder und Jugendliche, die nicht wahlberechtigt waren. In der Folge gingen bei uns Eingaben und Beschwerden sowie von der betroffenen Kommune eine Meldung über eine Datenschutzverletzung ein. Durch einen Eingabefehler bei der Auswahl der gewünschten Personengruppe erhielt die Partei die Namen und Anschriften der Kinder und Jugendlichen. Vor Versand der Wahlwerbung konnte der Fehler nicht mehr auffallen, da die Partei als Empfängerin der Meldedaten von korrekten Daten ausgehen musste – die Geburtsdaten der vermeintlich Wahlberechtigten hatte sie ja richtigerweise nicht erhalten.

Den gegen die Kommune gerichteten Beschwerden haben wir stattgegeben und eine Verwarnung ausgesprochen.

Keine Datenübermittlung gewünscht?

Bürgerinnen und Bürger können Melderegisterauskünften bei Wahlwerbung und in anderen besonderen Fällen[3] widersprechen.[4] Auf die Widerspruchsmöglichkeiten nach dem Bundesmeldegesetz weisen die Meldebehörden bei der Anmeldung und einmal jährlich durch ortsübliche Bekanntmachung hin. Viele Städte und Gemeinden halten in ihren Rathäusern entsprechende Formulare bereit. Die Widersprüche sind bei der Meldebehörde abzugeben. Vermehrt besteht auch die Möglichkeit, Widersprüche digital einzureichen.

Viele Kommunen halten Widerspruchsformulare bereit.

3 § 50 Abs. 1, 2 und 3 BMG.
4 § 50 Abs. 5 BMG.

G.6.5 Datenschutz an der Leine – Recht auf Löschung im Hunderegister

Im Hunderegister müssen Halter gemäß den Vorgaben des Niedersächsischen Hundegesetzes Informationen über ihr Tier angeben – dies kann auch online über ein Benutzerkonto erfolgen. Was aber, wenn die Halterin oder der Halter das eigene Nutzerkonto löschen will, der Hund aber registriert bleiben soll?

Im Berichtsjahr erreichte uns die Beschwerde eines Hundehalters. Er hatte zu seinem Tier die gesetzlich vorgeschriebenen Informationen an die verantwortliche Stelle, die das Register führt, übermittelt. Anstelle einer postalischen oder telefonischen Registrierung hatte er sich für den Anmeldeweg des digitalen Nutzerkontos entschieden.

Zu einem späteren Zeitpunkt forderte er die verantwortliche Stelle auf, sein digitales Nutzerkonto wieder zu löschen. Dies lehnte die Stelle mit der Begründung ab, dass man sein digitale Nutzerkonto nur dann löschen könne, wenn er nicht mehr Halter des Hundes sei, also wenn zugleich sämtliche Informationen über das Tier wegfallen könnten. Daraufhin wandte er sich mit einer Beschwerde an uns.

Unsere Prüfung hat ergeben, dass diese Vorgehensweise gegen das Recht auf Löschung[1] verstößt. Die Informationen über den Hund sind gesetzlich festgelegte Informationen, die der Halter an die registerführende Stelle übermitteln muss.[2] Hierfür kann aus drei Kommunikationswegen gewählt werden: schriftlich, telefonisch oder digital per Nutzerkonto. Auf dem schriftlichen und telefonischen Weg werden nur die gesetzlich festgelegten Pflichtinformationen, also keine zusätzlichen freiwilligen Daten, übermittelt. Für den digitalen Weg muss ein Nutzerkonto angelegt werden. Dafür müssen als Zugangsdaten eine E-Mail-Adresse angegeben und ein Passwort vergeben werden.

Die Verarbeitung dieser personenbezogenen Zugangsdaten ist nicht im Niedersächsischen Hundegesetz (NHundG) festgelegt und basiert daher

1 Art. 17 DSGVO.
2 § 6 NHundG.

auf der Einwilligung der Person, die ihren Hund anmelden möchte. Die Einwilligung kann jederzeit für die Zukunft widerrufen werden. Wenn die Person ihre Einwilligung widerruft, sieht die Datenschutz-Grundverordnung vor, dass die oder der Verantwortliche ihre personenbezogenen Daten löschen muss.[3]

Fazit

Nach unserem Hinweis hat die verantwortliche Stelle ihre Verfahrensweise und die Datenschutzerklärung auf der Webseite des Hunderegisters entsprechend angepasst. Der Fall zeigt, dass der eigentliche Inhalt einer verpflichtenden Anmeldung, hier die Registrierung eines Hundes, von dem freiwilligen Anmeldeweg des digitalen Nutzerkontos zu unterscheiden ist – beide Vorgänge sind datenschutzrechtlich unterschiedlich zu betrachten. Der Beschwerdeführer kann daher sein digitales Nutzerkonto löschen lassen – die Registrierung des Hundes bleibt davon unabhängig bestehen.

3 Art. 17 Abs. 1 Buchst. b DSGVO.

G.6.6 EuGH-Urteil: Datenschutzaufsichten auch für Parlamente zuständig

Am 16.01.2024[1] hat der Europäische Gerichtshof zu einem Fall aus Österreich entschieden, dass auch parlamentarische Tätigkeiten wie ein parlamentarischer Untersuchungsausschuss in den Anwendungsbereich der Datenschutz-Grundverordnung fallen und damit der Aufsicht der zuständigen Datenschutzbehörde unterliegen. Welche Auswirkungen ergeben sich aus diesem Grundsatzurteil für die Rechtslage in Niedersachsen?

Hintergrund des konkreten Falls war, dass vom österreichischen Parlament ein Untersuchungsausschuss eingesetzt worden war, um den Verdacht politischer Einflussnahme auf eine Staatsschutzbehörde zu untersuchen. Im Rahmen hiervon befragte der Ausschuss einen Polizeibeamten und legte nachfolgend dessen Identität offen, indem die vollständige Fassung des Befragungsprotokolls auf der Website des Untersuchungsausschusses veröffentlicht wurde. Die von dem Beamten hiergegen gerichtete Beschwerde wurde von der österreichischen Datenschutzbehörde mit der Begründung zurückgewiesen, keine Aufsichtszuständigkeit über die Tätigkeiten eines Organs eines Parlaments zu haben. Nachdem das österreichische Bundesverwaltungsgericht den Bescheid der Behörde aufgehoben hatte, weil die Datenschutz-Grundverordnung (DSGVO) aus Sicht des Gerichts keine Ausnahme für die Anwendbarkeit auf die Organe der Gesetzgebung vorsehe, legte der von der Behörde im Rahmen der Revision angerufene österreichische Verwaltungsgerichtshof den Fall dem Europäischen Gerichtshof (EuGH) vor.

Befassung des EuGH

Der EuGH nahm zunächst Bezug auf sein früheres Urteil aus dem Jahr 2020[2], mit dem er bereits die Geltung der DSGVO für einen parlamentarischen Petitionsausschuss bejaht hatte. Darauf aufbauend entschied der

1 Aktenzeichen C-33/22.

2 EuGH, Urteil vom 09.07.2020 – C-272/19, betreffend den Petitionsausschuss des Hessischen Landtages.

EuGH durch Auslegung der einschlägigen Bereichsausnahme[3], dass die DSGVO grundsätzlich auch für die Tätigkeit eines parlamentarischen Untersuchungsausschusses gelte, der vom Parlament eines Mitgliedsstaats in Ausübung seines Kontrollrechts gegenüber der Exekutive eingesetzt worden sei.

Im konkreten Fall sah der EuGH die vom parlamentarischen Untersuchungsausschuss durchgeführte Untersuchung des Verdachts politischer Einflussnahme auf eine Staatsschutzbehörde nicht als eine die nationale Sicherheit betreffende Tätigkeit an, welche außerhalb des Anwendungsbereichs des Unionsrechts liege.[4] Zugleich wies der EuGH darauf hin, dass ein parlamentarischer Untersuchungsausschuss im Rahmen seiner Tätigkeit durchaus Zugang zu personenbezogenen Daten haben könne, die aus Gründen der nationalen Sicherheit besonders zu schützen seien. Daher seien Beschränkungen einzelner Pflichten und Rechte aus der DSGVO im Wege von Gesetzgebungsmaßnahmen möglich.[5]

Anschließend wandte sich der EuGH der Frage nach der zuständigen Datenschutzaufsicht zu. Die DSGVO[6] würde den Mitgliedsstaaten einen Ermessensspielraum hinsichtlich der Anzahl der einzurichtenden Aufsichtsbehörden einräumen. Sofern im jeweiligen Zuständigkeitsgebiet jedoch nur eine Aufsichtsbehörde eingerichtet sei, folge aus der unmittelbaren Geltung der DSGVO[7], dass bei dieser Behörde zwangsläufig alle Zuständigkeiten lägen, die die DSGVO den Aufsichtsbehörden überträgt. Dieser Behörde sei dann – auch bei fehlender ausdrücklicher Aufsichtszuständigkeit – unmittelbar die Zuständigkeit übertragen, über Beschwerden zu einer Datenverarbeitung des parlamentarischen Untersuchungsausschusses zu entscheiden. Entgegenstehende nationale Regelungen seien aufgrund der unmittelbaren Geltung und des Vorrangs des Unionsrechts unbeachtlich. Dies gälte auch für nationale Regelungen mit Verfassungsrang. In dem ihm vorgelegten Fall entschied der EuGH daher, dass die DSGVO grundsätzlich anwendbar und die österreichische Datenschutzbehörde für die Bearbeitung der eingereichten Beschwerde zuständig sei.

3 Art. 2 Abs. 2 Buchst. a DSGVO und Art. 16 Vertrag über die Arbeitsweise der Europäischen Union (AEUV).
4 Vergleiche Erwägungsgrund 16 der DSGVO.
5 Art. 23 DSGVO
6 Art. 51 Abs. 1 DSGVO.
7 Art. 55 Abs. 1 DSGVO und Art. 77 Abs. 1 DSGVO.

Das Urteil des EuGH dürfte auch Auswirkungen auf die Rechtslage in Niedersachsen haben. Derzeit sieht das Landesrecht vor, dass die Vorschriften des ersten Teils des Niedersächsisches Datenschutzgesetzes (NDSG) für den Landtag, seine Mitglieder, die Fraktionen sowie ihre jeweiligen Verwaltungen und Beschäftigten nur gelten, soweit sie Verwaltungsaufgaben wahrnehmen.[8] Dementsprechend sieht die Datenschutzordnung des Niedersächsischen Landtags (DO LT) vor, dass sie für die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben des Landtages[9] anstelle des NDSG anzuwenden ist.[10] Hierzu hat der Landtag eine Datenschutzkommission gebildet[11], welche die Einhaltung der Vorschriften seiner Datenschutzordnung sowie anderer Rechtsvorschriften überwacht, Beschwerden entgegennimmt und das Präsidium und die Landtagspräsidentin über festgestellte Verstöße unterrichtet.[12]

Fazit

Mit Blick auf das genannte EuGH-Urteil sind Zweifel angebracht, ob diese zeitlich früher geschaffene Rechtslage noch uneingeschränkt Geltung beanspruchen kann.

Zum einen ist die DSGVO jedenfalls grundsätzlich auf die Arbeit von parlamentarischen Petitionsausschüssen und parlamentarischen Untersuchungsausschüssen, deren Tätigkeit nicht der Wahrung der nationalen Sicherheit dient, anwendbar. Darüber hinaus könnte das Urteil aufgrund der vom EuGH vorgenommenen engen Auslegung der genannten Bereichsausnahme[13] möglicherweise auch auf andere Bereiche der parlamentarischen Tätigkeit übertragbar sein.

Zum anderen ist für das Land Niedersachsen der Landesbeauftragte für den Datenschutz „einzige" Aufsichtsbehörde.[14] Das hat zur Folge, dass nach den Ausführungen des EuGH jedenfalls für parlamentarische Petitions- und Untersuchungsausschüsse grundsätzlich unsere Behörde zustän-

8 § 1 Abs. 3 NDSG.
9 Durch seine Gremien, seine Mitglieder, die Fraktionen und deren Beschäftigte sowie durch die Landtagsverwaltung einschließlich des Gesetzgebungs- und Beratungsdienstes.
10 § 1 Abs. 1 DO LT.
11 § 12 DO LT.
12 § 13 DO LT.
13 Art. 2 Abs. 2 Buchst. a DSGVO.
14 Art. 62 Niedersächsische Verfassung und § 18 NDSG.

dige Aufsichtsbehörde wäre und nicht die Datenschutzkommission des Landtages.

Daraus folgt, dass sich unsere Behörde beispielsweise mit Beschwerden von betroffenen Personen bezüglich der Verarbeitung ihrer personenbezogenen Daten im parlamentarischen Bereich befassen und soweit erforderlich gegebenenfalls von ihren Untersuchungs- und Abhilfebefugnissen Gebrauch machen könnte.[15]

Es bliebe dem Landtag unbenommen, die Aufsichtszuständigkeit in Niedersachsen im parlamentarischen Raum abweichend gesetzlich zu regeln. Hierzu könnte der niedersächsische Gesetzgeber eine andere unabhängige und weisungsfreie Aufsichtsbehörde vorsehen und diese mit besonderen Aufsichtszuständigkeiten betrauen. Tut er dies nicht, liegt die Aufsicht über das Parlament in Gänze beim Landesbeauftragten für den Datenschutz.

15 Art. 7 DSGVO.

Schule und Hochschule

G.7.1 Chancen für den digitalen Datenschutz an Schulen

Der Bund fördert die Digitalisierung der Schulen mit finanziellen Mitteln auch für Projekte des Medieninstituts der Länder. Der Datenschutz muss in diesen Projekten immer mit- und zu Ende gedacht werden, um die Schulen wirklich zu entlasten.

Schulen nutzen bereits heute vielfältige digitale Bildungsmedien. Dabei ist es aber noch von der Personalstärke der Schule und der IT-Affinität der Lehrkräfte abhängig, inwieweit der Bildungsauftrag datenschutzkonform über und mit digitalen Angeboten erfüllt wird. Um diesen Zustand zu verbessern, fördert der Bund die Projekte „Vermittlungsdienst für das digitale Identitätsmanagement in Schulen" (VIDIS) und eduCheck digital des Medieninstituts der Länder (FWU)[1] sowie das Forschungsprojekt Data Protection Certification for Educational Information Systems (DIRECTIONS) des Karlsruher Institut für Technologie (KIT), der Universität Kassel, der datenschutz cert GmbH und dem Kompetenznetzwerk Trusted Cloud e. V.[2]

Zusammen mit dem Arbeitskreis Schule und Bildungseinrichtungen der Datenschutzkonferenz (DSK), dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder, begleiteten wir im Berichtsjahr die beiden FWU-Projekte.

VIDIS und eduCheck digital

Das FWU entwickelte auf der ersten Projektstufe einen digitalen Identitätsdienst. Schülerinnen und Schüler können über ein durch die FWU er-

1 FWU Institut für Film und Bild in Wissenschaft und Unterricht gemeinnützige GmbH.
2 Vgl. hierzu bereits 28. Tätigkeitsbericht 2022 der LfD, S. 142.

stelltes Pseudonym Angebote von Bildungsverlagen mittels einer einheitlichen digitalen Identität nutzen. Als zweite Projektstufe wurde sodann eine kursorische datenschutzrechtliche Vorprüfung konzipiert. Die genaue Abgrenzung zum Projekt eduCheck digital ist unklar. Das FWU führt dazu sinngemäß aus, dass im Gegensatz zu VIDIS bei eduCheck digital die Begutachtung von digitalen Bildungsmedien nicht „Mittel zum Zweck" ist, sondern den „Kern des Projekts" bildet.[3]

In Niedersachsen wurde im Berichtsjahr weder VIDIS noch eduCheck digital eingeführt, unter anderem, weil nicht geklärt wurde, welche Stelle im Land die Datenschutzkonformität der Bildungsangebote abschließend prüft.

Das FWU nimmt nur eine datenschutzrechtliche Vorprüfung der Angebote vor. Die Bildungsmedienanbieter erteilen eine Selbstauskunft anhand eines Fragenkatalogs, die kursorisch auf Schlüssigkeit von einem vom FWU beauftragten Dienstleiter geprüft wird. Das ist für sich schon einiges wert, unter anderem wird so verhindert, dass die Bildungsanbieter Werbetracking mittels Cookies betreiben. Lückenhaft ist hingegen die Konzeption und Prüfung von Datenschutzfolgenabschätzungen.

Eine Abschlussprüfung digitaler Bildungsangebote sollte nicht auf die Schulen abgewälzt werden.

Aus unserer Sicht sollte eine Abschlussprüfung nicht auf die Schulen abgewälzt werden, weil sie gerade im Bereich des digitalen Datenschutzes entlastet werden sollten. Zudem erscheint auch nicht sinnvoll, dass das FWU 16 Landesschulgesetze prüft. Daher setzten wir uns gegenüber dem Kultusministerium dafür ein, dass eine zentrale Stelle des Landes die Abschlussprüfung für alle Schulen durchführt. Wir werden weiter über die Ergebnisse dieses Vorhabens und die Gespräche mit dem Kultusministerium berichten.

Ausblick

Wir begrüßen die hier vorgestellten Projekte, weil sie Schulen in allen 16 Bundesländern gleichermaßen bei der Erfüllung des digitalen Bildungsauftrages unterstützen. Allerdings ist die Schulbildung Ländersache und dem folgt als Annex auch die strategische Gesamtverantwortung des Kultusministeriums hinsichtlich datenschutzrechtlicher Vorgaben.

3 Vgl. https://t1p.de/educheck (Kurzlink).

G.7.2 Einsatz von „Künstlicher Intelligenz“ an niedersächsischen Schulen?

Im Berichtsjahr prüften wir den Einsatz von adaptiven Tutorensystemen an niedersächsischen Schulen, die in der öffentlichen Diskussion und Werbung der Anbieter dem Bereich der Künstlichen Intelligenz zugerechnet werden. Wir stellten insbesondere fest, dass die Anbieter den Betroffenen die Datenverarbeitung nicht transparent erklärte.

Die Anbieter adaptiver („anpassungsfähiger“) Tutorensysteme versprechen eine neue Form des individualisierten Lernens. Tutorensysteme erfassen den Lernstand von Schülerinnen und Schülern, indem sie deren Antworten auf Aufgaben analysieren. Je nach Stärken und Schwächen erstellen Tutorensysteme dem jeweiligen Wissensstand angepasste Aufgaben. In Niedersachsen hat das Kultusministerium zum Beispiel die Anwendung bettermarks der gleichnamigen GmbH lizenziert, mit der Schulen die mathematischen Kenntnisse der Schülerinnen und Schüler prüfen und erweitern. Ein weiteres in Niedersachsen eingesetztes System ist die Online-Diagnose des Westermann-Verlags, die Schülerinnen und Schüler auch in den Fächern Deutsch und Englisch fördert.

KI-Systeme vs. adaptive Tutorensysteme

Die Prüfung ergab, dass die untersuchten Tutorensysteme bettermarks und Westermann OnlineDiagnose aktuell keine KI-Systeme im Sinne der KI-Verordnung[1] sind. Der zwölfte Erwägungsgrund der KI-Verordnung macht deutlich, dass Anwendungen, die auf ausschließlich von Menschen definierten Regeln beruhen, nicht den Vorgaben der KI-Verordnung unterliegen. Es reicht daher nicht aus, dass ein IT-System menschenähnliche Verhaltensweisen zeigt. Wenn zum Beispiel ein Chatbot eines Internetshops auf Fragen eines Interessenten nach Signalwörtern sucht, um ihm mit einem vom Webshop-Betreiber vorformulierten Textbaustein zu

1 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz.

antworten, dann ahmt auch dieser Chatbot menschliche Kommunikation nach. Ein solcher Chatbot ist aber kein KI-System im Sinn der KI-Verordnung. Vielmehr erlernen KI-Systeme ihre Regeln eigenständig; sie haben die Fähigkeit, aus Eingaben oder Trainingsdaten Entscheidungen autonom abzuleiten. Diese Fähigkeit erlernen KI-Systeme, indem Anbieter sie mit Methoden des maschinellen Lernens entwickeln.

Im Fall von Tutorensystemen wie bettermarks hinterlegen Anbieter typische Fehlermuster von Schülerinnen und Schüler in der Programmstruktur. Wenn eine Schülerin oder ein Schüler eine Aufgabe falsch löst und der Fehler in der Programmstruktur hinterlegt ist, werden ihr oder ihm die vom Anbieter definierten Aufgaben vorgeschlagen. Sofern ein Fehler nicht im System hinterlegt ist, passen die Programme ihre Programmstruktur nicht autonom an. Vielmehr muss der Anbieter den neuen Fehler erst in das Programm einpflegen.

In der öffentlichen Diskussion werden adaptive Tutorensysteme teilweise mit KI-Systemen gleichgesetzt, was im Fall der untersuchten Anwendungen zumindest ungenau ist.

Datenschutzrechtlicher Rahmen

Das Datenschutzrecht bildet technologieneutrale Rahmenbedingungen ab, die unabhängig von der Funktionalität eines Programms zu beachten sind. Verantwortliche sollten sich daher im Ausgangspunkt fragen, welche personenbezogene Daten von Schülerinnen und Schüler absolut notwendig sind, um den Zweck der Datenverarbeitung zu erreichen. Sofern wie regelmäßig ein Dienstleister die Software über eine Cloud-Umgebung bereitstellt, hilft ein Blick in den Lizenzvertrag und den Auftragsverarbeitungsvertrag. Die dort hinterlegten personenbezogenen Daten und deren Verarbeitungszwecke sind abzugleichen mit der gesetzlichen Rechtsgrundlage der Datenverarbeitung.[2] Eine Einwilligung kommt für die Verarbeitung von personenbezogenen Daten zu pädagogischen Zwecken nicht in Betracht. Aufmerksam müssen Schulen werden, wenn sich ein Dienstleister vorbehält, personenbezogene Daten der Schülerinnen und Schüler zum Beispiel für Werbung zu eigenen Zwecken zu verarbeiten.[3] Dies wäre nicht

2 § 31 des NSchG.

