Der Landesbeauftragte für den Datenschutz Niedersachsen

Tätigkeitsbericht 2023

Niedersachsen

Der Landesbeauftragte für den Datenschutz Niedersachsen

29. Tätigkeitsbericht 2023

Impressum

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

Verantwortlich
Denis Lehmkemper

Redaktion
Achim Barczok, Marius Engelskirchen

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

Bildnachweis
Seite 8: Daniel George
Seiten 37, 38, 47, 58, 179, 201, 204: LfD Niedersachsen
Alle anderen: Adobe Stock

Das Titelbild zeigt den Leuchtturm Obereversand an der Wurster Nordseeküste zwischen Bremerhaven und Cuxhaven.

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

Inhalt

A Vorwort

Für den Datenschutz war das Jahr 2023 ein Besonderes: Die Datenschutz-Grundverordnung feierte als europäisches Erfolgsmodell ihren fünften Geburtstag. Die Europäische Union hat die EU-Digitalstrategie konsequent vorangetrieben, die ganz sicher Einfluss auf die Arbeit der Datenschutzaufsichten in den nächsten Jahren haben wird. Wichtige Urteile des Europäischen Gerichtshofs festigten und bestätigten unsere Datenschutzpraxis in vielen Punkten, in einigen stellen sie uns aber auch vor künftige, neue Aufgaben. Wir haben 2023 einen starken Europäischen Datenschutzausschuss erlebt, dessen Mitglieder sich gemeinsam und erfolgreich mit Themen wie der Bußgeldpraxis und der Sanktionierung europaweit agierender Digitalkonzerne befasst haben.

Auch für Niedersachsen hat sich etwas geändert. Am 15. September durfte ich mein neues Amt als der, als Ihr Landesbeauftragter für den Datenschutz antreten. Vom ersten Tag an erlebe ich hier eine oberste Landesbehörde, deren knapp 60 Mitarbeiterinnen und Mitarbeiter mit großer Expertise und Leidenschaft für den Datenschutz in Niedersachsen eintreten. Ich bin stolz auf diese kompetente Datenschutzaufsicht, die Haltung zeigt, sich konstruktiv und lösungsorientiert für die Rechte der Bürgerinnen und Bürger einsetzt und den Gesetzgeber berät. Mich begeistert die Arbeit mit den Kolleginnen und Kollegen jeden Tag aufs Neue.

Besonders danken möchte ich an dieser Stelle meinem Stellvertreter Dr. Christoph Lahmann, der die Behörde in der Übergangszeit bis zu meinem Amtsantritt souverän und kollegial geführt hat – und mir so einen schnellen und reibungslosen Einstieg ermöglichte. Gemeinsam mit den Kolleginnen und Kollegen haben wir schon einiges auf den Weg gebracht.

Das ist auch nötig, denn Zeit zum Verschnaufen gibt es 2024 in diesem Amt nicht. Im sechsten Jahr der DSGVO sind die Herausforderungen für

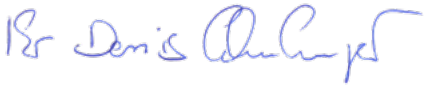
den Datenschutz und für uns als Aufsicht immens. Der technische Fortschritt und die Digitalisierung in Unternehmen und öffentlichen Stellen nehmen deutlich an Fahrt auf. Künstliche Intelligenz, vernetzte Welten, die Digitalisierung in Wirtschaft, Verwaltung und im Gesundheitssystem: Bei all diesen Entwicklungen sind wir in der Pflicht, die Rechte und Bedürfnisse der Bürgerinnen und Bürger sowie der Unternehmen in Niedersachsen zu achten und zu schützen. Wir tun dies konstruktiv, als Mahner und Ratgeber – und wir tun es gern.

Um den Datenschutz in Niedersachsen voranzubringen, müssen Gesetzgeber, Unternehmen, Aufsicht und Gesellschaft effektiv zusammenarbeiten und werden so die Zukunft gestalten. Mich freut es, dass ich in dieser Hinsicht in den ersten Monaten meiner Amtszeit bereits viele gute Gespräche – mit Mitgliedern des Niedersächsischen Landtages und der Landesregierung, aber beispielsweise auch mit Unternehmensverbänden, Wissenschaft und Gesellschaft – führen und einiges vereinbaren konnte, was auch die kommenden Jahre unserer Arbeit prägen wird.