3 Die untersuchten Anwendungen gaben keine Anlass zur Beanstandung in dieser Hinsicht.

zulässig, war aber bei den geprüften Tutorensystemen auch nicht zu beanstanden.

Sofern Schulen die Datenverarbeitung auf die gesetzliche Rechtsgrundlage stützen können und den Dienstleister beauftragen wollen, ist ein Auftragsverarbeitungsvertrag abzuschließen.[4] Neben den wichtigen Zwecken der Datenverarbeitung sollte die Liste der sogenannten Unterauftragsverarbeiter geprüft werden. Denn auch Dienstleister nutzen ihrerseits Sub-Dienstleister, die ihren Sitz in einem Drittland außerhalb der Europäischen Union haben könnten, was Fragen des internationalen Datenverkehrs aufwirft.[5]

Sofern eine Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Schülerinnen und Schüler verursacht, ist zudem eine Datenschutzfolgenabschätzung durchzuführen.

Zwar unterstützen die Dienstleister die Schulen mit Auftrags-Mustern und Mustern zu Datenschutzfolgenabschätzungen. Allerdings haben Schulen und nicht die Dienstleister als Verantwortliche sicherzustellen, dass die Datenverarbeitung den datenschutzrechtlichen Rahmen einhält.

Sodann ist die Datenschutzdokumentation zu vervollständigen (Eintrag in das Verzeichnis der Verarbeitungstätigkeiten, Erstellen von Datenschutzinformationen für Schülerinnen und Schüler sowie Lehrkräfte, Löschkonzept, Rechte und Rollenkonzept).[6]

Besonderheiten bei adaptiven Tutorensystemen

Bei adaptiven Tutorensystemen sind mehrere Besonderheiten zu beachten, auf die wir die Schulen hingewiesen haben. Bei der Bildung von Lernstandsprofilen liegt es auf der Hand, dass der Anbieter und die Lehrkräfte die Lernentwicklungskurve von Schülerinnen und Schülern mit der Zeit detailliert in Form von Lernstandsprofilen nachvollziehen können. Schulen müssen Schülerinnen und Schüler sowie Eltern informieren, dass Tutorensysteme individuelle Lernstandsprofile in dem jeweiligen Fach erstellen. Zudem müssen in Grundzügen der Programmablauf und die Tragweite und

4 Art. 28 DSGVO.

5 Art. 44 ff. DSGVO; Die untersuchten Anwendungen gaben keine Anlass zur Beanstandung in dieser Hinsicht.

6 Ein Deutschlehrer benötigt keinen Zugriff auf die Lernstandsprofile von Schülerinnen und Schülerin, die im Fach Mathematik entstanden sind.

Auswirkungen der Programmentscheidungen erklärt werden (z. B. ob die Lernstandsprofile Auswirkungen auf die Leistungsbewertung haben).[7]

Tutorensysteme erstellen individuelle Lernstandsprofile.

Die Datenschutz-Grundverordnung (DSGVO) enthält eine Regelung[8], dass Personen beziehungsweise in diesem Fall Schülerinnen und Schüler keiner ausschließlichen Entscheidungsgewalt einer Software unterworfen werden dürfen, die zu einer rechtlichen Wirkung oder einer ähnlichen Beeinträchtigung führt. Es wäre zum Beispiel mit dieser Regelung nicht zu vereinbaren, wenn Lehrkräfte eine Zeugnisnote ausschließlich auf Basis des Lernstandsprofils einer Schülerin oder eines Schülers, das ein Tutorensystem gebildet hat, vergeben.

Fazit

Die festgestellten Mängel haben wir dem Kultusministerium, den Regionalen Landesämtern für Schulen und Bildung und den Schulen mitgeteilt. Wir gehen davon aus, dass die Mängel zeitnah abgestellt werden.

7 Art. 4 Abs. Nr. 4 i. V. m. Art. 5 Abs. 1 Buchst. a i. V. m. Art. 13 Abs. 2 Buchst. f DSGVO.
8 Art. 22 DSGVO.

G.7.3 Datenschutzaspekte beim Einsatz privat finanzierter Tablets an Schulen

In niedersächsischen weiterführenden Schulen wird kurz- bis mittelfristig auf elternfinanzierte Tablets als Lernmittel gesetzt. Aus Sicht des Datenschutzes sollte die Landesregierung weiterhin anstreben, landeseigene Tablets für Schulen anzuschaffen.

Im Berichtsjahr kündigte das Niedersächsische Kultusministerium an, anders als ursprünglich im Koalitionsvertrag zur aktuellen 19. Wahlperiode zwischen SPD und Bündnis 90/Die Grünen vorgesehen, keine schulischen Tablets für Schülerinnen und Schüler zu finanzieren. Aus Sicht des Datenschutzes aber wären die eigentlich versprochenen Schulgeräte der risikoärmste Weg gewesen, um Schülerinnen und Schüler mittels Tablets zu unterrichten. Wir sprechen uns daher weiter dafür aus, alle Schülerinnen und Schüler mit landeseigenen Tablets auszustatten, soweit der Bildungsauftrag den Einsatz solcher Geräte erfordert.

Sorgen und Beschwerden der Eltern

Bei unserer Behörde drückten Eltern ihre Sorgen in Form von einigen Beschwerden aus. Sie monierten einerseits den Preis der Endgeräte, zumal die Schulen den Einsatz besonders teurer Modelle vorgaben. Andererseits zweifelten sie an dem Versprechen der Schulen, Kindern digitale Kompetenzen in gleichwertiger Art und Weise auch mit analogen Lernmaterialien vermitteln zu können, sollten Erziehungsberechtigte sich entscheiden, keine Tablets anzuschaffen.

Im Hinblick auf den Datenschutz hinterfragten sie kritisch, dass schulische Administratoren vollen Zugriff auf die Tablets erhielten, um die für den Schulbetrieb notwendigen Anwendungen zu installieren. Die schulischen Administratoren können durch den Zugang per sogenanntem Mobile Device Management (MDM) sehen, welche Anwendungen Schülerinnen und Schüler nutzen. Dies löst bei den besorgten Eltern ein Gefühl des Überwachtseins aus, das man aus dem analogen Schulbetrieb jedenfalls so bis-

In vielen niedersächsischen Schulen müssen Eltern die Schultablets privat finanzieren – aus Sicht des Datenschutzes ist das nicht ideal.

lang nicht kannte. In den von uns entschiedenen Fällen waren die Sorgen der Eltern aus Sicht des Datenschutzes aber unbegründet.

Der Datenschutz als Multifunktionswerkzeug?

Das Datenschutzrecht und unsere damit begründete Zuständigkeit löst leider nicht alle Probleme, die mit der Einführung von elternfinanzierten Tablets einhergehen. Fragen der Finanzierung und insbesondere zu einer Verpflichtung der Eltern, ihre Kinder mit Tablets auszustatten[1], beantwortet das Datenschutzrecht nicht. Ebenso wenig können wir als Datenschutzaufsicht bei medienpädagogischen Problemstellungen rund um den Einsatz digitaler Schulgeräte beraten.

Das Datenschutzrecht versucht hier, die Spannungslage zwischen dem schulischen Bildungsauftrag[2] und dem Recht auf informationelle Selbstbestimmung der Schülerinnen und Schüler aufzulösen, nicht mehr und nicht weniger.

Digitaler Bildungsauftrag der Schulen

Einzelne Beschwerdeführer rügten, dass die für die Einbindung der Tablets in den Schulbetrieb erforderliche Erhebung eines Nutzernamens der Schülerinnen und Schüler sowie die Speicherung von Daten, die bei der

1 § 71 NSchulG.
2 § 2 NSchulG.

Nutzung der Tablets und einzelner Anwendungen entstehen[3], auf eine Einwilligung gestützt werden. Eine Einwilligung zur Datenverarbeitung zu pädagogischen Zwecken kam aber aufgrund des Über- Unterordnungsverhältnisses zwischen Schulen und Schülerinnen sowie Schülern nicht in Betracht.[4]

Tabletklassen waren nunmehr im Regelbetrieb des Schulunterrichts angekommen. Die Auffassung der Schulen, Lehrkräfte würden Schülerinnen und Schüler mit analogen Materialien in vergleichbarer Weise unterrichten, wenn keine Einwilligung erteilt wurde, war insbesondere in einem Fall nicht haltbar: Eine Schule erteilte den Eltern den Hinweis, Schülerinnen und Schüler könnten ja einfach die Schule wechseln, wenn sie die Datenverarbeitung nicht akzeptierten. Deutlicher hätte die Schule das bestehende Über-/Unterordnungsverhältnis zwischen Schule und Betroffenen nicht ausdrücken können.

Das Niedersächsische Schulgesetz sieht grundsätzlich den Einsatz von digitalen Lernmitteln und die damit einhergehende Datenverarbeitung vor.[5] Das gilt auch für Tablets, denn sie sind als digitale Lernmittel anzusehen, weil Schülerinnen und Schüler sie für die Vor- und Nachbereitung sowie für die Durchführung des Unterrichts verwenden.

Vorausgesetzt, es wurden die erforderlichen Auftragsverarbeitungsverträge mit dem Schulträger und weiteren einbezogenen Dienstleistern abgeschlossen, war die Verarbeitung personenbezogener Daten der Schülerinnen und Schüler zur Erfüllung des digitalen Bildungsauftrages der Schulen zulässig.

Technisch-organisatorische Rahmenbedingungen

Unter engen technisch-organisatorischen Rahmenbedingungen können Schulen auch elternfinanzierte Tablets im Unterricht einsetzen. Neben einer ordnungsgemäßen Datenschutzinformation[6] der Eltern und Datenschutzdokumentation[7] der Schule müssen schulische Administratoren

3 Sogenannte Metadaten.
4 ErwGr. 43 der DSGVO.
5 § 31 Abs. 5 NSchG.
6 Art. 13 DSGVO.
7 Art. 30, 35 DSGVO.

auch auf die aus privaten Mitteln finanzierten Tablets zugreifen können. Nur dann sind Schulen in der Lage, die Gewährleistungsziele der Datenschutz-Grundverordnung in einem vertretbaren Umfang zu erreichen.

Allerdings ist dabei festzustellen, dass insbesondere die Gewährleistungsziele der Verfügbarkeit, Integrität und Vertraulichkeit mit elternfinanzierten Tablets tatsächlich nur in einem „vertretbaren Umfang" zu erreichen sind. Denn Schulen verarbeiten personenbezogene Daten von Minderjährigen mittels Tablets in einem großen Umfang. Die Schülerinnen und Schüler erhalten Zugang zum Schulnetzwerk, gegebenenfalls zur Niedersächsischen Bildungscloud, IServ und anderen Lernplattformen. Auf den Lernplattformen versammeln sich personenbezogene Daten von Schülerinnen und Schülern sowie Lehrkräften aus ganz Niedersachsen.[8] Jedes elternfinanzierte und nicht fachgerecht administrierte Tablet ist – auch ohne Wissen von Schülerinnen, Schülern und Eltern – ein potenzielles Eintrittstor für Kriminelle, um mittels Schadsoftware das Schulnetz und die digitalen Lernplattformen zu infiltrieren. Ein Datenleck könnte potenziell eine große Zahl minderjähriger Schülerinnen und Schüler sowie deren Lehrkräfte betreffen.

Der Bildungsauftrag von Schulen darf nicht gegenüber dem Datenschutz ausgespielt werden.

Um diesen Risiken bestmöglich entgegenzutreten, wäre daher die Anschaffung von länderfinanzierten Schultablets angemessen. Die Risiken sind auch der Grund, warum Schulen oder eine zentralen Stelle des Landes entscheiden muss, welche Anwendungen sie auf den elternfinanzierten Tablets installieren. Schülerinnen und Schüler hingegen dürfen nur solche Anwendungen nutzen, die mittels einer entsprechenden Administratorenumgebung freigegeben werden.

Daneben halten schulische Administratoren diese Anwendungen auch mit Updates auf dem aktuellsten Stand der Technik, um das Risiko der Datenverarbeitung auf niedrigem Niveau zu halten.[9]

8 Allein im Schuljahr 2024/25 wurden in Niedersachsen 881.745 Schülerinnen und Schüler in Allgemeinbildenden Schulen und 220.000 Schülerinnen und Schüler in Berufsbildenden Schulen beschult.

9 Diese und weitere Pflichten ergeben sich auch aus den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (Mindeststandard des BSI für Mobile Device Management nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 05.09.2022).

Ausblick

Der Bildungsauftrag von Schulen darf nicht gegenüber dem Datenschutz ausgespielt werden. Es muss das Ziel sein, sowohl das Recht auf informationelle Selbstbestimmung sicherzustellen, als auch dem öffentlichen Bildungsauftrag wirksam nachzukommen.

Für die Praxis und das weitere Vorgehen bedeutet dies, dass nicht einzelne schulische Administratoren entscheiden sollten, welche Anwendungen sie auf den Tablets installieren. Vielmehr werden wir in gemeinsamen Gesprächen mit dem Kultusministerium auf einheitliche Leitlinien hinwirken.

Hochschule versüßt Teilnahme an wissenschaftlicher Studie mit Leistungspunkten G.7.4

Eine Hochschule vergab im Berichtsjahr Leistungspunkte an Lehramts-Studierende für die Teilnahme an zwei Umfragen, um die Qualität von externen Praktika zu erforschen. Die auf eine Einwilligung gestützte Datenverarbeitung war rechtswidrig.

Studierende durchlaufen im Verlauf ihres Studiums vielfältige Praktika, die mal mehr und mal weniger lehrreich sind. In einem Fall wollte eine niedersächsische Hochschule erforschen, was gute Praktika von schlechten Praktika unterscheidet. Um die Studierenden zu motivieren, jeweils zu Beginn und am Ende des Praktikums an einer Umfrage teilzunehmen, entschied sich die Hochschule, den Aufwand der Studierenden mit zwei Leistungspunkten zu versüßen. Ein Studierender beschwerte sich bei uns, woraufhin wir die Hochschule anhörten.

Nach Auffassung der Hochschule war die auf eine Einwilligung gestützte Datenverarbeitung nicht zu beanstanden. Sie führte aus, dass Studierende freiwillig entscheiden konnten, ob sie an der Studie teilnehmen. Nach Ansicht der Hochschule war es ausgeschlossen, dass Studierende spürbare Nachteile erleiden, wenn sie ihre Einwilligung zur Datenverarbeitung nicht erteilen. Studierende hätten die Bestnote auch ohne Teilnahme an der Studie erreichen können. Zudem sei durch ein Zugangsschlüssel-Verfahren sichergestellt, dass die prüfenden Professoren die Leistung der Studierenden im Übrigen unbeeinflusst von einer (Nicht-)Teilnahme an der Studie bewertet haben.

Leistungspunkte hätten über Bestehen entscheiden können.

Fehlende Leistungspunkte

Dabei übersah die Hochschule, dass Studierenden zwei Leistungspunkte im Prüfungsportfolio fehlten, wenn sie die Umfragebögen nicht ausgefüllt haben. Es mag daher Fälle geben, in denen gerade diese zwei Leistungspunkte über das Bestehen oder das Nichtbestehen des Prüfungsportfolios entscheiden. Zwar hat es solch einen Fall nach Auskunft der Hoch-

schule (noch) nicht gegeben, aber es durfte nicht übersehen werden, dass eine Prüfungswiederholung ein großer Nachteil für Studierende wäre. Die Hochschule sah ihren Fehler ein, löschte bereits erhobene Datensätze und stützte die Datenverarbeitung fortan nicht mehr auf eine Einwilligung.

Die neue Argumentation der Hochschule, sich nunmehr auf eine gesetzliche Rechtsgrundlage[1] zu berufen, womit die Hochschule die Studierenden sinngemäß auch verpflichten wollte, an den Umfragen teilzunehmen, wurde hingegen von uns verworfen: Ein Gesetz, das eine bestimmte Verarbeitung personenbezogener Daten erlaubt, begründet grundsätzlich keine Auskunftspflicht. Daher durfte die Hochschule die Studierenden auch nicht verpflichten, an der Studie teilzunehmen. Das Verfahren wurde mit einem Hinweis auf diese Rechtslage und einer Verwarnung beendet.

1 § 13 NDSG.

Innere Sicherheit und Justiz

Telekommunikationsüberwachung: Gemeinsames Zentrum im Nordverbund startet nach DSFA-Prüfung G.8.1

Die Beratungsphase unserer Behörde für das geplante neue Verfahren zur Telekommunikationsüberwachung in Norddeutschland setzte sich auch 2024 fort und fand nach intensiver Arbeit ihren Abschluss.

Im Dezember 2024 nahm das neue Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung[1] (RDZ-TKÜ) der Polizei im Verbund der norddeutschen Küstenländer einen ersten Teil-Betrieb auf. Im Laufe der mehr als 10-jährigen Planungs- und Errichtungsphase waren wir kontinuierlich beratend an der Umsetzung der datenschutzrechtlichen Anforderungen beteiligt.

Dreh- und Angelpunkt für die Beurteilung unsererseits waren technische Dokumentationen und weitere Unterlagen, sowie speziell die Datenschutz-Folgenabschätzung (DSFA). Eine DSFA ist insbesondere dann im Rahmen der datenschutzrechtlichen Dokumentationspflichten zu erstellen, wenn eine Verarbeitungstätigkeit ein „voraussichtlich hohes Risiko für die Rechte und Freiheiten betroffener Personen" in sich birgt. Dies ist im Fall von strafprozessualen TKÜ-Maßnahmen hinsichtlich der Verarbeitung personenbezogener Daten und bei TKÜ-Maßnahmen nach dem Gefahrenabwehrrecht gemäß Landesrecht[2] gegeben.

1 TKÜ-Maßnahmen gründen sich im Gefahrenabwehrrecht auf § 33a NPOG und im Strafprozessrecht auf Anordnungen gemäß § 100a Abs. 1 StPO, vgl. Statistik beim Bundesamt für Justiz, https://t1p.de/tkueberwachung (Kurzlink).

2 Im Beispielfall der Polizei Niedersachsens gemäß § 49 NPOG in Verbindung mit § 23 und § 39 NDSG.

Eine DSFA stellt eine systematische Risikoanalyse dar und dokumentiert die getroffenen angemessenen technischen und organisatorischen Sicherungsmaßnahmen um die Risiken weitestmöglich zu reduzieren. Sie ist vor dem Produktivstart einer Anwendung fertigzustellen.

Am 29. Februar 2024 legte die im Landeskriminalamt (LKA) Niedersachsen eingerichtete Projektgruppe der Polizeien der fünf Trägerländer den zuständigen Aufsichtsbehörden eine DSFA für das geplante RDZ-TKÜ-Verfahren vor. Die Gruppe der zuständigen Aufsichtsbehörden prüfte diese daraufhin auf Vollständigkeit, Systematik und Konsistenz, um so die Datenschutzkonformität des Produktiveinsatzes der TKÜ-Verfahren beurteilen zu können.

Die Datenschutzaufsicht Niedersachsen war hierbei die Koordinationsstelle für die Bewertung des technisch-organisatorischen Datenschutzes, während das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein[3] die Koordination für die Bewertung der materiell-datenschutzrechtlichen Aspekte verantwortete.

Die Bedeutung dieser intensiven Befassung ergab sich bereits aus dem hohen Schutzbedarf aufgrund der durchweg besonders ausgeprägten grundrechtlichen Eingriffstiefe bei allen TKÜ-Maßnahmen. Zudem erforderte die Komplexität aufgrund der in den fünf Bundesländern gegebenenfalls uneinheitlichen Anforderungen des landesspezifischen Gefahrenabwehrrechtes unter Umständen Anpassungen im Verfahren.

Hinweise zu Nachbesserungsbedarf bei der DSFA

In einer gemeinsamen Stellungnahme vom September 2024 haben die Datenschutzbehörden der Projektgruppe darauf hingewiesen, dass bezüglich der dokumentierten Rechtsgrundlagen und in der Systematik der Risikobewertung der DSFA Nachbesserungen erforderlich waren. Hieraus ergab sich für die Verantwortlichen die Notwendigkeit, erneut zu prüfen, ob die aus der Risikobewertung abgeleiteten technisch-organisatorischen Maßnahmen (TOM) auf der neuen Grundlage noch als ausreichend und angemessen gelten können. Daher war die DSFA von der Projektgruppe nochmals zu überarbeiten.

3 Datenschutzaufsichtsbehörde des Landes Schleswig-Holstein.

Darüber hinaus empfehlen die Datenschutzaufsichtsbehörden die Einrichtung einer dauerhaft arbeitenden Organisationseinheit für Datenschutz, die die ergriffenen technischen Maßnahmen und den Reifegrad der Umsetzung regelmäßig wiederkehrend evaluiert. Dabei müssen insbesondere die IT-Architektur, die Prozesse und Verarbeitungsschritte, die Datenstrukturen und die Standards auditiert werden. Fortlaufend sind die rechtlichen und technischen Entwicklungen zu beobachten und zu bewerten, um auf neue Anforderungen zeitnah adäquat reagieren zu können.

Produktivstart Ende 2024

Im Dezember 2024 hat schließlich das RDZ-TKÜ seinen Teil-Betrieb aufgenommen. Wir gehen davon aus, dass unsere Hinweise zur Verbesserung des Datenschutzmanagements und der Erfüllung der Dokumentationspflichten für das neue TKÜ-System noch vor dem Produktivstart umgesetzt worden sind. Eine diesbezügliche Verlautbarung des LKA-Präsidenten deutet dies an[4], konnte allerdings von uns im Berichtszeitraum nicht verifiziert werden.

Fazit

Nach vielen Jahren des Ringens um eine TKÜ-Anlage, die dem Stand der Technik entspricht und zeitgemäße Ermittlungsmöglichkeiten bietet, ist nun ein wichtiger Teilschritt erreicht. In den kommenden Monaten soll schrittweise die Anbindung der anderen Länder erfolgen und planmäßig bis Mitte 2025 abgeschlossen sein. Das unter erheblichen datenschutzrechtlichen Mängeln betriebene Altsystem ist damit Vergangenheit.

Die langjährige und intensive Beratung der Datenschutzaufsicht Niedersachsen in der Begleitung des gesamten Planungs- und Realisierungsprozesses war fruchtbar und hat sich nicht nur aus unserer Sicht gelohnt. Der Präsident des LKA Niedersachsen stellte zum Start der neuen Anlage fest: „Die intensiven Befassungen in diesen Themenkomplexen [Anm. d. Red.: IT-Sicherheit und Datenschutz] waren eine lohnenswerte Investition." Auf dieser Basis gehen wir davon aus, dass das LKA die von uns in diesem Jahr eingebrachten Nachbesserungserfordernisse vollständig umgesetzt

4 Pressemitteilung des Niedersächsischen Innenministeriums vom 17.12.2024: https://www.mi.niedersachsen.de/238167.html

hat und das hierbei höchstmögliche Datenschutzniveau durch regelmäßige Neubewertungen über den gesamten Lebenszyklus der TKÜ-Verfahren hinweg sichergestellt wird.

Prüfung des Niedersächsischen Verfassungsschutzes abgeschlossen G.8.2

Im Jahr 2024 haben wir beim Niedersächsischen Verfassungsschutz die Verarbeitung von personenbezogenen Daten überprüft und nachfolgend unsere Prüfungserkenntnisse dem Verfassungsschutz zur Verfügung gestellt.

Der Landesbeauftragte für den Datenschutz hat beim Niedersächsischen Verfassungsschutz die Einhaltung der gesetzlichen Vorschriften über die Verarbeitung personenbezogener Daten zu kontrollieren. Nach dem Niedersächsischen Verfassungsschutzgesetz ist sogar eine verpflichtende Prüfung bei personenbezogenen Daten, die mit Mitteln des Nachrichtendienstes erhoben wurden, im Abstand von höchstens zwei Jahren vorgesehen.[1]

Diese uns durch den Gesetzgeber auferlegte Prüfungspflicht haben wir im Berichtszeitraum erfüllt. Schwerpunkt war die Einhaltung der gesetzlichen Vorschriften über die Verarbeitung von personenbezogenen Daten, die mit einem der gesetzlich vorgesehenen nachrichtendienstlichen Mittel erhoben und verarbeitet wurden.[2] In der detaillierten Prüfung haben wir entsprechende Datensätze auf eine rechtmäßige Verarbeitung überprüft. Die Verfassungsschutzbehörde hat unsere Prüfung in fachlicher und organisatorischer Hinsicht vollumfänglich unterstützt. Das Ergebnis haben wir mit der verantwortlichen Abteilungsleitung des Niedersächsischen Ministerium für Inneres und Sport besprochen. Auf Details der Prüfung können wir im Tätigkeitsbericht aufgrund bestehender Geheimhaltungspflichten nicht weiter eingehen.

Ausblick

Aktuell ist seitens der Landesregierung beabsichtigt, das Niedersächsische Verfassungsschutzgesetz zu novellieren.[3] Bei der Umsetzung des Gesetzesvorhabens ist unter anderem geplant, die Mitteilungspflichten gegenüber

1 § 33a Abs. 1 des Niedersächsischen Verfassungsschutzgesetzes (NVerfSchG).
2 § 14 Abs. 1 Nr. 6 bis Nr. 12 NVerfSchG.
3 https://www.stk.niedersachsen.de/237506.html

dem Betroffenen nach Ende des Einsatzes nachrichtendienstlicher Mittel zu beschränken.[4] So sollen künftig lediglich „erheblich betroffene Personen" informiert werden. Hier wird der Gesetzgeber zu prüfen haben, ob er bereit ist, den damit einhergehenden Verlust an datenschutzfreundlicher Transparenz durch den Wegfall einer Informationspflicht ohne jegliche Kompensationsmaßnahme hinzunehmen.

Sollte der Gesetzgeber die erwogenen Änderungen der gesetzlichen Mitteilungspflichten beschließen, hätte dies auch Auswirkungen auf die künftigen datenschutzrechtlichen Prüfungen des Verfassungsschutzes. Insbesondere werden sich die Prüfungen zusätzlich mit der Frage beschäftigen müssen, ob die Verneinung einer „erheblichen Betroffenheit" seitens des Verfassungsschutzes rechtmäßig war.

4 Niedersächsischer Landtag, Drucksache 19/5930, Art. 1 Nr. 10 (§ 22 NVerfSchG).

Datenschutz-Folgenabschätzung für das Einsatzleitsystem der polizeilichen und kooperativen Leitstellen geprüft G.8.3

Im Berichtsjahr 2024 haben wir die Datenschutz-Folgenabschätzung zur aktuellen Leitstellensoftware der niedersächsischen Polizei überprüft und unsere Prüfergebnisse anschließend in Erörterungsgespräche und Coachings mit der Polizei einfließen lassen.

Der Prüfung vorangegangen war eine im Jahr 2022 abgeschlossene Kontrolle der Leitstellen der niedersächsischen Polizei, über die wir bereits im 28. Tätigkeitsbericht ausführlich berichtet hatten.[1] Da die verantwortlichen Polizeibehörden zu der seinerzeit eingesetzten Leitstellensoftware ihrer gesetzlichen Pflicht zu einer Datenschutz-Folgenabschätzung (DSFA)[2] nicht ausreichend nachgekommen waren, stellten wir im Hinblick auf die neue Leitstellensoftware eine enge Begleitung in Aussicht.

Im Zuge der Prüfung konnten wir mehrere Herausforderungen identifizieren. So sind die Leitstellen zuständig für die Notrufannahme und Koordination der Einsätze von Rettungsdiensten, Feuerwehren und Hilfsorganisationen. Im Kontext dieser Leitstellen gibt es daher mehrere Verantwortliche (gemeinsame Verantwortliche) sowie Auftragsverarbeiter. Gerade in solch vielschichtigen Konstellationen ist eine eindeutige Zuordnung und transparente Dokumentation der jeweiligen Verantwortlichkeiten ein wichtiger Bestandteil der Dokumentationspflichten.

Erforderlich ist zudem eine vollständige Ableitung der Anforderungen aus den zugrunde liegenden Datenschutznormen, in diesem Fall insbesondere aus dem Niedersächsischen Datenschutzgesetz (NDSG), Teil 1 und 2 sowie der Datenschutz-Grundverordnung (DSGVO).

Gerade beim Umgang mit sensiblen Daten in diversen Verarbeitungsketten ist die Darstellung von Verfahren, Garantien und verfahrensrechtlichen Vorkehrungen zur Einhaltung von Löschfristen, der Meldung von Verlet-

1 Siehe Tätigkeitsbericht 2022, J.1.1.
2 § 39 Abs. 1 NDSG.

zungen des Schutzes personenbezogener Daten, der Protokollierung und zur Sicherheit der Datenverarbeitung von herausgehobener Bedeutung.

Ausgangspunkt der Bewertung angemessener technisch-organisatorischer Maßnahmen (TOM) ist stets eine durchgängig aussagefähige und systematische Beschreibung der geplanten Verarbeitungsvorgänge und -zwecke, inklusive der Schnittstellenprozesse.

Schließlich ist eine vollumfängliche Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und die zu deren Eindämmung getroffenen Maßnahmen erforderlich. Garantien zur Einhaltung der gesetzlichen Vorgaben sollten ebenso nachgewiesen werden wie auch die Verfahren, mit denen die Wirksamkeit der getroffenen Maßnahmen zum Beginn der jeweiligen Verarbeitungstätigkeiten und während des Regelbetriebes kontrolliert und aufrecht erhalten werden.

DSFA-Coaching für die Polizei

Aufgrund der identifizierten Verbesserungspotenziale haben wir der niedersächsischen Polizei eine begleitende Beratung in Form eines „DSFA-Coachings" angeboten, um die Fortschreibung der DSFA zur Datenverarbeitung in den Leitstellen mit der notwendigen Methodenkenntnis zu unterstützen. In dieser begleitenden Beratung haben wir den behördlichen Datenschutzbeauftragten und zuständigen Beschäftigten Methoden zur Analyse sowie zur prägnanten und systematischen Darstellung von Analyseergebnissen vermittelt – die dann direkt für die Leitstellen umgesetzt wurden.

Gleichzeitig wurden mit diesem Vorgehen die Ergebnisse der DSFA nochmals überprüft, fortgeschrieben und gegebenenfalls Maßnahmen zur weiteren Verbesserung umgesetzt. Denn auch die Durchführung von Datenschutz-Folgenabschätzungen und dem damit verbundenen Wissensgewinn folgt dem sogenannten PDCA-Zyklus und ermöglicht somit eine kontinuierliche Verbesserung.[3]

3 Der PDCA-Zyklus (Plan, Do, Check, Act), auch Deming-Kreis genannt, ist eine Vorgehensweise zur kontinuierlichen Verbesserung und Bestandteil vieler Management-Systeme, wie beispielsweise ISO/IEC 27001 Information technology – Security techniques – Information security management systems - Requirements specification, BSI Standard 200-1, Standard-Datenschutzmodell (SDM) der DSK, sowie der „Prozess zur Auswahl angemessener Sicherungsmaßnahmen" (ZAWAS) –Version 1.0 des LfD Niedersachsen.

Ausblick und Fazit

Die begleitende Beratung der DSFA-Erstellung wird 2025 fortgesetzt. Damit wollen wir auch einen „Multiplikationseffekt" innerhalb der niedersächsischen Polizei erzielen, um damit einen Beitrag zu systematischer aufgebauten, leichter prüfbaren und damit im Ergebnis zu verbesserten Datenschutz-Folgeabschätzungen zu leisten.

G.8.4 Fehlende Rechtsgrundlagen bei Gefahrenabwehr, Gefahrenvorsorge und Strafverfolgung

Sowohl im Bereich der Gefahrenabwehr und Gefahrenvorsorge als auch im Bereich der Strafverfolgung wird immer wieder deutlich, dass für bestimmte Maßnahmen der Sicherheitsbehörden keine Rechtsgrundlagen für die damit einhergehende Datenverarbeitung vorhanden sind, obwohl diese zwingend erforderlich wären.

Nach den europarechtlichen Vorgaben sowie deren niedersächsischer Umsetzung haben wir als Datenschutzaufsichtsbehörde unter anderem als Aufgabe und Befugnis die Exekutive und Legislative datenschutzrechtlich zu beraten.[1] Dieser Aufgabe kommen wir gerne nach und weisen beispielhaft auf die aus unserer Sicht derzeit bestehenden gesetzgeberischen Handlungspflichten in den oben genannten Bereichen hin.

Rechtsgrundlage für PHW und EHW

Ein Fall betrifft die sogenannten personengebundenen und ermittlungsbezogenen Hinweise (PHW und EHW). Diese führt die Polizei als Datenbankeinträge zum Schutz der Polizistinnen und Polizisten im Arbeitsalltag – etwa vor gewalttätigen Personen. Auf Bundesebene existiert hierfür eine Rechtsgrundlage im Bundeskriminalamtsgesetz (BKAG), die jedoch nur eine Weiterverarbeitung der Daten durch das Bundeskriminalamt zulässt.[2] Außerhalb dieser Rechtsgrundlage werden durch die niedersächsischen Polizeibehörden zum Teil jedoch auch PHW und EHW in eigenen Systemen verarbeitet und landesintern genutzt. Hierfür bedarf es einer konkreten Regelung im Niedersächsischen Polizei- und Ordnungsbehördengesetz

1 Art. 46 Abs. 1 Buchst. c und Art. 47 Abs. 3 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (sogenannte JI-Richtlinie) sowie § 57 Abs. 2 Nr. 3 NDSG.

2 § 29 in Verbindung mit § 16 Abs. 6 BKAG.

(NPOG). Da es sich bei den PHW und EHW häufig um personenbezogene Daten besonderer Kategorien handelt, sollte die Rechtsgrundlage zudem eine Differenzierung nach diesen Kategorien personenbezogener Daten vorsehen, die der besonderen Eingriffsintensität der Datenspeicherung gerecht wird.[3]

Rechtsgrundlage für Zuverlässigkeitsprüfungen

Ein weiteres Beispiel für den bestehenden Anpassungsbedarf ist die rechtliche Ausgestaltung von Zuverlässigkeitsüberprüfungen bei Großereignissen. Hierfür werden in Niedersachsen derzeit Einwilligungen der betroffenen Personen eingeholt.[4]

Wir raten dringend an, eine spezifische Rechtsgrundlage im NPOG zu schaffen. Da die Sicherheitsüberprüfungen häufig mit der Ausübung einer beruflichen Tätigkeit verbunden sind, ist insbesondere die Freiwilligkeit einer Einwilligung in diesem Zusammenhang schwerlich zu gewährleisten.

Rechtsgrundlage für Datenübermittlung an Europol

Weitere Erkenntnisse lieferte eine gemeinsame Prüfung der deutschen Datenschutzaufsichtsbehörden mit dem Fokus auf Übermittlungen personenbezogener Daten Minderjähriger durch die Landespolizei an Europol.[5]

Hieraus ergab sich, dass es für derartige Übermittlungen durch das Niedersächsische Landeskriminalamt an Europol gesetzlicher Anpassungen der Rechtsgrundlagen im NPOG bedarf.[6]

Rechtsgrundlage für Drohneneinsätze

Auch bedarf es einer speziellen Rechtsgrundlage für den Einsatz von Videoflugdrohnen durch die Polizei angesichts der erhöhten Eingriffsintensität der Maßnahme. Eine solche gibt es bislang im NPOG nicht.[7]

3 In Umsetzung des Art. 10 JI-Richtlinie.
4 § 31 Absatz 4 NPOG.
5 Siehe Tätigkeitsbericht 2023, G.7.1.
6 Etwa in § 43 Absatz 2 Nummer 1 NPOG.
7 Siehe G. 1.4 zum Thema Rechtsgrundlagen für den Drohneneinsatz.

Gleiches gilt auch bezüglich des beabsichtigten Zulassens von Drohneneinsätzen im Niedersächsischen Verfassungsschutzgesetz (NVerfSchG). Im aktuellen Gesetzgebungsverfahren zum NVerfSchG ist die Aufhebung des bisherigen Einsatzverbots von Drohnen durch den Niedersächsischen Verfassungsschutz vorgesehenen. Auch hier bedarf es einer speziellen Rechtsgrundlage.[8]

Umsetzung der Vorgaben des Bundesverfassungsgerichts

Darüber hinaus sind weitere Anpassungen sowohl im Bereich der Polizei als auch im Bereich des Verfassungsschutzes vorzunehmen. So sind etwa die Vorgaben des Bundesverfassungsgerichts aus seinem Urteil „BKAG II"[9] sowie weiterer seiner verfassungsrechtlichen Entscheidungen, die seit 2018 ergangen sind, im NPOG vollständig umzusetzen.

Zugleich bedarf es im Bereich des Verfassungsschutzes der noch weitergehenden Umsetzung von bundesverfassungsgerichtlichen Vorgaben.[10] Dies betrifft etwa die Regelungen im NVerfSchG zur Übermittlung von Daten an Stellen mit operativen Befugnissen. Hierfür ist es insbesondere erforderlich, die Vorgabe einer konkreten Gefahr im Gesetz zu verankern.[11]

Umsetzung der JI-Richtlinie

Auch im zweiten Teil des NDSG, der insbesondere für die Polizei- und Strafverfolgungsbehörden zur Anwendung kommt, besteht weiterhin Anpassungsbedarf. Viele der in unserer Stellungnahme vom 8. Januar 2024 zur Änderung des NDSG[12] enthaltenen wichtigen Änderungs- und Ergänzungsbedarfe zur Umsetzung der JI-Richtlinie wurden bislang nicht berücksichtigt.

So mangelt es beispielsweise weiterhin an der Schaffung der in der JI-Richtlinie vorgesehenen wirksamen Abhilfebefugnisse für unsere Behörde.[13]

8 Siehe G.1.4 zum Thema Rechtsgrundlagen für den Drohneneinsatz.
9 BVerfG, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19.
10 Siehe BVerfG, Urteil vom 17. September 2024 – 1 BvR 2133/22.
11 Siehe BVerfG, Urteil vom 17. September 2024 – 1 BvR 2133/22.
12 Siehe Vorlage 1 zu Niedersächsischer Landtag, Drucksache 19/2631 sowie Niedersächsischer Landtag, Drucksache 19/3433, Zu Artikel 4 (Änderung des Niedersächsischen Datenschutzgesetzes).
13 Vergleiche Art. 47 Abs. 2 JI-Richtlinie sowie § 57 Absatz 5 NDSG.

Fazit und Ausblick

Es ist festzustellen, dass es in verschiedenen Bereichen dringenden Handlungsbedarf hinsichtlich der rechtlichen Grundlagen für die Datenverarbeitung gibt. Es ist stets erforderlich, europarechtliche und verfassungsgerichtliche Vorgaben umzusetzen, um sich nicht dem Vorwurf eines rechtswidrigen Handelns aussetzen zu müssen.

Die Notwendigkeit zur Schaffung ausreichender Rechtsgrundlagen drängt sich zudem besonders beim (künftigen) Einsatz von KI-Anwendungen mit nicht nur geringer Eingriffstiefe auf.

H Abgeschlossene Bußgeldverfahren

Abgeschlossene Bußgeldverfahren

Im Jahr 2024 hat die niedersächsische Datenschutzaufsicht Bußgelder in Höhe von rund 1,04 Millionen Euro verhängt. Die Mehrzahl der im Jahr 2024 verhängten Geldbußen betraf erneut die unzulässige Videoüberwachung – besonders hohe Summen waren für Profilbildungen zu eigenen Werbezwecken bei Kreditinstituten fällig.

Im Jahr 2024 hat unsere Behörde insgesamt 98 neue Fälle unter Gesichtspunkten einer möglichen Geldbuße geprüft. Im gleichen Zeitraum haben wir 56 Erstbescheide in Bußgeldsachen erlassen, die sich zum Teil auf Fälle bezogen, die bereits in den Vorjahren eingeleitet wurden. Insgesamt haben wir Geldbußen in Höhe von rund 1,04 Millionen Euro festgesetzt.[1] Von diesen Erstbescheiden sind 47 rechtskräftig geworden, da die Adressaten keinen Einspruch eingelegt haben oder nach Erlass des Bescheides ausdrücklich auf einen Einspruch verzichtet haben. Das entspricht einer Bußgeldsumme von rund 834.000 Euro. Die nicht mit Geldbußen abgeschlossenen Verfahren sind entweder anhängig, waren nicht bußgeldwürdig, wurden eingestellt oder wurden an andere zuständige Stellen abgegeben.

Insgesamt haben wir im Jahr 2024 Geldbußen in Höhe von rund 1,04 Millionen Euro festgesetzt.

Die Erstbescheide wurden gegenüber Verantwortlichen aus den Bereichen Gastgewerbe, Einzelhandel, Finanzdienstleistungen, Fitnessstudios, Gesundheitswesen, sonstige Dienstleister sowie gegen natürliche Personen erlassen. Die natürlichen Personen haben die Verstöße teilweise als Inhaberinnen beziehungsweise Inhaber von Unternehmen begangen.

Geahndet haben wir Verstöße gegen die Artikel 5, 6, 9, 12, 13, 15, 17, 25, 30, 31, 32, 35, 38 sowie 83 Absatz 5 Buchstabe e Datenschutz-Grundverordnung (DSGVO) und § 26 Bundesdatenschutzgesetz (BDSG). Bei den Verstößen handelte es sich um die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage, um Verstöße gegen die Informations-, Aus-

1 Für die Summe wurden nur die in den Vorverfahren ergangenen Bußgeldbescheide berücksichtigt (Erstbescheide). Legt der Bußgeldadressat Einspruch ein, kann im Zwischenverfahren ein neuer Bußgeldbescheid ergehen (Zweitbescheid).

kunfts- und Löschpflicht, die Nichtführung beziehungsweise Nichtvorlage von Verzeichnissen der Verarbeitungstätigkeit, um unzureichende technische Maßnahmen, um die Nichtanfertigung einer Datenschutzfolgenabschätzung sowie um die Nichtbeachtung behördlicher Anweisungen.

Gerichtliche Entscheidungen

Im Jahr 2024 haben Gerichte Entscheidungen zu acht unserer Bußgeldverfahren getroffen. In einer Mehrzahl der Fälle haben die Bußgeldadressaten die Verstöße im Wege einer gerichtlichen Verständigung[2] eingeräumt und ihre Einsprüche auf die Rechtsfolgenseite beschränkt. Bei solch einer Beschränkung wird die vom Landesbeauftragten für den Datenschutz (LfD) ausgesprochene Feststellung des Verstoßes unmittelbar rechtskräftig, sodass das Gericht noch über die Höhe der Geldbuße zu entscheiden hat.

Weitere gerichtliche Entscheidungen wegen Bußgeldbescheiden unserer Behörde werden für das Jahr 2025 erwartet.

Profilbildung zu Werbezwecken mit Smart-Data-Verfahren

Im Berichtszeitraum haben wir erneut mehrere Bußgeldverfahren im Zusammenhang mit Smart-Data-Verfahren zum Abschluss gebracht.[3] Einzelne Kreditinstitute bildeten mit vorhandenen personenbezogenen Daten aktiver Kundinnen und Kunden Profile zur werblichen Ansprache. Ausgewertet wurden Zahlungsdaten (zum Beispiel das im Vorjahr eingegangene Gehalt, Zahlungen per E-Payment und Grundkosten wie Energieversorgung), Stammdaten (zum Beispiel Alter, Familienstand und Dauer der Kundenbeziehung) sowie Angaben zum Wohnumfeld (zum Beispiel Anteil der Erwerbstätigen und Anzahl der PKW-Neuzulassungen im sogenannten Mikromarkt).