Gleichwohl muss ich feststellen, dass sich einige Unternehmen bei ihren Projekten zu wenig Gedanken um den Datenschutz machen. Beratungsanfragen zu Gesetzesvorhaben oder Initiativen gehen bisweilen reichlich spät in unserem Haus ein. Meine sechs Empfehlungen auf den folgenden Seiten sind deshalb ein eindringlicher Appell an Landtag, Landesregierung und Unternehmen, für einen wirksamen und starken Datenschutz einzutreten.

Sie sind nicht das einzige, das im 29. Tätigkeitsbericht anders ist als in den Berichten zuvor: Wir haben das Layout modernisiert und den Schwerpunkt der Artikel stärker auf unser Wirken in Niedersachsen ausgerichtet. Zusätzlich finden Sie in diesem Bericht ein längeres Schlaglicht über Künstliche Intelligenz – ein Thema, das uns im vergangenen Jahr stark beschäftigt hat und das auch sicher 2024 einen Schwerpunkt bilden wird. Zudem wollen wir mehr Einblick in die Arbeit vor Ort geben, mit der wir als Datenschutzbehörde die Rechte der Bürgerinnen und Bürger in Niedersachsen stärken.

Ich wünsche Ihnen viele spannende Erkenntnisse bei der Lektüre unseres 29. Tätigkeitsberichts.



Denis Lehmkemper

B Empfehlungen des Landesbeauftragten für den Datenschutz Niedersachsen

An den Niedersächsischen Landtag

1. Der verantwortungsvolle Umgang mit personenbezogenen Daten jeder Art benötigt einen klaren Rechtsrahmen, der Möglichkeiten eröffnet, aber auch Grenzen setzt. Füllen Sie konsequent die sichtbaren Lücken bei diesen Rechtsgrundlagen – einige davon haben uns auch in dieser Berichtsperiode beschäftigt und sind in den folgenden Kapiteln unseres Tätigkeitsberichts dargestellt.

2. Insbesondere sehen wir Lücken bei den Rechtsgrundlagen für den Einsatz der Künstlichen Intelligenz in den niedersächsischen Verwaltungen. Hier hat die Entwicklung rasant an Fahrt aufgenommen. Dabei basiert die Künstliche Intelligenz auf Algorithmen, die grundsätzlich neu strukturiert sind und geänderten Regeln folgen. Daraus entsteht eine hoch innovative, aber auch hoch riskante Form der Datenverarbeitung, die der Gesetzgeber bis vor Kurzem noch gar nicht im Blick haben konnte, um den Schutz der Persönlichkeitsrechte Betroffener zu wahren. Umso dringlicher ist es, sich nunmehr damit zu befassen und so zu einem guten Datenschutzniveau zu kommen.

An die Niedersächsische Landesregierung

3. Die datenschutzkonforme Umsetzung von Vorhaben der Landesregierung steigert die Akzeptanz dieser Vorhaben bei Bürgerinnen und Bürgern. Die frühzeitige Einbindung des Landesbeauftragten für den Datenschutz bei allen relevanten Projekten des Landes unter Vorlage eines zumindest vorläufigen Datenschutzkonzeptes ist dabei zwingende Voraussetzung.

4. Videoüberwachung im privaten Bereich beschäftigt nach wie vor viele Bürgerinnen und Bürger. Am Markt sind günstige Überwachungskameras in großer Zahl verfügbar und dies befördert unserer Erfahrung nach

den eher sorglosen Umgang damit. Wir fordern die Landesregierung dazu auf, mit einer niedersächsische Bundesratsinitiative zu „Beipackzetteln" für Überwachungskameras die Bürgerinnen und Bürger beim rechtskonformen Einsatz von Videokameras auf Privatgrundstücken zu unterstützen.

An die niedersächsischen Unternehmen

5. Die Datenschutz-Grundverordnung fordert von Verantwortlichen bei der Einführung neuer Systeme Datenschutz durch Technikgestaltung („Data Protection by Design") und datenschutzfreundliche Voreinstellungen („Data Protection by Default"). Um das zu erleichtern, sollten Hersteller ihre elektronischen Produkte von Beginn an so entwickeln, dass sie datenschutzrechtliche Grundsätze erfüllen und Verantwortliche sie leicht und gut angeleitet datenschutzfreundlich einsetzen können.
6. Ein hohes Datenschutzniveau ist gerade in Deutschland für die Kundinnen und Kunden ein Beweis für ein besonders sorgfältig arbeitendes und solides Unternehmen. Außerdem tragen die dafür nötigen technisch-organisatorischen Maßnahmen zum Schutz gegen die zunehmende Gefahr von Cyber-Angriffen bei. Wir fordern die niedersächsischen Unternehmen deshalb dazu auf, ihre Prozesse datenschutzkonform aufzustellen und in den innerbetrieblichen Datenschutz zu investieren.