Ziel der Institute war es, anhand der so gebildeten Profile Kundinnen und Kunden zu identifizieren, die für spezifische Produkt besonders zugänglich sein könnten. Solche Auswertungen der vorhandenen Daten sowie die Hinzuziehung weiterer Daten für Werbezwecke war von den Kundinnen und Kunden vernünftigerweise nicht zu erwarten. Die Unternehmen

2 Siehe auch Tätigkeitsbericht 2021, I.4.
3 Siehe hierzu auch Tätigkeitsbericht 2023, H und G.3.3.

konnte sich daher nicht auf ein berechtigtes Interesse[4] als Rechtsgrundlage stützen. In 12 Verfahren hat unsere Behörde Geldbußen in Höhe von insgesamt 631.000 Euro festgesetzt. Weitere Verfahren sind anhängig.

Ebenfalls im Smart-Data-Kontext hat unsere Wirtschaftsaufsicht aufgrund von Beschwerden in drei gesonderten Verwaltungsverfahren die Art der Einholung von Einwilligungen überprüft. Die Beschwerdeführer hatten im Onlinebanking in den von uns geprüften Einzelfällen keine Möglichkeit, die Erteilung der Einwilligung abzulehnen. Wollten sie keine Einwilligung erteilen, konnten sie das entsprechende Dialogfenster lediglich durch Betätigung der Schaltfläche „Jetzt nicht zustimmen" schließen. Dies führte dazu, dass die Abfrage alle sechs Wochen erneut erschien. Somit war nicht gewährleistet, dass die Kundinnen und Kunden ihre Einwilligung freiwillig erteilen. Wir haben den Kreditinstituten angekündigt, die Nutzung dieser Einwilligungen verwaltungsrechtlich zu untersagen. Die Untersagung musste nicht mehr ausgesprochen werden, weil die Institute rechtzeitig eine Schaltfläche zum Ablehnen der Einwilligung integriert haben. Bußgeldverfahren wurden nicht eingeleitet.

Technisch-organisatorische Maßnahmen

Ein größeres Unternehmen aus dem Gesundheitssektor verfügte über eine aus dem Internet zugängliche Schnittstelle für den Zugriff auf die E-Mail-konten des Unternehmens. Aufgrund einer Beschwerde wurden wir darauf aufmerksam, dass verschiedene Funktions-E-Mail-Adressen mit einem einfachen Passwort wie „123456" gesichert waren. Mit Kenntnis der E-Mail-Adresse und der dazugehörigen Domäne war aus dem Internet ein Zugriff auf die Inhalte der E-Mail-Postfächer möglich.

Mehrere der so zugänglichen Postfächer waren leer oder enthielten keine sonderlich sensiblen Daten. Einzelne Postfächer enthielten jedoch umfangreiche Bewerbungsunterlagen und Gesundheitsdaten Dritter.[5] Für solche Daten gilt die (zweithöchste) Schutzstufe D nach dem Schutzstufenkonzept[6] des LfD Niedersachsen, da die unsachgemäße Handhabung solcher

4 Art. 6 Abs. 1 Buchst. f DSGVO.

5 Gesundheitsdaten gelten als besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO.

6 Schutzkonzept zum Download unter https://www.lfd.niedersachsen.de/download/137188/ (PDF).

Daten die datenschutzrechtlich Betroffenen in ihrer gesellschaftlichen Stellung oder ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigen und zu einer Existenzgefährdung führen könnte.

Die Zugänglichkeit mit einfachen Passworten stellt einen Verstoß gegen den Grundsatz der Vertraulichkeit[7] dar: Das Unternehmen hatte nicht die erforderlichen technischen und organisatorischen Maßnahmen ergriffen, um zu verhindern, dass auf die E-Mail-Konten zugegriffen werden konnte.[8] Das Unternehmen stellte die Verstöße nach Kenntniserlangung zeitnah ab. Im Verlauf des Verfahrens wurde deutlich, dass die technisch-organisatorischen Maßnahmen im Übrigen überdurchschnittlich ausgeprägt sind. Der Geldbuße in Höhe von 115.000 Euro ging eine Erörterung zwischen dem Unternehmen und der Behörde voraus.

Veröffentlichung von personenbezogenen Daten auf Social-Media-Kanälen

Im Berichtsjahr wurden vermehrt Verstöße im Zusammenhang mit der Veröffentlichung von personenbezogenen Daten auf Social-Media-Kanälen nach vorangegangenen persönlichen Konflikten mit einem Bußgeld geahndet.

In einem Fall veröffentlichte die Betreiberin eines Online-Kleiderverleihs den Chatverlauf mit einer Kundin in ihrer für sämtliche Instagram-Nutzer sichtbaren Instagram-Story, nachdem diese sich öffentlich über den Kundenservice beschwert hatte. In dem veröffentlichten Chatverlauf waren unter anderem der Name und die Privatanschrift der Kundin erkennbar.

In einem anderen Fall hatte ein Verantwortlicher die private Mobilfunknummer seiner Ex-Freundin mit Hinweis auf deren Instagram-Account in einer Instagram-Story veröffentlicht und diese dadurch für seine Kontakte verfügbar gemacht. Zu den Zwecken des Verantwortlichen zählte offenbar, die Öffentlichkeit an seinem Unmut über seine Ex-Freundin teilhaben zu lassen.

Weitere sanktionierte Fälle betrafen die Veröffentlichung von Fotografien von Beschuldigtenanhörungen auf diversen Social-Media-Kanälen. Die

7 Art. 5 Abs. 1 Buchst. f DSGVO.

8 Die Verpflichtung zur Ergreifung solcher Maßnahmen ergibt sich aus Art. 32 DSGVO.

Veröffentlichung hatte in einem Fall zur Folge, dass einer unbestimmten Anzahl von Personen die Information zugänglich war, dass ein namentlich benannter Polizeibeamter mit der Sachbearbeitung politisch motivierter Kriminalität befasst ist und im Bereich einer bestimmten Stadt tätig sein könnte. Hierdurch wurde die Möglichkeit für Dritte eröffnet, den Polizeibeamten in seiner Aufgabenwahrnehmung beispielsweise durch Anrufe zu belästigen und diesen in seinem persönlichen Lebensbereich zu schädigen.

Die Veröffentlichung von Namen und weiteren personenbezogenen Daten auf öffentlichen Social-Media-Kanälen stellt einen Grundrechtseingriff dar und setzt eine Einwilligung der Betroffenen oder eine sonstige Rechtsgrundlage zwingend voraus. Einwilligungen lagen in den geschilderten Fällen nicht vor. Eine Rechtsgrundlage müsste auf der Verfolgung berechtigter Interessen der Verantwortlichen beruhen, denen keine schutzwürdigen Interessen der Betroffenen entgegenstehen. Eine solche Rechtslage war in den verfolgten Fällen nicht ansatzweise gegeben. Für die Verstöße setzten wir Geldbußen im mittleren dreistelligen Bereich fest.

Videoüberwachung

Viele Fälle betrafen auch im Jahr 2024 den Bereich der Videoüberwachung. Dabei lag ein Schwerpunkt auf Verfahren, in denen Arbeitgeber ihre Beschäftigten sowie Kundinnen und Kunden per Video überwachen. Das Vorgehen gegen Videoüberwachung am Arbeitsplatz haben wir bereits in vergangenen Tätigkeitsberichten ausführlich vorgestellt.[9] Einzelne Fälle werden kurz exemplarisch dargestellt:

11.200 Euro gegen ein Unternehmen des Beherbergungs- und Gaststättengewerbes mit weniger als 900.000 Euro Jahresumsatz wegen Überwachung von Aufenthaltsbereichen für Gäste („Hochzeitssaal“) sowie unzureichender Erteilung von Pflichtinformationen[10] und eines fehlenden Verzeichnisses der Verarbeitungstätigkeit.

52.600 Euro gegen ein Unternehmen des Einzelhandels mit diversen Standorten mit etwa 6,0 Millionen Euro Jahresumsatz wegen Überwachung von Kundinnen und Kunden sowie Beschäftigten. Die Entscheidung ist nicht rechtskräftig. Es gilt die Unschuldsvermutung.

9 Siehe Tätigkeitsbericht 2019 J.9.4, Tätigkeitsbericht 2020 I.5 und Tätigkeitsbericht 2021 J.9.2.
10 Art. 13 DSGVO.

5.000 Euro gegen ein Unternehmen des Beherbergungsgewerbes mit etwa 500.000 Euro Jahresumsatz wegen Überwachung von Aufenthaltsbereichen für Gäste sowie des öffentlichen Verkehrsraums.

19.000 Euro gegen ein Unternehmen mit etwa 5,6 Millionen Euro Jahresumsatz wegen der Überwachung von Trainingsflächen in mehreren Fitnessstudios im Wege einer Erörterung mit der Verwaltungsbehörde. Berücksichtigt wurden verschiedene mildernde Umstände.

5.700 Euro gegen den Inhaber einer Vergnügungsstätte (Spielhalle) wegen Überwachung von Beschäftigten sowie Kundinnen und Kunden im Wege einer gerichtlichen Verständigung ohne Verhandlung.

Dashcams

Diverse Bußgeldentscheidungen entfielen zudem erneut auf Dashcams und andere Kamerasysteme, die anlasslos Videosequenzen aufzeichneten und damit von den Verantwortlichen unzulässig eingesetzt wurden. Geldbußen in Höhe von 2.500 Euro beziehungsweise 4.200 Euro wurden gegen Unternehmen festgesetzt, die in jeweils einem Firmenfahrzeug eine Dashcam verwendet haben.

Sanktioniert werden nur Fälle, in denen Videosequenzen anlasslos aufgezeichnet (gespeichert) werden. Ist die Kamera so eingestellt, dass nur bei Anlässen die Speicherung einer kurzen Videosequenz erfolgt, sanktionieren wir dies nicht. Dabei darf die Videosequenz bei diesem sogenannten Prerecording auch einen kurzen Zeitraum von bis zu 30 Sekunden vor dem Ereignis umfassen. Unabhängig davon haben die Betreiber von Dashcams und ähnlichen Kameras auf die Informationspflichten zu achten.

Zu Dashcam-Geldbußen haben wir bereits ausführlich berichtet[11] und einen umfangreichen Fragen-Antworten-Katalog für Betreiberinnen und Betreiber von Dashcams veröffentlicht, den wir im Berichtszeitraum aktualisiert haben.[12]

11 Siehe Tätigkeitsbericht 2019, I.5.

12 https://lfd.niedersachsen.de/dashcam

Nichterteilung verlangter Auskünfte

In mehreren Fällen hat die Datenschutzaufsicht Niedersachsen Geldbußen bis zu 6.100 Euro wegen der Nichterteilung verlangter Auskünfte durch datenschutzrechtlich Verantwortliche ausgesprochen. Die Geldbußen richteten sich im Berichtsjahr gegen Verantwortliche mit geringerem Umsatz. Allen Fällen ging ein bestandskräftiges Auskunftsverlangen voraus.[13]

Verantwortliche sind verpflichtet, mit der Aufsichtsbehörde auf deren Anfrage zusammenzuarbeiten.[14] Kommen Verantwortliche dieser Verpflichtung nicht nach, führt dies in der Praxis unserer Behörde allerdings nicht unmittelbar zu einem Bußgeldverfahren. Zunächst versuchen wir, die Verpflichtung im Verwaltungsverfahren mit Zwangsmitteln durchzusetzen. Insbesondere werden Zwangsgelder angedroht und festgesetzt. Wird die Auskunft in diesem Verfahren erteilt, wird regelmäßig auf die Durchführung eines Bußgeldverfahrens verzichtet. Haben die Zwangsmittel hingegen keinen Erfolg, wird in der Regel ein Bußgeldverfahren eingeleitet.

Selbst mit Zahlung des Bußgelds ist das Überprüfungsverfahren nicht erledigt, und die Behörde kann weitere Ermittlungen anstellen. Bei zureichenden tatsächlichen Anhaltspunkten für einen Verstoß können gegebenenfalls auch Räumlichkeiten durchsucht werden. Weitere festgestellte Verstöße können gesondert mit Geldbuße geahndet werden.

Zuspitzung im Verwaltungsverfahren

In geeigneten Fällen geben wir Beschwerden an die Datenschutzbeauftragten der Verantwortlichen. Jene bitten wir, eine Abhilfe der Beschwerde durch die Verantwortlichen zu prüfen. Diese Vorgehensweise wird der besonderen Bedeutung von Datenschutzbeauftragen und ihrer Position in Unternehmen und der Funktion als verlängerter Arm der Aufsichtsbehörde gerecht. Häufig führt dies zu einer schnellen, für alle Beteiligten zufriedenstellenden Abhilfe der Beschwerde.

Im Berichtszeitraum konnten wir in einem Beschwerdeverfahren die Angelegenheit allerdings nicht auf diese Weise klären, stattdessen führte der Vorgang schlussendlich sogar zur Verhängung eines Bußgelds gegen den

13 Anweisung im Sinne von Art. 58 Abs. 1 Buchst. a DSGVO.
14 Art. 31 DSGVO.

Verantwortlichen. In dem Fall kontaktierte ein Unternehmen eine Person, obwohl nach deren Kenntnis schon einige Zeit kein Vertrag mehr bestand. Ziel der Kontaktaufnahme war zudem ein neuer Zweck, nämlich der Versuch, an eine dritte Person über den Kontaktierten heranzutreten. Dieser beschwerte sich bei unserer Behörde. Die von uns erwartete Abhilfe durch den Verantwortlichen erfolgte nicht. Stattdessen gingen für den Verantwortlichen teilweise widersprüchliche Stellungnahmen von Bevollmächtigten ein.

Im Laufe des Verfahrens wurde mitgeteilt, dass der Beschwerdeführer insbesondere noch einen Vertrag über ein elektronisches Postfach mit dem Verantwortlichen habe. Über ein solches Postfach stellt der Verantwortliche seinen Kundinnen und Kunden Unterlagen zur Verfügung gestellt, zum Beispiel Rechnungen. Warum dieses Postfach nach Kündigung der übrigen Verträge weiter bestand, konnten wir nicht nachvollziehen. So sah das auch der Beschwerdeführer, der daraufhin Auskunft vom Verantwortlichen verlangte[15], welche wiederum nicht innerhalb der gesetzlichen Frist von einem Monat[16] erteilt wurde.

Im Ergebnis haben wir Geldbußen in Höhe von insgesamt 9.000 Euro festgesetzt. Diese deckte sowohl die unzulässige zweckändernde Verarbeitung als auch die nicht rechtzeitige Auskunftserteilung ab.

15 Art. 15 DSGVO.
16 Art. 12 Abs. 3 Satz 1 DSGVO.

I Deutsche Datenschutzkonferenz

I.1 Arbeitskreis Beschäftigtendatenschutz: Gesetzliche Regelungen noch immer nicht in Kraft

Im Jahr 2024 lag ein Schwerpunkt des von uns geleiteten Arbeitskreises Beschäftigtendatenschutz bei Zuarbeiten für die Datenschutzkonferenz zum Gesetzgebungsvorhaben der Bundesregierung für ein Beschäftigtendatengesetz. Als weitere Themen standen vor allem die Verarbeitung von Beschäftigtendaten bei „Asset Deals" und der „Plattformarbeit" im Vordergrund.

Der Arbeitskreis (AK) Beschäftigtendatenschutz der Datenschutzkonferenz (DSK) erarbeitet einheitliche Positionen aller Aufsichtsbehörden zu datenschutzrechtlichen Fragen im Beschäftigtenkontext. Er bereitet zudem Entscheidungen der Datenschutzkonferenz vor und bespricht aktuelle Themen und Urteile.

Mit unseren Kolleginnen und Kollegen aus den anderen Datenschutzbehörden tauschten wir uns Anfang 2024 zu besonderen Fallkonstellationen aus, beispielsweise zur aktuellen Rechtslage zum Auskunftsrecht im Beschäftigtenkontext. Ein weiteres Thema war die Frage der Vorlage von Führungszeugnissen. Hierzu wurde festgestellt, dass deren gesetzlich geforderte Vorlage regelmäßig nicht die Speicherung von Originalen oder Kopien in den Personalunterlagen umfasst. Stattdessen reicht es aus, in einem Vermerk zu dokumentieren, dass die Voraussetzungen zur Aufnahme oder Fortsetzung einer Tätigkeit gegeben sind.

DSK-Beschluss „Asset Deal"

Intensiv auseinandergesetzt hat sich der AK Beschäftigtendatenschutz im Jahr 2024 mit der Verarbeitung von Beschäftigtendaten im Rahmen von sogenannten Asset Deals. Dabei handelt es sich um eine Art des Unternehmenskaufs, bei dem nicht das Unternehmen als Ganzes, sondern dessen Vermögenswerte und Wirtschaftsgüter (Assets) an den Käufer übertragen werden. In datenschutzrechtlicher Hinsicht erfordert diese Form der Un-

ternehmensveräußerung bei der Übermittlung personenbezogener Daten eine besondere Betrachtung.

Zu diesem Thema veröffentlichte die DSK im September den Beschluss „Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset Deals“[1]. Für diesen Beschluss arbeitete unser Arbeitskreis dem AK Wirtschaft zu für den Abschnitt IV, der sich mit Beschäftigtendaten befasst.

Wichtig ist in diesem Zusammenhang, dass zum Zeitpunkt eines zivilrechtlichen Betriebs- oder Betriebsteilübergangs[2] die Verarbeitung von Beschäftigtendaten regelmäßig zur Erfüllung arbeitsvertraglicher Regelungen erforderlich ist. Schwieriger hingegen gestaltet sich eine rechtskonforme Datenverarbeitung im Zuge von vorvertraglichen Verhandlungen. Hierbei lässt sich die Datenverarbeitung in den allermeisten Fällen allenfalls mit einer Einwilligung[3] des Betroffenen rechtfertigen.

Stakeholder-Dialog zum Thema Plattformarbeit

Auf Einladung des Bundesministeriums für Arbeit und Soziales fand am 1. Oktober 2024 ein Stakeholder-Dialog zum Thema Plattformarbeit statt. Ziel des Dialogs war ein Austausch zur nationalen Umsetzung der EU-Richtlinie zur Verbesserung der Arbeitsbedingungen in der Plattformarbeit.[4] Als Vorsitz des AK Beschäftigtendatenschutz konnten wir bei dem Dialog verdeutlichen, an welchen Stellen datenschutzrechtliche Belange bei der rechtlichen Ausgestaltung von Plattformarbeit und der Umsetzung der vorgenannten EU-Richtlinie zum Tragen kommen. So sollten beispielsweise in dem Gesetz die datenschutzrechtlichen Rollen „Verantwortlicher“, „gemeinsam Verantwortliche“ sowie „Auftragsverarbeiter“ im Fall der Plattformarbeit klargestellt werden.

1 Siehe DSK-Beschluss „Übermittlungen personenbezogener Daten an die Erwerberin oder den Erwerber eines Unternehmens im Rahmen eines Asset-Deals“ vom 11. September 2024, abrufbar unter https://t1p.de/dsk-asset
2 § 613a BGB.
3 Art. 6 Abs. 1 Buchst. a DSGVO.
4 Richtlinie (EU) 7212/24.

Beschäftigtendaten(schutz)gesetz

Seit nunmehr bereits einem Jahrzehnt fordert die DSK wiederholt und vehement spezifische gesetzliche Regelungen zur Datenverarbeitung im Beschäftigtenkontext. Zum Ende des Berichtzeitraums wurde leider absehbar, dass es aufgrund der vorzeitig beendeten Legislaturperiode auf Bundesebene erneut nicht zum Abschluss eines Gesetzgebungsvorhabens für ein Beschäftigtendaten(schutz)gesetz kommen wird.

Bereits 2014 hatte die DSK in einer Entschließung auf fehlende Regelungen zu den Grenzen der Verhaltens- und Leistungskontrolle bei Beschäftigten und zum Umgang mit sensiblen Beschäftigtendaten hingewiesen. Forderungen nach entsprechenden gesetzlichen Grundlagen wurden erneut im April 2022 und zuletzt im Mai 2023 in Entschließungen der DSK aufgegriffen.[5]

Im Koalitionsvertrag für die 20. Legislaturperiode wurde als Ziel vereinbart, gesetzliche Regelungen zum Beschäftigtendatenschutz zu schaffen. Im Folgenden wurden – teils unter unserer Beteiligung – die maßgeblichen Eckpunkte für ein entsprechendes Gesetz entwickelt. Aufgrund der bundespolitischen Entwicklungen hat die Bundesregierung den bereits weit gediehenen „Gesetzentwurf zur Stärkung eines fairen Umgangs mit Beschäftigtendaten und für mehr Rechtssicherheit für Arbeitgeber und Beschäftigte in der digitalen Arbeitswelt (BeschDG)“ nicht mehr für den nächsten Schritt einer Verbandsanhörung freigeben. Mithin kam es nicht zur Fortsetzung des Gesetzgebungsverfahrens. Stattdessen wurde Ende Oktober 2024 lediglich ein Referentenentwurf für ein BeschDG öffentlich.

Ausblick

Im Rahmen unserer Aufgaben als Vorsitz des AK Beschäftigtendatenschutz haben wir insbesondere für die Begleitung des oben genannten Gesetzgebungsverfahren erhebliche Ressourcen zur Verfügung stellen müssen. In der Hoffnung, dass die neue Bundesregierung nach ihrer Konstituierung die Arbeiten an einem Beschäftigtendatenschutzgesetz zeitnah wieder

5 Siehe Tätigkeitsbericht 2023, Abschnitt I. 2, sowie DSK-Entschließungen vom 29. April 2022 „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!“ sowie vom 11. Mai 2023 „Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt‘!“, beide abrufbar unter dem Kurzlink: https://datenschutzkonferenz-online.de/entschliessungen.html

aufnehmen wird, kann und wird sich dieser erhebliche Einsatz als sinnvoll erweisen. Mit Blick auf die Entwicklung der digitalen Arbeitswelt, insbesondere beim Einsatz von Künstlicher Intelligenz, ist es dringlicher denn je, zeitnah ein Gesetz zum Schutz von Beschäftigtendaten zu schaffen. Sowohl zum Schutz der Beschäftigten bei der Verarbeitung ihrer personenbezogenen Daten als auch, um Rechtsklarheit für Arbeitgeber und Arbeitgeberinnen zu schaffen, bedarf es dringend sowohl schlanker wie auch zugleich unzweideutiger gesetzlicher Regelungen zur Datenverarbeitung im Beschäftigtenkontext.

I.2 Arbeitskreis Versicherungswirtschaft: Verhaltensregeln und Einwilligungen

Im Arbeitskreis Versicherungswirtschaft der Datenschutzkonferenz beraten wir als Vorsitzende mit den anderen Datenschutzbehörden Fragestellungen aus der Versicherungsbranche. In diesem Jahr standen insbesondere die Prüfung von Verhaltensregeln sowie die Einwilligung in die Verarbeitung von Gesundheitsdaten im Fokus.

Verhaltensregeln in der Versicherungswirtschaft

Die Beratungen im Arbeitskreis waren im Berichtszeitraum insbesondere vom Antrag des Gesamtverbandes der Deutschen Versicherungswirtschaft zur Genehmigung von Verhaltensregeln geprägt. Solche Verhaltensregeln dienen dazu, die Vorgaben der Datenschutz-Grundverordnung zu konkretisieren und so deren Anwendung zu erleichtern. Es wird damit eine einheitliche Auslegung der Datenschutz-Grundverordnung durch die Versicherungswirtschaft erreicht.

Die für den Genehmigungsantrag zuständige Behörde hat bei der Prüfung den Arbeitskreis beteiligt, weil die Verhaltensregeln deutschlandweit gelten sollen. Nachdem die Aufsichtsbehörden sich untereinander abgestimmt haben, werden nun mögliche Änderungsbedarfe mit dem Gesamtverband der Deutschen Versicherungswirtschaft besprochen.

Muster für Datenschutzeinwilligungen

Im Berichtszeitraum konnten wir die Prüfung einer Mustereinwilligung des Gesamtverbandes der Versicherungswirtschaft abschließen. Auf Grundlage des Musters können Unternehmen der Versicherungswirtschaft Einwilligungen in die Verarbeitung besonderer Kategorien personenbezogener Daten (insbesondere Gesundheitsdaten) einholen, welche für die Begründung und Durchführung von Lebens- und Krankenversicherungen erforderlich sind. Der Arbeitskreis hat das Muster abschließend zur Kenntnis genommen.

Datenschutzkonforme Nutzung von Gesundheitsdaten zu Forschungszwecken I.3

Auch 2024 befasste sich die Datenschutzkonferenz mit der Nutzung personenbezogener Daten zu Forschungszwecken, beispielsweise von Gesundheitsdaten. Damit hat sie der hohen Bedeutung der Forschung für eine zukunftsfähige Gesellschaft Rechnung getragen. Zugleich machten die Datenschutzbehörden erneut deutlich, dass wissenschaftliche Forschung und Datenschutz in keinem Widerspruch zueinander stehen.

Die Datenschutzkonferenz hat sich zur Sekundärnutzung von Daten zu Forschungszwecken in zwei Positionspapieren geäußert, die sich sowohl an die Gesetzgeber von Bund und Ländern als auch an forschende Stellen richten.

In dem Positionspapier zum Begriff der „wissenschaftlichen Forschungszwecke“[1] definiert die DSK die Voraussetzungen, unter denen sich öffentliche und nichtöffentliche Stellen auf die Forschungsprivilegien der Datenschutz-Grundverordnung (DSGVO) sowie des spezifischen Fachrechts[2] berufen können. Dies ist insbesondere relevant für private Stellen, deren Vorhaben oftmals auch kommerziellen Zwecken dienen. In Anlehnung an den Forschungsbegriff[3] des Bundesverfassungsgerichts wird festgestellt, dass sich auch private Stellen grundsätzlich auf die Forschungsfreiheit berufen können, sofern das Vorhaben auch dem Gemeinwohl zugutekommt und nicht ausschließlich kommerziellen Interessen dient.

Forschung mit Genomdaten

In dem Positionspapier „Anforderungen an die Sekundärnutzung von genetischen Daten zu Forschungszwecken“[4] legt die DSK die rechtlichen Rahmenbedingungen für die Nutzung dieser speziellen und besonders

1 Abrufbar unter https://t1p.de/z5zy1
2 Beispielsweise § 27 BDSG, § 13 NDSG, § 287 SGB V, §§ 67 c, 75 SGB X.
3 BVerfGE 35, 79 ff.
4 Abrufbar unter https://t1p.de/n9pkg

sensitiven Daten zu Forschungszwecken fest. Unter anderem fordert sie eine gesetzliche Vollregelung, die auf eine Einwilligungslösung setzt sowie die Kontroll- und Mitwirkungsmöglichkeiten der Betroffenen vorsieht. Begleitet werden soll dies von einer Ethikkommission.

Rechtssicherheit und schlanke Verfahren

Im März 2024 trat das Gesundheitsdatennutzungsgesetz (GDNG) in Kraft, das neue Rechtsgrundlagen für die Sekundärnutzung von Gesundheitsdaten durch Gesundheitseinrichtungen schafft und es den Datenaustausch im Rahmen länderübergreifender Forschungsvorhaben im Gesundheitsbereich ermöglicht. Zudem werden die bestehenden datenschutzaufsichtsrechtlichen Zuständigkeiten modifiziert indem es neue Abstimmungsverfahren regelt. Eine Unterarbeitsgruppe der von der DSK eingerichteten Task Force Forschungsdaten bereitet gegenwärtig eine Auslegungshilfe zu diesen neuen Rechtsvorschriften vor und steht in einem engen Austausch mit der Technologie- und Methodenplattform für vernetzte medizinische Forschung e. V. bezüglich eines Verfahrens zur Koordinierung von Genehmigungsanträgen kooperierender Einrichtungen an die zuständigen Datenschutzaufsichtsbehörden. Hierdurch sollen bestehende Verfahren verschlankt und eventueller Rechtsunsicherheit bei den forschenden Stellen begegnet werden.

Fazit

Die DSK und ihre Arbeitsgruppen haben auch im Berichtsjahr 2024 wichtige Schritte unternommen, um die bei der Umsetzung geänderter Rechtsvorschriften zur datenschutzkonformen Nutzung von personenbezogenen Daten zu Forschungszwecken zu unterstützen.

Leitfaden für den Einsatz von Anwendungen mit Künstlicher Intelligenz I.4

Im Mai 2024 hat die Datenschutzkonferenz die Orientierungshilfe „Künstliche Intelligenz und Datenschutz – Version 1.0" beschlossen. Sie bietet einen Überblick über datenschutzrechtliche Kriterien, die für die datenschutzkonforme Nutzung von KI-Anwendungen zu berücksichtigen sind.

Die Datenschutzkonferenz beschäftigt sich bereits seit einigen Jahren mit dem Thema Künstliche Intelligenz (KI). Die ersten beiden Veröffentlichungen der DSK aus dem Jahr 2019 dazu befassen sich mit abstrakten datenschutzrechtlichen Anforderungen für Künstliche Intelligenz und Empfehlungen für technische und organisatorische Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen. Sie hatten somit einen starken Fokus auf die Entwicklung von KI-Systemen. Spätestens seitdem der KI-Chatbot ChatGPT in Europa verfügbar ist, denken Unternehmen, Behörden und sonstige Organisationen ernsthaft über den Einsatz derartiger KI-Anwendungen nach. Den Landesbeauftragten für den Datenschutz Niedersachsen erreichen dementsprechend immer mehr Beratungsanfragen, was hierbei datenschutzrechtlich zu beachten ist. Daran anknüpfend soll die Orientierungshilfe „Künstliche Intelligenz und Datenschutz"[1] als Leitfaden für Unternehmen, Behörden, Schulen, Universitäten und weitere Stellen dienen, unter Beachtung des Datenschutzrechts KI-Systeme auszuwählen, zu implementieren und zu nutzen.

Die Struktur der Orientierungshilfe ist an einen typischen Entscheidungsprozess bei der Einführung neuer Anwendungssysteme in Organisationen angelehnt. Die drei Kapitel beschäftigen sich mit der Konzeption des Einsatzes und der Auswahl von KI-Anwendungen, der Implementierung von KI-Anwendungen und der Nutzung von KI-Anwendungen. Dabei ist zuerst zu berücksichtigen, ob ein KI-Modell mit personenbezogenen Daten trainiert worden ist oder ob die KI-Anwendung personenbezogene Daten in Form von In- und Output verarbeitet. Die Anforderungen des Daten-

1 Abrufbar unter https://lfd.niedersachsen.de/dsk-ki als PDF.

schutzrechts sind stets dann zu erfüllen, wenn personenbezogene Daten betroffen sind. Darüber hinaus werden im ersten Teil der Orientierungshilfe Hinweise gegeben, welche Parameter eines KI-Systems für einen datenschutzkonformen Betrieb wichtig sind.

Der zweite Teil zur Implementierung von KI-Anwendungen hebt vor allem die aus datenschutzrechtlicher Sicht erforderlichen technischen und organisatorischen Maßnahmen ab. Dazu zählen insbesondere die gegebenenfalls bestehende Pflicht zur Datenschutz-Folgenabschätzung, datenschutzfreundliche Konfigurationen der KI-Anwendung und Mitarbeiterschulungen.

Der dritte und letzte Teil zur Nutzung von KI-Anwendungen adressiert insbesondere Mitarbeitende in Unternehmen und Behörden, die die KI-Anwendung konkret nutzen. Bei der Eingabe von personenbezogenen Daten in ein KI-System sind im Rahmen der Rechtmäßigkeitsbewertung die besonderen Risiken durch die Verarbeitung in einem KI-System zu berücksichtigen. Die personenbezogenen Output-Daten müssen auf ihre Richtigkeit und Aktualität überprüft werden. Bewertungsergebnisse einer KI-Anwendung, die individuelle Entscheidungen in Bezug auf eine Person enthalten, dürfen in vielen Fällen nicht ungeprüft übernommen werden.

Fazit

KI-Systeme stellen eine neue technische Entwicklung dar. Insbesondere generative KI-Systeme weisen ein breites Spektrum an Einsatzmöglichkeiten auf. Daher kann die Orientierungshilfe Künstliche Intelligenz und Datenschutz nicht auf alle Datenschutzfragen eine Antwort enthalten. Wir haben uns durch die Mitarbeit in der Taskforce KI aktiv für diese Veröffentlichung eingesetzt, da wir in ihr eine wertvolle Hilfestellung bei der Einführung von datenschutzkonformen KI-Systemen in Unternehmen, Behörden und sonstigen Organisationen sehen.

OZG 2.0: Orientierungshilfe zum neuen Onlinezugangsgesetz I.5

Das 2024 verabschiedete OZG-Änderungsgesetz regelt unter anderem den Datenschutz bei länderübergreifenden Onlinediensten für die Bereitstellung von elektronischen Verwaltungsleistungen von Bund, Ländern und Kommunen. Mit einer Orientierungshilfe unterstützen wir Stellen, die länderübergreifende Onlinedienste betreiben oder nutzen, bei der Anwendung des Gesetzes.

Als Mitglied der Kontaktgruppe OZG 2.0 der Datenschutzkonferenz begleitet unsere Behörde schon seit langem den Gesetzgebungsprozess rund um das Onlinezugangsgesetz[1] und hat die jeweiligen Gesetzesentwürfe mehrfach kommentiert.[2] Im nun geänderten Onlinezugangsgesetz[3] war neben den Grundsatzfragen der Digitalisierung und der Finanzierungsthematik auch die seit langem erwartete datenschutzrechtliche Regelung der länderübergreifenden Onlinedienste ein wesentlicher Baustein.

Bei einem länderübergreifenden Onlinedienst handelt es sich um einen gegenüber dem „eigentlichen" Verwaltungsverfahren selbstständigen elektronischen Dienst, der der Vorbereitung des Verwaltungsverfahrens dient. Ein solcher Dienst kann beispielsweise ein elektronisches Antragsformular zur Beantragung einer Baugenehmigung sein. Dabei kann die Behörde eines Landes das Antragsformular hosten und sowohl den Baugenehmigungsbehörden des eigenen Bundeslandes als auch denen der anderen Bundesländer zur Erhebung der Antragsdaten der Antragsteller zur Verfügung stellen. In diesem Fall wird der Onlinedienst länderübergreifend betrieben.

1 Onlinezugangsgesetz vom 14. August 2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 1 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nummer 245) geändert worden ist.

2 Siehe dazu auch Tätigkeitsbericht 2023, I.9.

3 Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG) vom 19.7.2024 (BGBl. 2024 I Nummer 245).

Wesentliche Inhalte der datenschutzrechtlichen Regelung des neuen Onlinezugangsgesetzes sind insbesondere:

- Die Zuweisung der datenschutzrechtlichen Verantwortlichkeit an die den länderübergreifenden Onlinedienst betreibende Behörde[4]
- Eigene Rechtsgrundlagen für die Verarbeitung personenbezogener Daten im länderübergreifenden Onlinedienst[5]
- (Mit einer Übergangsfrist versehene) Ersetzung der Bürgerkonten der Länder durch die BundID, die zur DeutschlandID weiterentwickelt wird[6]

Da sich für die (bisherigen und neuen) Verantwortlichen mit den neuen Regelungen diverse Fragen stellen, hat unsere Behörde die Erstellung einer Orientierungshilfe der Datenschutzkonferenz initiiert und maßgeblich gestaltet. Die Datenschutzkonferenz hat die Orientierungshilfe in ihrer 108. Sitzung verabschiedet, sie ist abrufbar unter:

https://t1p.de/dsk-ozg

Die Orientierungshilfe richtet sich an Stellen, die länderübergreifende Onlinedienste nach dem OZG betreiben oder nutzen. Sie geht unter anderem auf die Rechtsgrundlagen der Verarbeitung in länderübergreifenden Onlinediensten sowie auf die datenschutzrechtliche Verantwortlichkeit bei solchen Diensten ein. Und das anhand von Beispielen aus der Praxis. Darüber hinaus thematisiert sie den Umgang mit Nutzerkonten und die Dokumentationspflichten, die mit der Verarbeitung bei länderübergreifenden Onlinediensten einhergehen.

Fazit

Mit der Orientierungshilfe möchten wir öffentlichen Stellen, die sich mit dem neuen Onlinezugangsgesetz befassen, unterstützen. In der Gesetzesanwendung kommen in den nächsten Monaten sicherlich weitere Fragen auf, die die Orientierungshilfe bislang noch nicht beantwortet hat. Wir beschäftigen uns deshalb auch weiter intensiv mit diesen Fragen und werden auf eine einheitliche Auslegung des Onlinezugangsgesetzes hinwirken.

4 § 8a Abs. 4 S. 1 OZG.
5 §§ 8a Abs. 1 bis Abs. 3 OZG, jeweils in Verbindung mit Art. 6 Abs. 1 Buchst. e, Abs. 2 und Abs. 3 S. 1 Buchst. b DS-GVO.
6 § 3 Abs. 1 S. 1 OZG, § 12 Abs. 1 OZG.

Orientierungshilfen, Beschlüsse und Entschließungen der Datenschutzkonferenz I.6

Die Datenschutzkonferenz fasst Ergebnisse ihrer Sitzungen in Entschließungen und Beschlüssen zusammen und gibt regelmäßig Orientierungshilfen zu aktuellen Datenschutzfragen heraus – im Jahr 2024 unter anderem zu Selbstauskünften bei Mietinteressenten.

Außer den in den vorigen Artikeln ausführlich beschriebenen Papieren der Datenschutzkonferenz (DSK) haben die Datenschutzbeauftragten der Länder und des Bundes 2024 weitere wichtige Informationen rund um den Datenschutz veröffentlicht. Im Folgenden haben wir die wichtigsten hervorgehoben, eine komplette Übersicht finden Sie unter https://datenschutzkonferenz-online.de in der Infothek der Datenschutzkonferenz.

Menschenzentrierte Digitalisierung in der Daseinsvorsorge

https://lfd.niedersachsen.de/dsk-digitalisierung
Die DSK appelliert an die Gesetzgeber, bei der fortschreitenden Digitalisierung des Staats faire Rahmenbedingungen für Menschen zu setzen, die keinen digitalen Zugang zu unverzichtbaren Dienstleistungen der Daseinsvorsorge haben oder nicht haben wollen.

Einholung von Selbstauskünften bei Mietinteressenten

https://lfd.niedersachsen.de/dsk-selbstauskunft
Vor der Vermietung von Wohnraum erheben Vermieter, Makler oder Hausverwaltungen bei Mietinteressenten persönliche Angaben, mit deren Hilfe sie eine Entscheidung über den Vertragsabschluss treffen. In einer Orientierungshilfe hat die DSK zusammengefasst, was erlaubt ist und was nicht.

Übermittlung personenbezogener Daten bei Asset Deals

https://lfd.niedersachsen.de/dsk-asset
Bei einem als Asset Deal ausgestalteten Unternehmensverkauf werden die Vermögenswerte und Wirtschaftsgüter an den Erwerber des Unterneh-

mens übertragen. Der Umgang mit personenbezogenen Daten bei einem solchen Verkauf hat einige Besonderheiten, die die DSK in einem Beschluss zusammengefasst hat.

Einsatz von Gesichtserkennung durch Sicherheitsbehörden

https://lfd.niedersachsen.de/dsk-gesichtserkennung
Vermehrt setzen Behörden automatisierte biometrische Gesichtserkennungssysteme im öffentlichen Raum ein. Dieser Einsatz kann einen sehr intensiven Eingriff in die Grundrechte der betroffenen Personen bedeuten. Deshalb fordert die DSK, das Sicherheitsinteresse der Allgemeinheit sorgfältig mit den Freiheitsrechten der Menschen abzuwägen.

Orientierungshilfe für Anbieter von digitalen Diensten

https://lfd.niedersachsen.de/dsk-dienste
Beim Betrieb von digitalen Diensten wie Apps und Webseiten werden häufig personenbezogene Daten verarbeitet. Außer der DSGVO müssen die Anbieter solcher Dienste das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) beachten. Hierzu gibt die Orientierungshilfe der DSK wertvolle Hinweise und bietet Hilfestellungen.

Die Datenschutzkonferenz veröffentlicht regelmäßig Beschlüsse, Entschließungen und Orientierungshilfe auf ihrer Webseite.

J Europäischer Datenschutzausschuss

J.1 Datenschutzkonforme KI-Modelle? Stellungnahme des Europäischen Datenschutzausschusses

Im Dezember 2024 hat der Europäische Datenschutzausschuss eine Stellungnahme zur Verwendung personenbezogener Daten für die Entwicklung und Einführung von KI-Modellen angenommen. Sie soll bei der datenschutzrechtlichen Bewertung des Trainings und des Einsatzes von KI-Modellen eine einheitliche Auslegung und einen einheitlichen Vollzug der Datenschutz-Grundverordnung in den Mitgliedstaaten unterstützen.

Die Stellungnahme des Europäischen Datenschutzausschusses (EDSA)[1] geht auf einen Antrag der irischen Datenschutzaufsichtsbehörde (DPC)[2] zurück. Diese hatte – sinngemäß – die folgenden Fragen gestellt:

1. Wann und unter welchen Voraussetzungen können KI-Modelle als anonym angesehen werden?
2. Unter welchen Voraussetzungen greift das berechtigte Interesse[3] als Rechtsgrundlage für die Verarbeitung personenbezogener Daten bei der Entwicklung oder Nutzung von KI-Modellen?
3. Wie wirkt es sich auf die datenschutzrechtliche Bewertung der Nutzung eines KI-Modells aus, wenn dieses KI-Modell unter Verwendung unrechtmäßig verarbeiteter personenbezogener Daten entwickelt wurde?

Die Datenschutzaufsicht Niedersachsen hat sich in dieses Verfahren intensiv eingebracht, da die konsistente Rechtsauslegung für Fragen rund um den relativ neuen Anwendungsbereich der Künstlichen Intelligenz von sehr großer praktischer Bedeutung ist.

Die Stellungnahme trifft keine Aussage über die Datenschutzkonformität konkreter KI-Modelle. Sie ist auch nicht auf bestimmte Arten von KI-Modellen wie zum Beispiel Large Language Modelle begrenzt, sondern weist

1 Abrufbar unter https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf
2 Gemäß Art. 64 Abs. 2 DSGVO.
3 Gemäß Art. 6 Abs. 1 Buchst. f DSGVO.

entsprechend der Definition von KI-Modellen in der europäischen KI-Verordnung einen weiten Anwendungsbereich auf.

Der EDSA stellt aber klar, dass vor dem Hintergrund der Fragestellungen in der Stellungnahme nur KI-Modelle betrachtet werden, die das Ergebnis eines Trainings mit personenbezogenen Daten sind.[4] Dies ist zum Beispiel in Bezug auf die auf dem Markt befindlichen Large Language Modelle bekannt, deren sehr umfassende Trainingsdatensätze im Wesentlichen aus dem Internet stammen und durch sogenanntes Web Scraping erhoben werden.[5]

Indem die datenschutzrechtlichen Anforderungen bezogen auf KI-Modelle konkretisiert und näher beschrieben werden, gibt die Stellungnahme eine Orientierungshilfe für die Beantwortung der gestellten Fragen. Hierbei ist deutlich erkennbar, dass die Kenntnisse über die eingesetzten Verfahren zum Training von Large Language Modellen in die Stellungnahme eingeflossen sind.