C Das Wichtigste in Kürze

Wir blicken im Datenschutz auf ein Jahr zurück, das von der guten Zusammenarbeit in Europa geprägt war – und von rasanten Entwicklungen in der Künstlichen Intelligenz. Nach Prüfungen in Fitnessstudios, Immobilienbüros und Schulen konnte unsere Behörde im Jahr 2023 zudem diverse Datenschutzmängel abstellen. Die Anzahl der Pannenmeldungen und Beschwerden von Bürgerinnen und Bürgern blieb auf einem hohen Niveau.

Mit dem Erfolg von Chatbots wie ChatGPT von OpenAI ist der Beratungsbedarf zu Künstlicher Intelligenz im Land immens gestiegen und damit ein Thema ins Rampenlicht gerückt, mit dem wir uns schon lange befassen.

Unter anderem haben deutsche Aufsichtsbehörden mit einer datenschutzrechtlichen Bewertung von ChatGPT begonnen und OpenAI dazu mit einem umfassenden Fragekatalog konfrontiert. Auf zahlreichen Veranstaltungen haben wir proaktiv über KI im Kontext von Datenschutz diskutiert und die Folgen der europäischen KI-Verordnung für die niedersächsische Verwaltung, für Unternehmen und unsere Arbeit analysiert. KI und KI-Systeme werden uns als anspruchsvolles datenschutzrechtliches Thema in den kommenden Jahren in vielen Bereichen begleiten.

Gute Zusammenarbeit auf europäischer Ebene

Viel erreicht haben wir 2023 gemeinsam mit unseren Partnerbehörden auf nationaler und europäischer Ebene. Erwähnenswert sind hier die Streitbeilegungsverfahren, die zu hohen Bußgeldern gegenüber Meta und TikTok geführt haben. So verhängte die irische Datenschutzbehörde infolge eines Streitbeilegungsverfahrens des Europäischen Datenschutzausschusses (EDSA) ein Bußgeld von 1,2 Milliarden Euro gegen Meta für die beim Betrieb des Facebook-Netzwerks stattfindenden Datenexporte in die USA. Für TikTok legte die irische Aufsichtsbehörde ein Bußgeld von 345 Millionen Euro für den Einsatz manipulativer Designs von Bedienoberflächen fest.

Die europäischen Aufsichtsbehörden stellten damit klar, dass auch global agierende Big-Tech-Unternehmen in Europa den Datenschutz einhalten müssen und andernfalls hohe Strafen riskieren. Die niedersächsische Datenschutzaufsicht war und ist im Rahmen der Enforcement Subgroup des EDSA maßgeblich an diesen Verfahren beteiligt.

Zwar sind Datenübermittlungen in die USA aufgrund des 2023 von der EU-Kommission gefassten Angemessenheitsbeschlusses für den Datenschutzrahmen EU-USA neu zu bewerten. Wir empfehlen dennoch, bereits umgesetzte oder eingeleitete Strategien wie zum Beispiel zu digitaler Souveränität unbedingt weiter zu verfolgen, um eine möglichst umfassende Kontrolle über die verarbeiteten Daten dauerhaft sicherstellen zu können.

Prüfungen decken zahlreiche Mängel auf

In diversen Prüfungen stießen wir im Jahr 2023 auf teils schwere datenschutzrechtliche Verstöße und Mängel in niedersächsischen Unternehmen. Das gilt insbesondere für Branchen, auf die wir aufgrund häufiger Beschwerden von Bürgerinnen und Bürgern aufmerksam geworden waren und die wir deshalb genauer unter die Lupe genommen haben. Auffällig waren Zahl und Schwere der Verstöße bei zehn Fitnessstudio-Unternehmen, die sich unter anderem in unzulässiger Videoüberwachung in Arbeits- und Trainingsbereichen widerspiegelten. In einigen Fällen haben wir deshalb Bußgeldverfahren eingeleitet.