Personenbezug von KI-Modellen

Die erste Frage der irischen Aufsichtsbehörde zielt darauf ab, ob im KI-Modell selbst personenbezogene Daten verarbeitet werden oder der technische Vorgang der Tokenisierung bei der Entwicklung eines KI-Modells datenschutzrechtlich als Anonymisierung gewertet werden kann. Relevant wird die Antwort auf diese Frage vor allem in Bezug auf die datenschutzrechtliche Verantwortlichkeit eines Betreibers oder Nutzers eines KI-Modells.[6]

In der Stellungnahme wird hierzu im Ergebnis festgestellt, dass KI-Modelle nicht generell anonym sind, sondern der Personenbezug eines KI-Modells von Fall zu Fall zu prüfen ist.[7] Damit ein Modell anonym ist, muss es sehr

4 Siehe Rn. 26 Opinion 28/2024: "Based on the above considerations, in line with the Request, the scope of this Opinion only covers the subset of AI models that are the result of a training of such models with personal data."

5 Siehe Rn. 18 Opinion 28/2024: "Web scraping is a commonly used technique for collecting information from publicly available online sources. Information scraped from, for example, services such as news outlets, social media, forum discussions and personal websites, may contain personal data."

6 Siehe hierzu auch die Ausführungen zu Frage 3.

7 Siehe Rn. 34 Opinion 28/2024.

unwahrscheinlich sein, Personen, deren Daten zur Erstellung des Modells verwendet wurden, direkt oder indirekt zu identifizieren und personenbezogene Daten durch Abfragen aus dem Modell zu extrahieren.

Ergänzend erhält die Stellungnahme eine nicht abschließende, aber dennoch sehr umfassende Liste von Methoden für den Nachweis der Anonymität durch Verantwortliche. Insgesamt ist eine zuverlässige Anonymisierung entsprechend der Vorgaben der Datenschutz-Grundverordnung (DSGVO) sehr anspruchsvoll.

Rechtsgrundlage für das KI-Training

Die irische Aufsichtsbehörde hat weiterhin an den EDSA sinngemäß die folgende Frage formuliert:

> Wenn sich ein für die Verarbeitung Verantwortlicher auf berechtigtes Interesse als Rechtsgrundlage für die Verarbeitung personenbezogener Daten beruft, um ein KI-Modell zu erstellen, zu aktualisieren oder weiterzuentwickeln, wie sollte dieser Verantwortliche die Angemessenheit der berechtigten Interessen in Bezug auf die Verarbeitung von Third-Party- und First-Party-Daten nachweisen?

Aufgrund der Fragestellung befasst sich die Stellungnahme ausschließlich mit dem berechtigten Interesse gemäß Artikel 6 Absatz 1 Buchstabe f DSGVO, nicht aber mit den weiteren Rechtsgrundlagen gemäß Artikel 6 Absatz 1 DSGVO. Die Unterscheidung zwischen sogenannten Third-Party- und First-Party-Daten wird von der irischen Datenschutzaufsichtsbehörde ohne weitere Begründung vorgenommen. Der EDSA hat sich deshalb damit auseinandersetzen müssen.

Der EDSA stellt zunächst klar, dass die in Frage stehende Rechtsgrundlage insgesamt drei Voraussetzungen hat. Entsprechend ist eine dreistufige Prüfung vorzunehmen: erstens das berechtigte Interesse des Verantwortlichen für die Verarbeitung der personenbezogenen Daten, zweitens die Erforderlichkeit der Verarbeitung der personenbezogenen Daten und drittens überwiegende Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person.

Die Stellungnahme enthält auch eine Reihe von Kriterien, anhand derer zu beurteilen ist, ob Einzelpersonen eine bestimmte Verwendung ihrer per-

sonenbezogenen Daten vernünftigerweise erwarten können. Als Kriterien werden – erkennbar mit einem starken Bezug auf Trainingsdaten, die durch Web Scraping erlangt werden – genannt,

- ob die personenbezogenen Daten öffentlich zugänglich waren,
- die Art der Beziehung zwischen der Person und dem Verantwortlichen,
- die Art des Dienstes,
- der Kontext, in dem die personenbezogenen Daten erhoben wurden,
- die Quelle, aus der die Daten erhoben wurden – hier fließt die Unterscheidung zwischen First- und Third-Party-Daten ein –,
- die möglichen weiteren Verwendungen des KI-Modells und
- ob Einzelpersonen tatsächlich wissen, dass ihre personenbezogenen Daten online sind.

Die Ausführungen des EDSA weisen nur indirekt auf den Spagat hin, den Verantwortliche zur Beachtung der Rechtsgrundlage anscheinend bewältigen müssen. Einerseits werden insbesondere beim Training von generativen KI-Modellen sehr große Trainingsdatensätze benötigt.[8] In vielen Fällen enthalten diese Datensätze im erheblichen Umfang personenbezogene Daten. Allein aufgrund des Umfangs wird der Verantwortliche allenfalls eine pauschalierte Prüfung der Rechtsgrundlage vornehmen können. Gleichzeitig benennt der EDSA Bewertungskriterien, die eine Einzelfallbetrachtung erfordern.

Anscheinend um dieses Dilemma aufzulösen, führt der EDSA ergänzend aus, dass bei einem negativen Abwägungstest Abhilfemaßnahmen zur Begrenzung der negativen Auswirkungen auf den Einzelnen vorgenommen werden können. Die Stellungnahme enthält eine nicht abschließende Liste von Beispielen für solche Abhilfemaßnahmen. Diese können technischer Natur sein, aber auch Einzelpersonen die Ausübung ihrer Rechte erleichtern oder die Transparenz erhöhen.

Es dürfen aber nur Maßnahmen berücksichtigt werden, die nicht der Erfüllung weiterer Anforderungen der DSGVO dienen, wie zum Beispiel die Erfüllung der Informationspflichten[9], sondern überobligatorisch vorgenommen werden.

8 Beispielsweise stellt der Webcrawler Common Crawl einen 250 Billionen Webseiten umfassenden Datensatz zur allgemeinen Nutzung bereit, der regelmäßig nach Herstellerangaben für das Training von generativen KI-Modellen genutzt wurde.

9 Gemäß Art. 13 DSGVO.

Datenschutzkonforme Nutzung datenschutzwidrig trainierter KI-Modelle

Die letzte Frage der irischen Aufsichtsbehörde steht unter der Prämisse, dass KI-Modelle unter Verstoß gegen Datenschutzvorschriften trainiert worden sind. Welche Auswirkungen hat dies auf den datenschutzkonformen Betrieb oder die datenschutzkonforme Nutzung dieses KI-Modells, je nachdem ob, das KI-Modell anonym ist oder das KI-Modell personenbezogen ist?

Der EDSA stellt fest, dass das rechtswidrige Training jedenfalls dann bei der Prüfung der Datenschutzkonformität des Betriebs des KI-Modells folgenlos bleiben wird, wenn das KI-Modell zuverlässig anonymisiert worden ist. In allen anderen Fällen wird davon ausgegangen, dass sich die Unrechtmäßigkeit des Trainings auf die Rechtmäßigkeit des Einsatzes auswirken kann. Letztlich ist dies im Einzelfall zu prüfen.

Ergänzende Hinweise

Die beantragte Stellungnahme des EDSA beschränkt sich im Wesentlichen auf die Beantwortung der konkreten Fragen. Es wird ausdrücklich darauf hingewiesen, dass für die Prüfung der Datenschutzkonformität sowohl des Trainings als auch des Betriebs von KI-Modellen weitere datenschutzrechtliche Aspekte eine wichtige Rolle spielen können. Hierzu zählen insbesondere

- die rechtmäßige Verarbeitung besonderer Kategorien personenbezogener Daten[10],
- KI-basierte, automatische Entscheidungsfindungen einschließlich Profiling[11],
- die Anforderung der Kompatibilität bei einer Zweckänderung insbesondere vom Training eines KI-Modells zum konkreten Betrieb[12],
- die Datenschutz-Folgenabschätzung[13] und
- die Anforderungen von Datenschutz by Design und by Default.[14]

10 Gemäß Art. 9 DSGVO.
11 Gemäß Art. 21 DSGVO.
12 Gemäß Art. 6 Abs. 4 DSGVO.
13 Gemäß Art. 35 DSGVO.
14 Gemäß Art. 25 DSGVO.

Fazit

Der EDSA hat unter hohem Zeitdruck zu sehr wichtigen und praxisrelevanten Datenschutzfragen bei KI-Modellen eine umfassende Stellungnahme erarbeitet. Die von der Praxis erhoffte Rechtssicherheit für KI-Modelle wird dadurch nicht herbeigeführt.

Erwartungsgemäß können die gestellten Fragen nicht nach dem Schema ja oder nein beantwortet werden. Dennoch ist es dem EDSA gelungen, die datenschutzrechtlichen Vorgaben KI-spezifisch zu konkretisieren und eine wertvolle Hilfestellung zu geben.

Es ist Aufgabe der Aufsichtsbehörden, diesen Meinungsbildungs- und Abstimmungsprozess bezogen auf neue, komplexe und vielfach noch im Entwicklungsstadium befindliche KI-Modelle fortzusetzen. Je prägnanter die datenschutzrechtlichen Gestaltungsanforderungen an KI-Modelle formuliert werden können, desto eher werden sie umgesetzt werden.

J.2 Datenschutzkonformes Geschäftsmodell? Stellungnahme des EDSA zu „Consent or Pay"-Modellen

Im April 2024 verabschiedete der Europäische Datenschutzausschuss (EDSA) eine Stellungnahme zu „Zustimmungs- oder Bezahlungsmodellen", die von großen Online-Plattformen eingesetzt werden. Kern der Ausführungen sind die datenschutzrechtlichen Anforderungen für wirksame Einwilligungen in die Verarbeitung personenbezogener Daten zum Zwecke personalisierter Werbung.

Viele Online-Angebote sind dazu übergegangen, sogenannte „Consent or Pay"-Modelle zur Finanzierung ihrer Dienstleistungen einzuführen. In Deutschland wird dieses Geschäftsmodell häufig als Pur-Abo-Modell bezeichnet.[1] In der Regel stellen die Seitenbetreiber die Nutzer vor die Wahl, entweder eine Gebühr für die Online-Angebote zu entrichten oder in die Nutzung ihrer personenbezogenen Daten für personalisierte Werbung einzuwilligen.

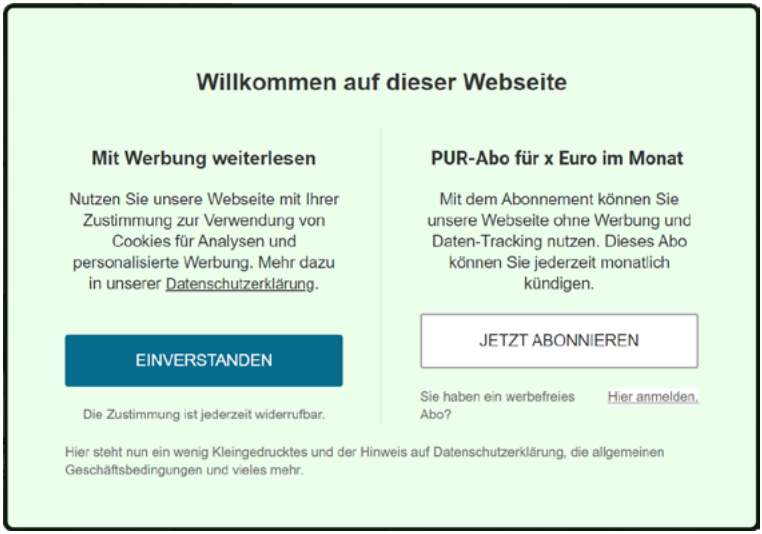
Bei dieser Werbeform analysieren Anbieter häufig über sehr lange Zeiträume Daten zum individuellen Surf-Verhalten und nutzen diese, um individualisierte Werbung auszuspielen. Wer beispielsweise häufig nach Ernährungstipps in einem Online-Magazin sucht, bekommt dann mit hoher Wahrscheinlichkeit Werbung für Diätprodukte angezeigt. Bei diesen Geschäftsmodellen ist sehr fraglich, ob die Anforderungen der Datenschutz-Grundverordnung (DSGVO) an die Freiwilligkeit der Einwilligung erfüllt werden können.

Vor diesem Hintergrund erarbeitete der EDSA auf Antrag mehrerer europäischer Datenschutzbehörden[2] eine insgesamt 50 Seiten umfassende Stellungnahme zur Gültigkeit der Einwilligung zur Verarbeitung personenbezogener Daten zum Zweck personalisierter Werbung im Rahmen von

1 Vgl. Beschluss der DSK, Bewertung von Pur-Abo-Modellen auf Websites, 22.3.2023, https://t1p.de/dsk-pur (Kurzlink zum PDF).

2 Gemäß Art. 64 Abs. 2 DSGVO kann jede Aufsichtsbehörde beim EDSA beantragen, eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat zu prüfen und Stellung zu nehmen.

„Consent or Pay"-Modellen.[3] Die Stellungnahme bezieht sich auf große Online-Plattformen, die Bewertungsmaßstäbe sind aber weitgehend auf alle Webseiten mit „Consent or Pay"-Modellen übertragbar.



Beispiel für ein Einwilligungsbanner mit Pur-Abo-Modell.

In seiner Stellungnahme stellt der EDSA klar, dass es für große Online-Plattformen in den meisten Fällen nicht möglich sein wird, die Anforderungen an eine gültige Einwilligung zu erfüllen, wenn sie den Nutzern vor die Wahl stellen, in die Verarbeitung personenbezogener Daten für personalisierter Werbung einzuwilligen oder ein kostenpflichtiges Abonnement abzuschließen. Dies sollte aus Sicht des EDSA kein Standardmodell sein.

Für die Nutzer sollte eine weitere kostenlose Alternative ohne personalisierte Werbung zur Verfügung gestellt werden. Dies könne beispielsweise die Nutzung mit rein kontextbasierter Werbung sein, welche nicht die Verarbeitung personenbezogener Daten der Nutzer erfordert. Weiterhin müsse die Einwilligung „freiwillig erteilt" werden, um wirksam zu sein.

3 Die Stellungnahme des EDSA ist verfügbar unter https://t1p.de/edsa-pay1 (Kurzlink zum PDF), eine Zusammenfassung als Pressemitteilung unter https://t1p.de/edsa-pay2 (Kurzlink).

Der EDSA betont in seiner Stellungnahme, dass ein etwaiges Entgelt nicht so hoch sein dürfe, dass Nutzer effektiv daran gehindert werden, eine freie Wahl zu treffen. Ferner könnten Nachteile entstehen, wenn Nutzer, die weder einwilligen noch ein Entgelt zahlen, vom Dienst ausgeschlossen werden, insbesondere In Fällen, in denen „der Dienst für die Teilhabe am gesellschaftlichen Leben oder den Zugang zu beruflichen Netzwerken eine herausragende oder entscheidende Rolle" spielt.

Mindestens in Bezug auf die großen Online-Plattformen sei ein „Consent or Pay"-Modell daher schon aus diesem Gesichtspunkt heraus grundsätzlich ungeeignet, von nicht zahlenden Nutzern eine wirksame Einwilligung für die Verarbeitung einzuholen.

Fazit

Mit seiner begrüßenswerten Stellungnahme zu „Consent or Pay"-Modellen hat der EDSA die Wahlfreiheit der Betroffenen gestärkt, die Voraussetzung für wirksame Einwilligungen in die Verarbeitung ihrer personenbezogenen Daten für Zwecke personalisierter Werbung ist.

Gleichzeitig bestätigt der EDSA den bereits im März 2023 von der Datenschutzkonferenz gefassten Beschluss zur Bewertung von Pur-Abo-Modellen auf Websites. Die großen Online-Plattformen werden ihre Geschäftsmodelle entsprechend anpassen müssen.

Leitfaden zu Datenschutzfällen mit strategischer Bedeutung für Europa J.3

Im November 2024 verabschiedete der Europäische Datenschutzausschuss einen überarbeiteten Leitfaden zu Fällen von strategischer Bedeutung für den gesamten Geltungsbereich des europäischen Datenschutzrechts. Mit seiner Hilfe sollen die nationalen Datenschutzbehörden besser, schneller und effizienter zusammenarbeiten.

Bei grenzüberschreitenden Datenverarbeitungen findet die Aufsicht und Durchsetzung der Datenschutz-Grundverordnung (DSGVO) als Kooperationsverfahren statt.[1] Das ist beispielsweise der Fall, wenn sich das Angebot eines Online-Shops an Kundinnen und Kunden in mehreren Mitgliedsstaaten der EU richtet. In solchen Verfahren arbeiten die für den jeweiligen Fall zuständigen europäischen Aufsichtsbehörden eng zusammen. Die Datenschutzaufsicht am Ort der europäischen Hauptniederlassung eines Verantwortlichen übernimmt die Rolle der federführenden Aufsichtsbehörde und führt die Ermittlung des Sachverhalts durch. In den ersten Jahren der Anwendung der DSGVO hat sich gezeigt, dass insbesondere in sehr komplexen Fällen die Zusammenarbeit der Aufsichtsbehörden im Kooperationsverfahren noch weiter verbessert werden kann.

Vor diesem Hintergrund hatten sich im April 2022 in Wien die Mitglieder des Europäischen Datenschutzausschusses (EDSA) darauf geeinigt, die Zusammenarbeit in strategisch bedeutsamen Fällen zu verbessern.[2] Fälle von strategischer Bedeutung sind Fälle, in denen ein strukturelles oder wiederkehrendes Problem in mehreren Mitgliedstaaten besteht. Das ist insbesondere dann der Fall, wenn es eine große Anzahl von Betroffenen oder eine große Anzahl von Beschwerden in mehreren Mitgliedstaaten gibt.

1 Gemäß Art. 60 DSGVO.

2 Ausführlich dazu siehe Tätigkeitsbericht 2022, C.1.

Wegen der europaweiten Relevanz wurde im Sommer 2022 ein unverbindlicher, interner Leitfaden zur Auswahl von Fällen strategischer Bedeutung verabschiedet.[3]

Umsetzung eines Auftrages des EDSA

Im Berichtszeitraum haben wir in unserer Funktion als Ländervertretung in der sogenannten Enforcement Subgroup des EDSA gemeinsam mit der Bundesbeauftragten für den Datenschutz einen Teil für den Leitfaden entwickelt, der den eigentlichen Prozess der Zusammenarbeit in grenzüberschreitenden Fällen von strategischer Bedeutung beschreibt. Diese Arbeitsgruppe fördert die kohärente Anwendung der Abhilfebefugnisse der DSGVO und verbessert dadurch die Durchsetzung der Verordnung in der Praxis.[4] Nach der Konsensfindung in der Enforcement Subgroup hat das Plenum des EDSA das überarbeitete Papier im November 2024 verabschiedet.

Der neue Teil des Leitfadens enthält Empfehlungen für die praktische Gestaltung und den Ablauf des Verfahrens. Außerdem stellt er allgemeine Verfahrensprinzipien zusammen, denen die beteiligten Aufsichtsbehörden bei der Bearbeitung strategischer Fälle folgen sollten – und durch die die gemeinsamen Ermittlungen effizienter und schneller werden sollen.

3 Abrufbar unter https://t1p.de/edsa-leitfaden (Kurzlink).

4 Die Arbeit in der Enforcement Subgroup haben wir ausführlich im Tätigkeitsbericht 2021, C.4, beschrieben.

Stellungnahme zur Evaluation der DSGVO J.4

Im Jahr 2024 hat sich unsere Behörde an einer Stellungnahme des Europäischen Datenschutzausschusses zur Evaluation der Datenschutz-Grundverordnung durch die EU-Kommission beteiligt.

Die EU-Kommission ist verpflichtet, alle vier Jahre in einem Bericht an das Europäische Parlament und den Europäischen Rat in einem Bericht die Datenschutz-Grundverordnung (DSGVO) zu bewerten und zu überprüfen.[1] Nach einem ersten Bericht im Jahr 2020 hat die EU-Kommission im Juli 2024 den zweiten vorgelegt.[2]

Der Evaluationsbericht kommt zu einem gemischten Fazit. Die Kommission bewertet einerseits positiv, dass die Datenschutzbehörden sich zunehmend bereit gezeigt haben, die in der DSGVO vorgesehenen Instrumente für die grenzüberschreitende Zusammenarbeit zu nutzen. Die Durchsetzungstätigkeit der Datenschutzbehörden habe in den letzten Jahren erheblich zugenommen, unter anderem durch die Verhängung erheblicher Geldbußen in bedeutsamen Fällen gegen multinationale Technologieriesen.

Andererseits fordert die Kommission die Datenschutzbehörden und den Europäischen Datenschutzausschuss (EDSA) auf, präzise, praktische und gut verständliche Leitlinien zur Anwendung der DSGVO bereitzustellen, die Antworten auf konkrete Probleme geben. Diese Leitlinien sollten auch für Personen in kleinen und mittelständischen Unternehmen ohne juristische Ausbildung leicht verständlich sein.

Stellungnahme des EDSA

Nach der Veröffentlichung des Evaluationsberichts der EU-Kommission beauftragte der EDSA eine Arbeitsgruppe, den Entwurf einer Stellungnahme zu erarbeiten. Wir haben in dieser Arbeitsgruppe mitgewirkt.

In seiner im Dezember 2024 verabschiedeten Stellungnahme fordert der EDSA Rechtssicherheit und Kohärenz der europäischen digitalen Gesetz-

1 Vgl. Art. 97 Abs. 1 DSGVO.
2 Abrufbar unter https://t1p.de/eu-dsgvo2 (Kurzlink).

gebung mit der DSGVO.[3] Aus Sicht des EDSA müsse das Zusammenspiel zwischen DSGVO und anderen digitalen EU-Rechtsakten geklärt werden, insbesondere mit der KI-Verordnung oder Rechtsakten aus der EU-Datenstrategie oder dem Paket „Digitale Dienste". Außerdem befürwortet der EDSA die rechtsgebietsübergreifende Kooperation der Datenschutzbehörden mit anderen Behörden.

Der EDSA unterstreicht in seiner Stellungnahme, dass angesichts immer komplexerer Herausforderungen und zusätzlicher Zuständigkeiten Bedarf an zusätzlichen finanziellen und personellen Ressourcen bei den Aufsichtsbehörden und dem EDSA besteht. Schließlich kündigt der EDSA an, die Erstellung von Inhalten zu intensivieren, die auch für Nicht-Experten und kleine und mittelständische Unternehmen verständlich sind.