Erhebliche Defizite stellten wir zudem bei unseren Kontrollen von Immobilienmaklern und Wohnungsunternehmen fest. Viele der geprüften Unternehmen der Immobilienwirtschaft verarbeiteten personenbezogene Daten von Mietinteressentinnen und -interessenten rechtswidrig. Unternehmen fragten von den Wohnungssuchenden als Voraussetzung für die Teilnahme an Besichtigungen viele nicht relevante Daten ab und speicherten teilweise insbesondere Kontaktdaten länger als erforderlich.

Es gibt aber auch Positives zu berichten: So konnten wir den von uns geprüften Apotheken gute Ergebnisse bei der datenschutzkonformen Verarbeitung von Corona- und Kundendaten bescheinigen. Und in einer Nachprüfung in Schulen stellten wir vor Ort fest, dass diverse Mängel abgestellt wurden. Damit steht fest, dass unsere Prüfungen zu einem höheren Datenschutzniveau in Niedersachsen beigetragen haben.

Pur-Abo-Modelle auf Webseiten

Mit sehr gemischten Gefühlen beobachten wir den Trend, dass viele Anbieter auf ihren Seiten Pur-Abo-Modelle einrichten. Im Hinblick auf Medienwebseiten werten wir dies als Folge der länderübergreifenden Prüfung der Webseiten von Medienhäusern. In diesen Modellen bezahlen die Nutzerinnen und Nutzer den Abopreis dafür, dass sie – teils einige, teils alle – Inhalte ohne Tracking sowie profilbasierte und individualisierte Werbung lesen können. Alternativ bleibt eine kostenfreie Nutzung zwar weiterhin möglich – jedoch nur, wenn sie stattdessen „mit ihren Daten" bezahlen und einwilligen, dass die Unternehmen profilbasierte und individualisierte Werbung ausspielen. Die Datenschutzkonferenz hat für diese Pur-Abo-Modelle klare Anforderungen formuliert. Umsetzungsdefizite zeigen sich vor allem bei den Anforderungen an Transparenz und Auswahlmöglichkeiten bei der Einwilligung.

Beschwerden und Bußgelder: Schwerpunkt Videoüberwachung

Besonders intensiv beschäftigte unsere Expertinnen und Experten die Prüfung der über 2.200 Beschwerden von Bürgerinnen und Bürgern, die uns 2023 erreicht haben und die wir mit hoher Priorität individuell so schnell wie möglich untersuchten. Ein Schwerpunkt dieser Beschwerden lag in diesem Jahr erneut beim Thema Videoüberwachung. So häuften sich die Beschwerden von Privatleuten zu Überwachungssystemen in der direkten Nachbarschaft. Oft ging es außerdem um Kameras am Arbeitsplatz, in Restaurants und im Einzelhandel.

Dass hier häufig Grenzen überschritten und Rechte verletzt wurden, zeigen die vielen Bußgelder, die wir in diesem Bereich verhängt haben. Das betraf Gaststätten, das Beherbergungsgewerbe, Läden sowie Privatgrundstücke und Fahrzeuge, wenn dort Kameras unzulässig installiert und nicht ausreichend gekennzeichnet waren.

Ungenügender Beschäftigtendatenschutz am Beispiel Amazon

Seit Jahren fordern die deutschen Datenschutzaufsichtsbehörden ein bundesweites Beschäftigtendatenschutzgesetz. Grund hierfür sind die technischen Entwicklungen, die eine immer umfassendere Überwachung von

Mitarbeiterinnen und Mitarbeitern ermöglichen. Die Datenschutzkonferenz hat diesbezüglich festgestellt, dass der für diesen Bereich geltende § 26 Bundesdatenschutzgesetz nicht hinreichend praktikabel, normenklar und sachgerecht ist.

Ein bemerkenswertes Urteil zum Beschäftigtendatenschutz fällte das Verwaltungsgericht Hannover 2023 gegen unsere Behörde. Wir hatten 2020 der Amazon Logistik Winsen GmbH die ununterbrochene Erhebung und Verwendung von bestimmten Beschäftigtendaten untersagt. Das Unternehmen klagte dagegen vor dem Verwaltungsgericht Hannover. Dieses entschied, dass Amazon weiterhin ununterbrochen Beschäftigtendaten erheben und verwenden darf. Begründet wurde diese Entscheidung hauptsächlich damit, dass die erhobenen Daten in erster Linie der Steuerung logistischer Prozesse dienen würden.

Aus unserer Sicht ist das für die Beschäftigten nicht zumutbar. Wir treten deshalb auch weiterhin für das Recht auf informationelle Selbstbestimmung der Mitarbeiterinnen und Mitarbeiter ein und haben gegen dieses Urteil vor dem Oberverwaltungsgericht Lüneburg Berufung eingelegt.

Aufklärung: Hoher Bedarf bei Vereinen

Aufgrund der hohen Belastung durch die Vielzahl an Beschwerden und anderen Aufsichtstätigkeiten ist es unserer Behörde nur begrenzt möglich, zu beraten und präventiv zum Datenschutz zu sensibilisieren. Deshalb müssen wir priorisieren und setzten im Jahr 2023 in der Beratung einen Schwerpunkt im Bereich der Vereine, um ehrenamtliche Datenschutzbeauftragte in ihrer Arbeit zu stärken.

Abgesehen von unserer Beratungshotline speziell für Vereine und den kostenlosen Schulungen für ihre Ehrenamtlichen bieten wir eine ausführliche schriftliche Handreichung mit praktischen Tipps an, die zu einem hohen Datenschutzniveau bei der Arbeit mit Mitgliederdaten beitragen kann. Dass es hier noch Handlungs- und Beratungsbedarf gibt, beweisen die vielen Anfragen, aber auch Beschwerden, die uns von Vereinsmitarbeitern und Mitgliedern 2023 erreichten.

Beratung des Gesetzgebers

Für ein hohes Datenschutzniveau in Niedersachsen ist es notwendig, bei Gesetzesvorhaben so früh wie möglich unsere Behörde und damit die Perspektive des Datenschutzes einzubinden. Damit vermeidet es der Gesetzgeber, dass er spät und unter hohem Zeitdruck oder im Nachhinein noch einmal nachbessern muss. Insofern freut es uns, dass wir in diesem Jahr an einigen Gesetzesvorhaben beteiligt waren und mitwirken konnten – nicht nur auf Landes-, sondern auch auf Bundesebene. Wir haben 2023 immerhin an über 30 Rechtsetzungsvorhaben mitgearbeitet und datenschutzrechtliche Vorgaben und die Rechte der Bürgerinnen und Bürger hierbei fest im Blick gehabt.

Digitalisierung in der Verwaltung

Besonders erwähnenswert sind außerdem die zahlreichen Digitalisierungsprojekte in der Verwaltung, bei denen wir beratend zur Seite standen. Dazu gehört unter anderem das Änderungsgesetz zum Onlinezugangsgesetz, das unter anderem für Onlinedienste der Verwaltung die nötigen Rechtsgrundlagen bei der länderübergreifenden Verarbeitung personenbezogener Daten schaffen wird. Die Datenschutzkonferenz 2023 hat mehrere Stellungnahmen zu den jeweils aktuellen Gesetzesentwürfen verfasst.

Microsoft 365: Handreichung unterstützt Verantwortliche

Die Datenschutzkonferenz hatte 2022 festgestellt, dass der Standard-Auftragsverarbeitungsvertrag (AVV) von Microsoft für ihr Produktpaket Microsoft 365 nicht den Anforderungen der Datenschutz-Grundverordnung entspricht. Im Jahr 2023 haben wir deshalb gemeinsam mit sechs weiteren Aufsichtsbehörden eine Handreichung veröffentlicht, die konkrete Hinweise für eine datenschutzkonforme Anpassung des Standard-AVV gibt. Verantwortliche können diese nutzen, um auf entsprechende vertragliche Änderungen hinzuwirken. Nun ist es an Microsoft, seinen Kundinnen und Kunden in Europa ein angemessenes Datenschutzniveau anzubieten.

Ein erster Erfolg dieser Handreichung: Das Niedersächsische Ministerium für Inneres und Sport hat sich nach unserer dahingehenden Beratung auf den Weg gemacht, mit Microsoft über die vertragliche Ausgestaltung in diesem Sinne zu verhandeln.