Fazit

Der EDSA hat in seiner Stellungnahme zum zweiten Bericht der EU-Kommission zur Evaluation der DSGVO zutreffend auf die große Bedeutung des Zusammenspiels der DSGVO mit anderen digitalen EU-Rechtsakten und den Austausch mit anderen Behörden hingewiesen. Als Reaktion auf die sich daraus ergebenden Herausforderungen hat der EDSA Ende 2024 entschieden, eine „Cross-Regulatory Interplay and Cooperation Expert Subgroup" (CIC ESG) einzurichten und erarbeitet Leitlinien zum Zusammenspiel der KI-Verordnung mit dem EU-Datenschutzrecht sowie – gemeinsam mit der Europäischen Kommission – Leitlinien zum Zusammenspiel des Digital Markets Acts mit der DSGVO. Das ist vor dem Hintergrund der aktuellen Entwicklungen zu begrüßen und soll dazu beitragen, dass die unterschiedlichen Rechtsakte besser verstanden werden und im Ergebnis besser ineinandergreifen.

3 Statement 6/2024 on the Second Report on the Application of the General Data Protection Regulation – Fostering Cross-Regulatory Consistency and Cooperation vom 3.12.2024, abrufbar unter https://www.edpb.europa.eu

EDSA nimmt Stellung zur geplanten Verfahrensordnung für bessere Zusammenarbeit der Aufsichtsbehörden J.5

Die Europäische Union arbeitet an einer Verordnung, um die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden zu verbessern und Aspekte des Verfahrens zu harmonisieren. Im laufenden Gesetzgebungsverfahren hat der EDSA Stellung genommen, um den beteiligten EU-Organen seine Perspektive auf den Gesetzentwurf zu vermitteln.

Die europäischen Datenschutzaufsichtsbehörden arbeiten bei grenzüberschreitenden Datenverarbeitungen im Kooperationsverfahren eng zusammen.[1] Allerdings hat in der Vergangenheit die lange Dauer der Verfahren grenzüberschreitender Datenverarbeitungen für Kritik gesorgt. Vor diesem Hintergrund hatte der Europäische Datenschutzausschuss (EDSA) im Herbst 2022 eine Liste von Verfahrensregelungen aufgestellt, die im EU-Recht harmonisiert werden sollten, um die Zusammenarbeit der Aufsichtsbehörden im Kooperationsverfahren zu verbessern.

Bisheriger Verlauf des Gesetzgebungsverfahrens

Die Europäische Kommission hat positiv auf diese Vorschläge des EDSA für harmonisierte Verfahrensregelungen reagiert und im Juli 2023 einen Vorschlag für eine Verfahrensverordnung vorgelegt.[2] Nachdem der EDSA und der Europäische Datenschutzbeauftragte (EDPS) auf den Vorschlag der Europäischen Kommission mit einer Gemeinsamen Stellungnahme reagiert hatten[3], haben sowohl das Europäische Parlament als auch der Rat der Europäischen Union umfangreiche Änderungsvorschläge, die wesentliche Vorschläge des EDSA aufgreifen, vorgelegt.

1 Gemäß Art. 60 DSGVO.
2 Siehe Tätigkeitsbericht 2023, I.11.
3 EDSA-EDSB Gemeinsame Stellungnahme 01/2023 vom 19.09.2023, abrufbar unter https://t1p.de/edsa-verfahrensordnung (Kurzlink).

Ende 2024 hat der Trilog begonnen, also die informellen Verhandlungen zwischen der Europäischen Kommission, dem Europäischen Parlament und dem Rat der Europäischen Union. Diese Beratungen haben das Ziel, möglichst rasch eine Einigung zwischen den am Gesetzgebungsprozess beteiligten EU-Organen herbeizuführen und das Gesetzgebungsverfahren auf diese Art und Weise zu beschleunigen.

Um den am Trilog beteiligten Institutionen die Perspektive des EDSA zum Vorschlag und den Änderungsvorschlägen zu vermitteln, hat dieser im Anschluss an die Änderungen, die das Europäische Parlament und der Rat beim Entwurf der Verfahrensverordnung gefordert haben, eine eigene Erklärung veröffentlicht.[4] An der Ausarbeitung dieser Erklärung hat sich unsere Behörde beteiligt.

Erklärung des EDSA

Der EDSA begrüßt in seiner Erklärung grundsätzlich die vom Europäischen Parlament und Rat vorgenommenen Änderungen. Zugleich weist er darauf hin, dass die Einführung neuer Verfahrensschritte und zusätzlicher Aufgaben der Aufsichtsbehörden zusätzliche Ressourcen bei diesen erfordern wird. Daher fordert er den EU-Gesetzgeber, die Europäische Kommission und die Mitgliedstaaten auf, sicherzustellen, dass bei den Aufsichtsbehörden genügend Ressourcen zur Verfügung stehen.

Der EDSA begrüßt, dass sowohl das Europäische Parlament als auch der Rat die in der Gemeinsamen Stellungnahme des EDSA und des Europäischen Datenschutzbeauftragten enthaltenen Anmerkungen zu den Verfahrensfristen berücksichtigt haben. Insbesondere begrüßt der EDSA die Einführung zusätzlicher Fristen durch den Rat, betont jedoch, dass diese Fristen realistisch sein sollten, damit diese in der Praxis eingehalten werden können.

In Bezug auf maßgebliche und begründete Einsprüche begrüßt der EDSA einige der Änderungsvorschläge des Europäischen Parlamentes und des Rates. Der EDSA betont, dass es für betroffenen Aufsichtsbehörden weiterhin möglich sein sollte, Einspruch gegen alle faktischen und rechtli-

4 Statement 4/2024 on the recent legislative developments on the Draft Regulation laying down additional procedural rules for the enforcement of the GDPR vom 07.10.2024, abrufbar unter https://t1p.de/edsa-statement (Kurzlink).

chen Elemente der Akte zu erheben. Vor diesem Hintergrund bekräftigt der EDSA seine Auffassung, dass Artikel 18 des Vorschlags, wonach ein Einspruch einer betroffenen Aufsichtsbehörde den Umfang der Anschuldigungen nicht durch zusätzliche Vorwürfe ändern darf, aus dem endgültigen Text der neuen Verordnung komplett gestrichen werden sollte.

Bezüglich des Vorschlags des Europäischen Parlamentes, eine gemeinsame Fallakte einzuführen, in die grundsätzlich alle Verfahrensbeteiligten Einsicht haben, wird die Zielsetzung der Herstellung größerer Transparenz begrüßt. Gleichzeitig wird jedoch darauf hingewiesen, dass die Einführung einer gemeinsamen Fallakte, wie sie vom Europäischen Parlament vorgeschlagen wird, komplexe Änderungen der auf europäischer und nationaler Ebene verwendeten Dokumentenverwaltungs- und Kommunikationssysteme erfordern würde.

Fazit

Der bisherige Verlauf des Gesetzgebungsverfahrens gibt Anlass zur Hoffnung, dass die zukünftige Verfahrensverordnung tatsächlich zu einer Verbesserung der Zusammenarbeit der Aufsichtsbehörden im Kooperationsverfahren bei grenzüberschreitenden Datenverarbeitungen führen wird. Eine solche Verbesserung würde den Schutz der personenbezogenen Daten der Bürgerinnen und Bürger in Europa spürbar stärken.

K Urteile im Datenschutzrecht

Entwicklung der Rechtsprechung im Datenschutzrecht

Im Jahr 2024 ergingen mehrere höchstrichterliche Entscheidungen zu Auslegungsfragen der Datenschutz-Grundverordnung. Die Urteile betreffen ganz unterschiedliche Themen und Fragestellungen: von Schadensersatz bis zu den Aufgaben der Aufsichtsbehörden.

Der Europäische Gerichtshof (EuGH) befasst sich vor allem im Wege von Vorabentscheidungsersuchen[1] nationaler Gerichte mit der Datenschutz-Grundverordnung (DSGVO). Die in diesem Zusammenhang erlassenen Urteile sind Einzelfallentscheidungen, die aber auch allgemeingültige Aussagen zur Anwendung der DSGVO beinhalten. Daneben entschied auch das Bundesverwaltungsgericht (BVerwG) im letzten Jahr in einer wesentlichen Datenschutzfrage.

DSGVO und Parlamente (C-33/22)

Bereits am 16. Januar 2024 stellte der EuGH in einem Urteil klar, dass die DSGVO auch auf parlamentarische Untersuchungsausschüsse Anwendung findet. Mehr zu dem Urteil lesen Sie in Kapitel G.6.6.

Personenbezug von Zeichenfolgen (C-604/22)

Der EuGH befasste sich in seinem Urteil vom 7. März 2024 mit der schwierigen Frage des Personenbezugs von nicht unmittelbar mit einer Person verbundenen Daten. In dem Fall handelte es sich um eine aus einer Kombination von Buchstaben und Zeichen erstellten Zeichenfolge, welche ein Branchenverband von Werbeunternehmen aus den Präferenzen von Internetnutzerinnen und -nutzern bezüglich ihrer Einwilligung in Werbung erstellt. Die dem Verband angeschlossenen Unternehmen konnten so aus der Zeichenfolge entnehmen, in welche Verarbeitungen von personenbezogenen Daten zu Werbezwecken die Nutzerin oder der Nutzer einer Webseite eingewilligt, beziehungsweise wogegen sie oder er Widerspruch ein-

1 Nach Artikel 267 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV).

gelegt hatte. Da hier die Zeichenfolge immer zusammen mit der IP-Adresse einer Nutzerin oder eines Nutzers übermittelt wurde, war eine Identifikation der einzelnen Person möglich.

Der EuGH bestätigte den Personenbezug dieser Zeichenfolge im Sinne des Artikel 4 Nummer 1 DSGVO. Insbesondere sah es der EuGH als unerheblich an, dass der Branchenverband als Ersteller der Zeichenfolge selbst keinen unmittelbaren Zugang zu den IP-Adressen der Nutzer hatte. Die objektiv bestehende Möglichkeit einer Identifizierung genügte hier nach Ansicht des EuGH.

Wir stimmen mit dem EuGH überein, dass es bei der Bestimmung der Personenbeziehbarkeit von Daten nicht nur auf die bereits beim Verantwortlichen vorhandenen Mittel ankommen kann, sondern auch die Möglichkeit berücksichtigt werden muss, weitergehende Informationen zur Identifizierung einer Person erlangen zu können.

Anordnung einer Löschung von Amts wegen (C-46/23)

In einem weiteren Urteil entschied der EuGH am 14. März 2024, dass die Datenschutzaufsichtsbehörden auch von Amts wegen ohne Antrag der betroffenen Person die Löschung unrechtmäßig verarbeiteter personenbezogener Daten anordnen dürfen. In diesem Verfahren ging es um eine behördliche Zusammenstellung in einer Datenbank von Personen, die von der Corona-Pandemie betroffen waren, zur Koordinierung finanzieller Hilfen.

Die betroffenen Personen waren allerdings weder über die Verwendung ihrer Daten noch über den Zweck der Datenbank informiert worden. Die daraufhin ergangene Löschungsanordnung durch die ungarische Aufsichtsbehörde sah der EuGH allein aufgrund des Verstoßes gegen die DSGVO als rechtmäßig an, ein entsprechender Antrag jeder betroffenen Person war nicht erforderlich. Die Möglichkeit zur Anordnung einer Löschung beruhe auf Artikel 58 Absatz 2 Buchstaben d und g DSGVO.

In Fällen, in denen die betroffene Person keine Kenntnis von einer Verarbeitung ihrer Daten hat, sei es zur Gewährleistung der wirksamen Durchsetzung der DSGVO unerlässlich, dass die Aufsichtsbehörde auch ohne Mitwirkung der betroffenen Person eine Datenlöschung anordnen dürfe. Wir begrüßen das Urteil als Stärkung unserer Befugnisse als Aufsichtsbehörde und als praxisnahe Lösung in den vom EuGH dargestellten Fällen.

Schadensersatz (C-741/21, C-687/21, C-182/22 und C-189/22)

In verschiedenen Urteilen setzte sich der EuGH mit Fragen der Auslegung des Artikel 82 DSGVO zum Schadensersatz nach einem Datenschutzverstoß auseinander.

Mit Urteil vom 11. April 2024 (C-741/21) entschied der EuGH, dass ein Verstoß gegen die Bestimmungen der DSGVO für sich genommen nicht genügt, um einen „immateriellen Schaden" im Sinne des Schadensersatzanspruchs nach Artikel 82 DSGVO darzustellen. Vielmehr muss der Anspruchsteller auch nachweisen, dass ihm durch den Verstoß ein Schaden entstanden ist.[2] Auch stellte der EuGH klar, dass sich ein für die Datenverarbeitung Verantwortlicher nach einem eingetretenen Schaden durch einen Datenschutzverstoß nicht dadurch von einer Haftung befreien kann, indem er geltend macht, der Schaden sei durch ein Fehlverhalten eines Mitarbeiters verursacht worden. Der Verantwortliche bleibt hier haftbar für im Rahmen der durch ihn veranlassten Datenverarbeitung entstandenen Schäden.

Im Verfahren C-687/21 entschied der EuGH mit Urteil vom 25. Januar 2024 weiter, dass die Schwere eines Verstoßes gegen Datenschutzbestimmungen im Rahmen der Bemessung eines möglichen Schadensersatzanspruchs nach Artikel 82 DSGVO jedenfalls nicht zu berücksichtigen sei. Denn der Schadensersatzanspruch solle eine Ausgleichsfunktion erfüllen und keine Straffunktion. Zugleich bestätigte das Gericht, dass der Anspruchsteller nicht nur den Datenschutzverstoß nachweisen muss, sondern auch den ihm dadurch konkret entstandenen Schaden. Die bloße Vermutung des Missbrauchs der eigenen personenbezogenen Daten durch einen Datenschutzverstoß genüge nicht zur Annahme eines immateriellen Schadens.

Zuletzt bestätigte der EuGH am 20. Juni 2024 (C-182/22 und C-189/22) seine Auffassung zur bloßen Ausgleichsfunktion des Schadensersatzanspruchs. Bei der Berechnung des Schadensersatzes ist dem Urteil zufolge die Schwere des Verstoßes unerheblich, lediglich der tatsächlich erlittene Schaden ist maßgeblich.

2 An den Nachweis des immateriellen Schadens sind aber keine allzu hohen Anforderungen zu stellen. Der EuGH setzt weder eine Erheblichkeitsschwelle voraus (Urteil vom 04.05.2023 – C-300/21) noch einen spürbaren Nachteil (Urteil vom 14.12.2023 – C-456/22).

Pflichten der Aufsichtsbehörde bei Verstoß (C-768/21)

In seiner Entscheidung vom 26. September 2024 stellte der EuGH fest, dass nicht jede festgestellte Verletzung des Schutzes personenbezogener Daten die Aufsichtsbehörde zur Ergreifung einer Abhilfemaßnahme nach Artikel 58 DSGVO verpflichtet. Der EuGH räumt den Aufsichtsbehörden insoweit ein Ermessen ein, ob und wenn ja mit welcher Abhilfemaßnahme sie auf einen Verstoß reagieren.

Allerdings sei dieses Ermessen begrenzt durch das Erfordernis, ein gleichmäßiges hohes Datenschutzniveau in der EU herzustellen. Die Aufsichtsbehörde sei daher dann zu einem Einschreiten verpflichtet, wenn das Ergreifen einer Abhilfemaßnahme unter Berücksichtigung der konkreten Umstände des Einzelfalles geeignet, erforderlich und verhältnismäßig ist, um dem festgestellten Verstoß abzuhelfen und die Einhaltung der DSGVO zu gewährleisten.

Ausnahmsweise dürfe die Aufsichtsbehörde vom Ergreifen einer Abhilfemaßnahme absehen, obwohl eine Datenschutzverletzung vorliegt, wenn dies nach den besonderen Umständen des Einzelfalles angemessen erscheint. Diese Entscheidung des EuGH stützt unsere bisherige Praxis im Umgang mit Verstößen und konkreten Abhilfemaßnahmen.

Grundsatz der Datenminimierung (C-446/21)

Mit Urteil vom 04. Oktober 2024 entschied der EuGH über ein Vorabentscheidungsersuchen im Zusammenhang mit der Datenspeicherung durch Meta. Nach Auffassung des EuGH bewirkt der Grundsatz der „Datenminimierung“ in Artikel 5 Absatz 1 Buchstabe c DSGVO, dass eine zeitlich und inhaltlich unbegrenzte Erhebung und Verarbeitung von Daten zu einer bestimmten Person durch einen Verantwortlichen wie den Betreiber eines sozialen Netzwerkes für Zwecke der zielgerichteten Werbung nicht zulässig ist.

Das Gericht wies insbesondere darauf hin, dass der Zeitraum der Erhebung personenbezogener Daten auf das in Bezug auf den Zweck absolut Notwendige zu beschränken ist. Vor diesem Hintergrund sei eine zeitlich unbegrenzte Erhebung und Verarbeitung von Daten durch ein soziales Netzwerk zu Zwecken der personalisierten Werbung jedenfalls unverhält-

nismäßig. Ebenso sei die allgemeine und unterschiedslose Datenerhebung unzulässig, da der Verantwortliche jedenfalls von der Erhebung solcher Daten absehen muss, welche für die Erreichung des Zwecks nicht unbedingt notwendig sind.

Allgemeine Rechtsgrundlage für Datenverarbeitungen und Zweckfestlegung (BVerwG 6 C 8.22)

Das BVerwG hatte sich mit der Frage auseinanderzusetzen, ob die ganz allgemein formulierte Ermächtigungsgrundlage nach Paragraf 3 Bundesdatenschutzgesetz (BDSG) für Datenverarbeitungen durch öffentliche Stellen des Bundes zur Erfüllung von Aufgaben im öffentlichen Interesse den Anforderungen an eine DSGVO-konforme Rechtsgrundlage genügt.

Nach Ansicht des BVerwG ist diese Regelung als „Brückennorm" anzusehen, welche auf Grundlage des Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e DSGVO zusammen mit fachspezifischen Regelungen dann als ausreichende Eingriffsgrundlage für eine Verarbeitung personenbezogener Daten durch öffentliche Stellen angesehen werden kann, wenn die Verarbeitung eine nur geringe Eingriffstiefe aufweist. Unter diesen Voraussetzungen sei nicht für jede einzelne Verarbeitung durch eine öffentliche Stelle zur Erfüllung ihrer Aufgaben ein spezifisches Gesetz erforderlich und die Regelung des Paragraf 3 BDSG als Generalklausel ausreichend. Erfolgt dagegen ein schwerwiegender Eingriff in die Grundrechte einer betroffenen Person, ist eine an den Prinzipien der Normklarheit und Verhältnismäßigkeit ausgerichtete Ermächtigungsgrundlage erforderlich. Diese Rechtsprechung kann aus unserer Sicht auf die Anwendbarkeit der in Paragraf 3 Niedersächsisches Datenschutzgesetz (NDSG) gleichlautend formulierten Generalklausel für die Datenverarbeitung durch öffentliche Stellen des Landes übertragen werden.

Das BVerwG entschied in diesem Verfahren weiter, dass die Zwecke, zu denen die Daten erhoben werden, durch den Verantwortlichen im Rahmen der behördlichen Selbstorganisation und nach Maßgabe der fachrechtlichen Anforderungen eigenständig festgelegt werden. Eine Überprüfung dieser konkreten Zweckfestlegung etwa am Maßstab des Grundsatzes der Datenminimierung nach Artikel 5 Absatz 1 Buchstabe c DSGVO erfolge dann nicht mehr.

Diese Entscheidung des BVerwG ist kritisch zu sehen, da die Datenschutzgrundsätze des Artikel 5 Absatz 1 DSGVO allgemein gelten und sich der Verantwortliche durch eine einmal getroffene selbstständige Festlegung der Zwecke der Datenverarbeitung nicht jeglicher Prüfung dieser Grundsätze entziehen darf.

Bedeutung für die Praxis

Die höchstrichterliche Rechtsprechung von EuGH und BVerwG ist für die praktische Anwendung der Datenschutzregelungen von besonderem Wert. Insbesondere vor dem Hintergrund des Erfordernisses einer einheitlichen Auslegung konkreter Regelungen durch Aufsichtsbehörden und Verantwortliche sind Entwicklungen in der Rechtsprechung stets zu verfolgen und zu beachten.

L Öffentlichkeitsarbeit

L.1 Schwerpunkt Datenschutz- und Medienkompetenz ausgebaut

Für das Jahr 2024 haben wir uns als niedersächsische Datenschutzaufsichtsbehörde einen Schwerpunkt zur Förderung der Datenschutz- und Medienkompetenz gesetzt. Anlass ist die zunehmende Bedeutung eines bewussten und sicheren Umgangs mit digitalen Medien, insbesondere bei Kindern und Jugendlichen.

Zahlreiche Institutionen in Niedersachsen engagieren sich im Bereich der Medienkompetenz, darunter die Landesschulbehörde, die Landeszentrale für politische Bildung und das Netzwerk Medienkompetenz Niedersachsen. Auch der Landesbeauftragte für den Datenschutz Niedersachsen bringt in diesem Bereich Expertise für den Datenschutz ein. Der Fokus liegt auf dem sicheren Umgang mit persönlichen Daten im Internet und in sozialen Medien sowie Cybergefahren wie Deepfakes und Cybermobbing.

Wie wichtig dies ist, bestätigt eine aktuelle Studie im Auftrag des Digitalverbands Bitkom: 92 Prozent der Kinder und Jugendlichen ab sechs Jahren nutzen das Internet, die meisten täglich über mehrere Stunden.[1] Mit zunehmendem Alter steigt auch der Anteil der selbstständigen Internetnutzung, während die elterliche Kontrolle abnimmt. Dies zeigt, dass junge Menschen frühzeitig für Datenschutzthemen sensibilisiert werden müssen, um sich sicher und kritisch in der digitalen Welt bewegen zu können.