D Zahlen und Fakten

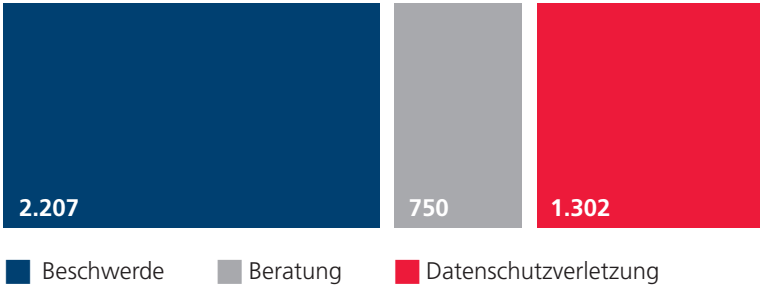
D.1 Beschwerden, Datenpannen, Bußgelder

Nachdem 2022 erstmals die Anzahl der uns gemeldeten Datenschutzverletzungen und Beschwerden zurückging, erhielten wir 2023 wieder geringfügig mehr Meldungen als im Vorjahr. So stieg die Zahl der Beschwerden um rund 7 Prozent an, die der gemeldeten Datenschutzverletzungen um rund 13 Prozent. Gegenstand vieler Beschwerden sind wiederkehrende Themen.

Als Datenschutzaufsicht sind wir zentraler Ansprechpartner für Anfragen und Beschwerden zum Datenschutz in Niedersachsen, außerdem müssen Verantwortliche gemäß der Datenschutz-Grundverordnung (DSGVO) aufgetretene Datenschutzverletzungen[1] an uns melden. Täglich erreichen uns Beschwerden von Bürgerinnen und Bürgern, die sich in ihrem Recht auf informationelle Selbstbestimmung verletzt sehen.

Für öffentliche Stellen und Unternehmen sind wir auch im Hinblick auf Beratung zu datenschutzkonformen Prozessen die niedersächsische Anlaufstelle. Insbesondere die Beratung von Unternehmen erfolgt jedoch in der Regel über die Zusammenarbeit mit Verbänden. In Summe erreichten uns 2023 rund 10 Prozent mehr Eingaben in Form von Beschwerden, Anfragen und gemeldeten Datenschutzverletzungen als im Vorjahr.

A1 – Beschwerden, Beratungsanfragen, Datenschutzverletzungen Fallzahlen 2023

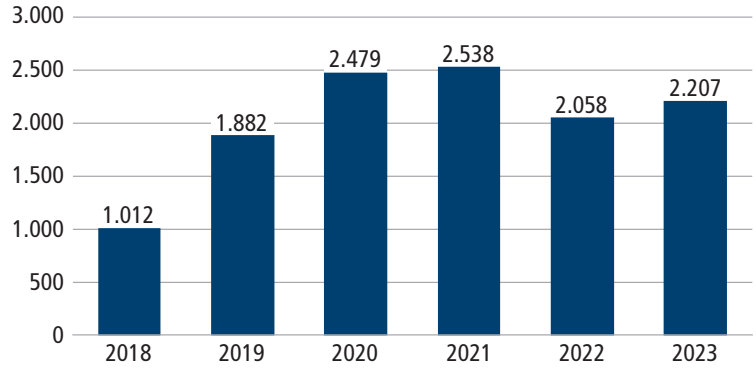


1 Gemäß Art. 33 DSGVO.

Beschwerden

Insgesamt 2.207 Beschwerden[2] gingen 2023 bei der Datenschutzaufsicht ein, was einem Anstieg um rund 7 Prozent zum Vorjahreszeitraum entspricht. Viele Beschwerden drehten sich um unerwünschte Werbung oder Kontaktaufnahmen auf Webseiten, per Newsletter oder per Post. Häufig meldeten uns Betroffene, dass sie keinen Geschäftskontakt mit der jeweiligen Firma hatten oder dass sie einer Verarbeitung ihrer personenbezogenen Daten nicht zugestimmt beziehungsweise dem Kontakt zu Werbezwecken widersprochen hatten.

A2 – Zahl der Beschwerden 2018 bis 2023



Generell gingen viele Beschwerden im Bereich des Online-Handels ein, aber auch zu Unternehmen der Finanzwirtschaft wie Auskunfteien, Banken, Finanzberatungen und Inkassobüros. Zu Webseiten allgemein, insbesondere aber Medienangeboten, erreichten uns viele Beschwerden rund um das Tracking von Nutzenden.

Auch das Recht auf Auskunft[3] war im vergangenen Jahr Gegenstand vieler Beschwerden – etwa, wenn ein Unternehmen nach Aufforderung eines Betroffenen nicht oder nur unzureichend offenlegt, welche Daten des Betroffenen das Unternehmen verarbeitet hat. Ein weiterer Schwerpunkt bei den Beschwerden lag beim Beschäftigtendatenschutz, zum Beispiel wenn

2 Gemäß Art. 77 DSGVO.
3 Gemäß Art. 15 DSGVO.

Beschäftigte sich überwacht fühlten oder Daten aus ihrer Sicht vom Arbeitgeber unerlaubt weitergegeben wurden.