Maßnahmen und Umsetzung

Die Landesdatenschutzbehörde bietet ab 2025 flächendeckend Unterrichtseinheiten zur Datenschutzkompetenz an Schulen an. Ziel ist es, den Schülerinnen und Schülern praxisnahes Wissen zu vermitteln, damit sie sich sicher und verantwortungsbewusst im digitalen Raum bewegen können. Bereits 2024 beteiligte sich die Behörde an der Initiative „Datenschutz geht zur Schule“, die bundesweit Schülerinnen und Schüler für Daten-

1 https://www.bitkom.org/Presse/Presseinformation/Kinder-Jugendliche-taeglich-zwei-Stunden-Smartphone

schutzthemen sensibilisiert. Dieses Engagement wird nun mit eigenen Schulungsinhalten ausgeweitet.

Die Vermittlung von Datenschutzkompetenz geht dabei über rein technische Aspekte hinaus. Neben praktischen Tipps zu sicheren Passwörtern und Privatsphäre-Einstellungen geht es auch um ein grundlegendes Verständnis dafür, wie große Digitalkonzerne mit Nutzerdaten umgehen und welche gesellschaftlichen Auswirkungen das hat. Datenschutz ist nicht nur eine technische, sondern auch eine ethische und gesellschaftliche Herausforderung.

Kooperationen und langfristige Strategie

Um das Thema Datenschutzkompetenz nachhaltig im Bildungssystem zu verankern, baut unsere Behörde die Zusammenarbeit mit Schulen, Bildungsbehörden und weiteren Akteuren im Bereich der Medienbildung aus.

Durch regelmäßige Evaluierung und Anpassung der Lehrinhalte stellen wir sicher, dass die Bildungsangebote stets den aktuellen Entwicklungen im Bereich Datenschutz und Digitalisierung entsprechen. Über die Fortschritte informieren wir regelmäßig unseren Auftraggeber, den Niedersächsischen Landtag.

Mit diesem Schwerpunkt leistet die niedersächsische Datenschutzbehörde einen wichtigen Beitrag zur digitalen Bildung und stärkt das Bewusstsein für Datenschutz als zentrale Kompetenz im digitalen Zeitalter.

An einer Zusammenarbeit interessierte Schulen und Schulträger in Niedersachsen können sich gerne an uns über medienkompetenz@lfd.niedersachsen.de wenden.

L.2 LfD Niedersachsen auf Mastodon: Datenschutzaufsicht informiert auch per datenschutzfreundlichem sozialem Netzwerk

Seit 2024 informiert der Landesbeauftragte für den Datenschutz Niedersachsen, Denis Lehmkemper, und seine Behörde auch über das soziale Netzwerk Mastodon. Über den Kurznachrichtendienst informieren wir rund um unsere Veröffentlichungen und aktuelle Themen und aus den Bereichen Datenschutz und Datensicherheit.

Seit Juni 2024 ist die Datenschutzaufsicht Niedersachsen auf dem sozialen Netzwerk Mastodon aktiv. Den Account des LfD Niedersachsen unter dem Handle social.bund.de/@datenschutz_nds betreibt die Datenschutzaufsicht auf der Mastodon-Instanz der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Auf dieser Instanz – einem Teil der dezentralen Serverstruktur von Mastodon – sind außer der BfDI (@bfdi) unter anderem die Datenschutzaufsichten von Berlin (@BlnBDI) und Rheinland-Pfalz (@lfdi_rlp) vertreten. Hier informieren und kommentieren wir rund um die Themen Datenschutz und Datensicherheit.

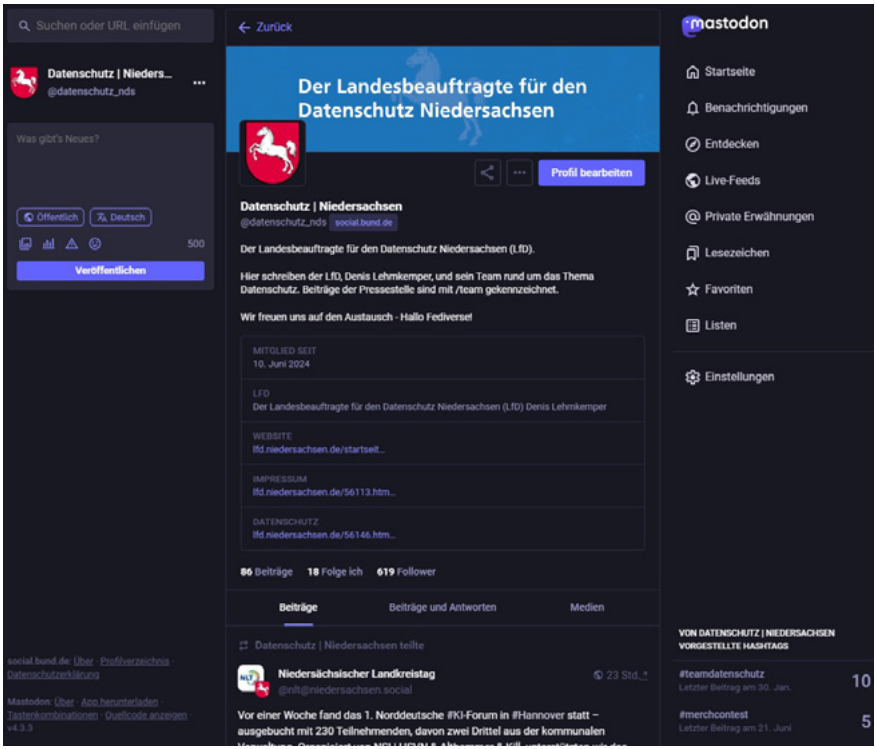
Mit unserer Präsenz auf Mastodon wollen wir zeigen, dass der direkte Austausch mit den Bürgerinnen und Bürgern über soziale Netzwerke auch ohne den Einsatz datenschutzrechtlich problematischer Plattformen möglich ist. Während die Geschäftsmodelle der großen werbefinanzierten Social Media-Plattformen üblicherweise Profilbildung und Tracking der Nutzerinnen und Nutzer zu Werbezwecken beinhalten und die so generierten Nutzerdaten mitunter auch weiterverkauft werden, gibt es inzwischen jedoch datenschutzfreundliche Alternativen.

Alternative Social Media

Mastodon ist so eine datenschutzfreundliche Alternative zu Kurznachrichtendiensten wie X, ehemals Twitter. Das soziale Netzwerk ist dezentral über Instanzen organisiert. Jeder kann eine eigene Instanz betreiben oder sich

einer bestehenden Instanz anschließen. Eine Kommunikation ist über die Grenzen der Instanzen hinweg möglich. Der Quellcode von Mastodon ist offen und frei verfügbar.

A1 – Screenshot des Mastodon Accounts des LfD



Im sogenannten Fediverse, der weltweiten Verbindung der Instanzen zu einem Netzwerk, können sich die Mastodon-Nutzerinnen und -Nutzer miteinander austauschen und Inhalte teilen.

Kanal der erweiterten Öffentlichkeitsarbeit

Neben den klassischen Kanälen der Presse- und Öffentlichkeitsarbeit kommt auch der Präsenz in der Online-Sphäre sozialer Netzwerke eine wachsende Bedeutung zu, um sich an öffentlichen Diskursen zu beteiligen. Hier können neue Zielgruppen angesprochen werden. So kann neben

dem reinen Verbreiten von Informationen mit dem Ziel Prävention auch der konstruktive Austausch und Diskurs mit Nutzerinnen und Nutzern gepflegt werden. In solche Debatten bringen wir uns mit unseren Positionen ein und wollen damit auch anderen staatlichen und nichtstaatlichen Akteuren zeigen, dass und wie datenschutzkonforme Nutzung von Social Media möglich ist.

Veranstaltungen, Workshops und Vorträge L.3

Vertreterinnen und Vertreter unserer Behörde haben im Jahr 2024 auf Dutzenden von Veranstaltungen und Workshops über Datenschutzthemen informiert. Besonders gefragt war unsere Expertise in den Bereichen Künstliche Intelligenz, Beschäftigtendatenschutz und digitale Souveränität.

Der Landesbeauftragte für den Datenschutz Denis Lehmkemper bei einer Diskussion zur KI-Verordnung auf dem German Legal Tech Summit in Hannover.

Datenschutz und Künstliche Intelligenz – nicht wenige Experten sind skeptisch, ob das überhaupt miteinander funktionieren kann. Der europäische Gesetzgeber hat jedenfalls klargestellt, dass die Datenschutz-Grundverordnung von der 2024 in Kraft getretenen KI-Verordnung unberührt bleibt.[1] Doch wie lässt sich die Datenschutz-Grundverordnung (DSGVO) auf das Training von KI-Systemen anwenden, bei dem Milliarden von Texten und Bildern verarbeitet werden? Und welche Behörden sollen künftig die Re-

1 Art. 2 Abs. 7 KI-VO.

gulierung von KI-Systemen überwachen? Diese und weitere offene Fragen diskutieren wir mit den anderen Datenschutzbehörden und mit Expertinnen und Experten aus der niedersächsischen Wirtschaft, Forschung und Politik.[2]

Da Unternehmen und öffentliche Stellen in Niedersachsen bereits mit KI-Systemen arbeiten oder zumindest experimentieren, haben wir im Jahr 2024 besonders viele Anfragen zu diesem Thema erhalten. Der Landesbeauftragte für den Datenschutz hat in seinen Vorträgen auf die besonderen Herausforderungen hingewiesen, die insbesondere im Hinblick auf die Trainingsdaten von KI-Systemen, die Korrektheit des Outputs und die Rechte der Betroffenen bestehen.[3]

Ein weiterer Schwerpunkt unserer Behörde und damit auch unserer Workshops im Jahr 2024 war der Beschäftigtendatenschutz. Zum einen leiten wir innerhalb der Datenschutzkonferenz den Arbeitskreis Beschäftigtendatenschutz[4], zum anderen verfolgen wir als Datenschutzaufsicht Niedersachsen mehrere Fälle rund um die Mitarbeiterüberwachung, die bundesweit für Aufsehen gesorgt haben.

In unseren Workshops ging es vor allem um die Möglichkeiten der digitalen Überwachung am Arbeitsplatz, neuerdings auch durch KI-Systeme. Wir haben aber auch praktische Tipps gegeben, wie man als Unternehmen gemeinsam mit den Mitarbeiterinnen und Mitarbeitern digitale Prozesse datenschutzkonform einführen kann. Unsere Hoffnung, dass der Gesetzgeber 2024 dafür endlich klarere Rahmenbedingungen durch ein nationales Beschäftigtendatenschutzgesetz einführt, hat sich nicht erfüllt.[5]

Ebenfalls gefragt war unsere Einschätzung rund um die digitale Souveränität. Nicht zuletzt aufgrund der aktuellen politischen Entwicklungen wächst der Wunsch in öffentlichen Stellen, aber auch in Unternehmen, sich nicht zu sehr von den großen Big-Tech-Unternehmen aus den USA abhängig zu machen. Auf der anderen Seite ist der Druck groß, aus Bequemlichkeit auf gängige international verbreitete Cloud-Dienste zu setzen, auch wenn es um den Umgang mit sensiblen Kunden- oder Beschäftigtendaten geht. In unseren Vorträgen zu diesem Thema haben wir versucht, den Verantwort-

2 Siehe Kapitel E.
3 Siehe Kapitel G.2.1.
4 Siehe Kapitel I.1.
5 Siehe Kapitel I.1.

lichen eine praxisnahe Orientierungshilfe zu geben und sie zum aktuellen Stand bei nationalen Projekten wie der Delos-Cloud zu informieren.

Immer wieder bitten uns Unternehmen und Verbände, ihnen einen Einblick in die Arbeit der niedersächsischen Datenschutzaufsicht zu geben. Solche Anfragen freuen uns besonders, da immer noch eine gewisse Angst vor der Aufsicht besteht. In solchen Workshops versuchen wir aufzuzeigen, warum sich eine gute und schnelle Zusammenarbeit für Unternehmen auszahlt. Dazu haben Referentinnen und Referenten aus unserem Haus im vergangenen Jahr beispielsweise bei den Handelskammern, in der Hotelbranche, bei Versicherungen und bei Unternehmensverbänden referiert.

Der LfD Niedersachsen Denis Lehmkemper hält eine Keynote zu Arbeitnehmerdatenschutz auf dem Euroforum Datenschutzkongress 2024.

L.4 Informationsmaterial: Von Abmahnungen bis Zensus

Auf unserer Homepage veröffentlichen wir regelmäßig FAQ, Infoblätter und Handreichungen zu aktuellen Datenschutzfragen. In diesem Jahr haben wir unter anderem Beiträge zum Datenschutz im Straßenverkehr, in Kommunen und im Gesundheitsbereich erstellt beziehungsweise aktualisiert.

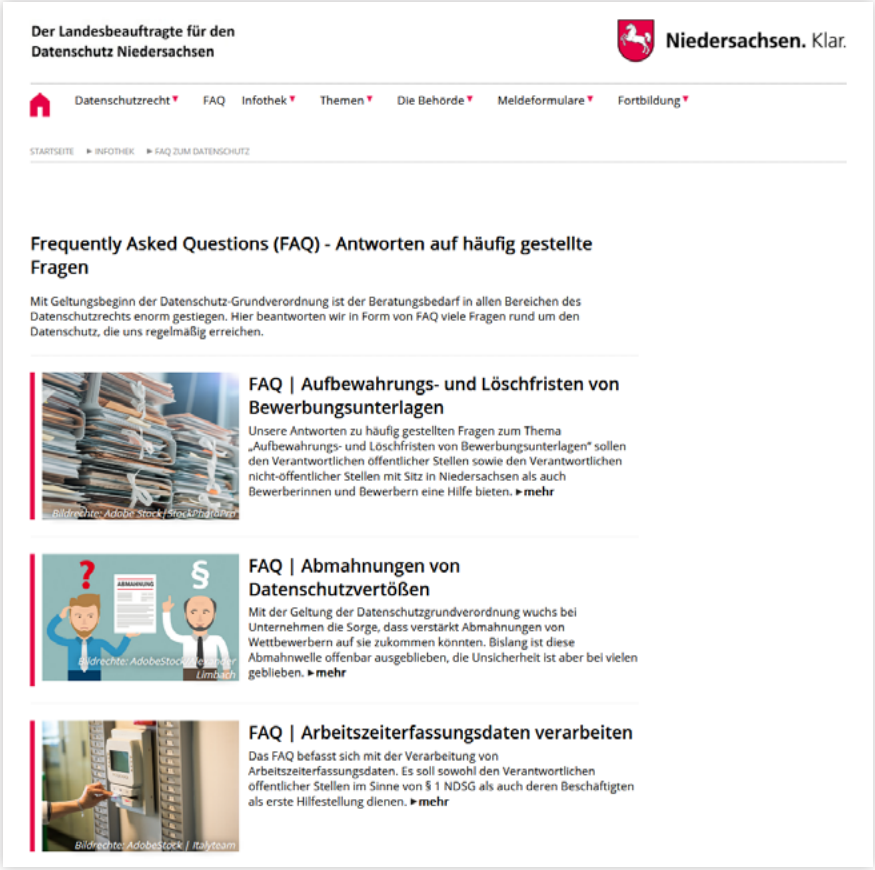
Regelmäßig erhalten wir Fragen von Bürgerinnen und Bürgern, Unternehmen und öffentlichen Stellen zum Datenschutz. Die Antworten zu den häufigsten Fragen veröffentlichen wir auf unserer Webseite, ebenso Checklisten, Orientierungshilfen und weiteres Informationsmaterial. Zu den über 20 FAQ auf lfd.niedersachsen.de/faq finden Sie im Folgenden einen Überblick über neue und aktualisierte Beiträge.

FAQ zu Dashcams im Straßenverkehr

https://www.lfd.niedersachsen.de/193497.html
Bei unserer Behörde gehen häufig Beschwerden zu Dashcams im Straßenverkehr ein, denen wir in jedem Fall nachgehen und bei rechtswidriger Nutzung auch Bußgelder erteilen. In unseren FAQ erklären wir, in welchen Fällen die Aufzeichnung zulässig sein kann und welche Kosten bei einem Verstoß drohen.

FAQ zum Datenschutz im Gesundheitsbereich

https://www.lfd.niedersachsen.de/229071.html
Verantwortliche in Praxen, Krankenhäusern, Pflegediensten oder anderen Bereichen des Gesundheitswesens stehen vor besonderen Herausforderungen im Datenschutz. Denn Gesundheitsdaten gehören in der DSGVO zu den besonderen Kategorien personenbezogener Daten, bei denen strenge Regeln gelten. Dazu beantworten wir auf unserer Webseite 39 Fragen und stellen darüber hinaus ein Muster für Antworten auf Transparenz- und Informationspflichten in Arztpraxen zur Verfügung.



Über 20 Datenschutz-FAQs von Abmahnungen bis Zensus finden Sie auf unserer Homepage.

FAQ zum kommunalen Datenschutz

https://www.lfd.niedersachsen.de/206875.html

Die niedersächsischen Kommunen verarbeiten unterschiedlichste personenbezogene Daten der Bürgerinnen und Bürger. Wir haben auf unserer Webseite ausführlich dargelegt, welche Pflichten die Kommunen dabei haben. Dazu gehören auch die Fragen, was bei einer Auskunft nach Artikel 15 der Datenschutz-Grundverordnung (DSGVO) oder bei Gewährung von Akteneinsicht zu beachten ist.

FAQ zum TDDDG

https://www.lfd.niedersachsen.de/206449.html
Im Mai 2024 wurde das TTDSG[1] in TDDDG umbenannt. TDDDG steht für Telekommunikation-Digitale-Dienste-Datenschutzgesetz, es enthält spezifische Datenschutzvorschriften für Anbieter von Telekommunikationsdiensten (z. B. Telefon- und Internetanbieter) und digitale Dienste (z. B. Webseitenbetreiber). Das Gesetz betrifft also auch Privatpersonen, die eine Webseite oder App betreiben.

FAQ zur Arbeitszeiterfassung in öffentlichen Stellen

https://www.lfd.niedersachsen.de/237890.html
Für die Arbeitszeiterfassung in öffentlichen Stellen in Niedersachsen gilt zum einen die DSGVO, zum anderen sind das Niedersächsische Datenschutzgesetz sowie das Niedersächsische Beamtengesetz anzuwenden. Unsere kürzlich aktualisierten FAQ setzen sich unter anderem mit der Frage auseinander, was überhaupt zu den Arbeitszeiterfassungsdaten zählt und wer Zugang zu diesen Daten erhalten darf.

Sollten Sie zu einem datenschutzrechtlichen Thema, das für Sie von Interesse ist, bei uns oder auf der Seite der DSK kein Material finden, schreiben Sie uns gerne über poststelle@lfd.niedersachsen.de an.

1 TTDSG steht für Telekommunikation-Telemedien-Datenschutzgesetz.

Abkürzungsverzeichnis

Abs.	Absatz (juristische Abkürzung)
AK	Arbeitskreis
Art.	Artikel (juristische Abkürzung)
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
BKAG	Bundeskriminalamtsgesetz
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
Buchst.	Buchstabe/Unterpunkt (juristische Abkürzung)
CRAI	Center of Research and Development of Trustworthy AI Applications for Midsized Companies
DFKI	Deutsches Forschungszentrum für Künstliche Intelligenz
DPA	Data Protection Addendum
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DsIN	Datenschutzinstitut Niedersachsen
DSK	Datenschutzkonferenz
DO LT	Datenschutzordnung des Niedersächsischen Landtags
DVS	Deutsche Verwaltungscloud-Strategie
EDPS	Europäische(r) Datenschutzbeauftragte(r)
EDSA	Europäischer Datenschutzausschuss
EHW	ermittlungsbezogene Hinweise
EinwV	Einwilligungsverwaltungsverordnung
ePA	elektronische Patientenakte
EuGH	Europäischer Gerichtshof
FAQ	Frequently Asked Questions
FWU	Institut für Film und Bild in Wissenschaft und Unterricht
GG	Grundgesetz
GGO	Gemeinsame Geschäftsordnung der Landesregierung und der Ministerien in Niedersachsen
GDNG	Gesundheitsdatennutzungsgesetz

ID	Identifikationsnummer
IfSG	Infektionsschutzgesetz
JI-Richtlinie	EU-Datenschutzrichtlinie zur Zusammenarbeit im Bereich Justiz und Inneres
KI	Künstliche Intelligenz
KIM	Kommunikation im Medizinwesen
KI-VO	Verordnung über Künstliche Intelligenz der EU
LfD	Landesbeauftragter für den Datenschutz
LKA	Landeskriminalamt
LLMs	Large Language Models
MDM	Mobile Device Management
NBrandSchG	Niedersächsisches Brandschutzgesetz
NDSG	Niedersächsisches Datenschutzgesetz
NKatSG	Niedersächsischen Katastrophenschutzgesetz
NOOTS	National Once-Only-Technical-Systems
NPOG	Niedersächsisches Polizei- und Ordnungsbehördengesetz
NSchG	Niedersächsisches Schulgesetz
NSI	Niedersächsisches Studieninstitut für kommunale Verwaltung
OWiG	Ordnungswidrigkeitengesetz
OZG	Onlinezugangsgesetz
PHW	Personengebundene Hinweise
RDZ-TKÜ	Rechen- und Dienstleistungszentrum zur Telekommunikationsüberwachung
SDM	Standard-Datenschutzmodell
SGB	Sozialgesetzbuch
StPO	Strafprozessordnung
TKÜ	Telekommunikationsüberwachung
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
TOM	Technische und organisatorische Maßnahme
VG	Verwaltungsgericht
VIDIS	Vermittlungsdienst für das digitale Identitätsmanagement in Schulen
VwVfG	Verwaltungsverfahrensgesetz
VO	Verordnung
ZAWAS	Prozess zur Auswahl angemessener Sicherungsmaßnahmen