Grundsätzlich stieg die Anzahl der Beschwerden in den meisten Bereichen, eine besondere Veränderung in einem einzelnen Bereich konnten wir nicht feststellen. Leider ist aber auch in keinem Bereich die Anzahl der Beschwerden signifikant zurückgegangen.

Beratungen

Im Jahr 2023 erreichten uns etwa 750 Beratungsanfragen zum Datenschutz. Im Vergleich zum Vorjahr mit knapp 1.000 Beratungsanfragen entspricht dies einem Rückgang um rund 25 Prozent. Unsere Behörde bemüht sich, die Beratungsanliegen auch hinsichtlich konkreter Einzelfälle bestmöglich zu unterstützen. In Anbetracht einer angespannten Personalsituation können wir dies leider nur in dem Rahmen leisten, den die Zeit der Kolleginnen und Kollegen neben ihren weiteren Aufgaben zulässt.

Datenschutzverletzungen nach Art. 33 DSGVO

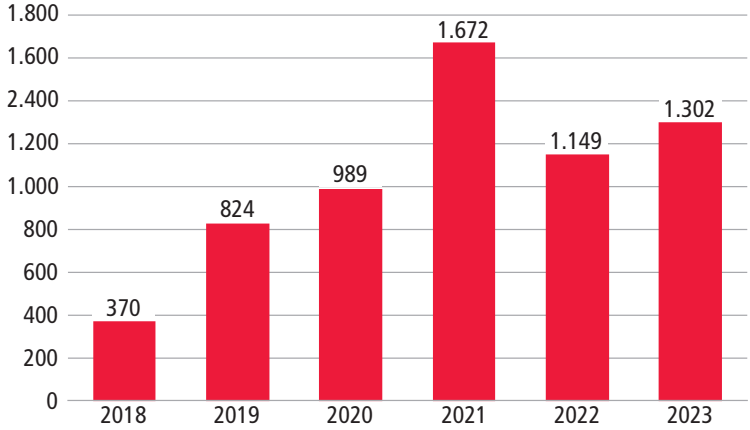
Aus Versehen online gestellte Mitarbeiterfotos, gehackte Geschäftskonten, falsch versendete Patientendaten: Wenn durch eine unerlaubte Datenverarbeitung die Rechte und Freiheiten einer Person betroffen sind, verpflichtet die DSGVO gemäß Artikel 33 den (für die Datenverarbeitung) Verantwortlichen, dies binnen 72 Stunden an die Datenschutzaufsicht zu melden. Die uns gemeldeten Datenschutzverletzungen stiegen 2023 im Vergleich zum Vorjahr geringfügig an. Mit 1.302 gemeldeten Datenschutzverstößen entspricht das einem Anstieg um gut 13 Prozent im Vergleich zum Berichtsjahr 2022.

Seit Inkrafttreten der Datenschutz-Grundverordnung 2018 ist die Zahl der gemeldeten Datenschutzverletzungen kontinuierlich angestiegen (siehe Abbildung 3). Einen Ausreißer nach oben bildet das Berichtsjahr 2021, in dem rund 500 Meldungen zu einer Sicherheitslücke[4] eingingen, die viele Unternehmen betraf.

4 Knapp 500 Meldungen gingen 2021 zum sogenannten Hafnium-Hack ein, einer Sicherheitslücke in Microsofts Exchange-Servern.

Die kontinuierliche Zunahme deutet darauf hin, dass sich der Umgang mit den Pflichten der DSGVO fünf Jahre nach ihrem Inkrafttreten bei den Verantwortlichen eingespielt hat. Vermutlich sind in dieser Zeit aber auch die Zahl von Cyberangriffen und anderen illegalen Zugriffen angestiegen, was sich ebenfalls in gestiegenen Fallzahlen darstellt.

A3 – Gemeldete Datenschutzverletzungen 2018 bis 2023



Bußgelder

Im Berichtsjahr 2023 haben wir mit Erstbescheid Geldbußen in Höhe von insgesamt rund 5,3 Millionen Euro verhängt.[5] Die summierte Höhe der verhängten Bußgelder geht überwiegend auf drei einzelne Verfahren zurück.[6]

Da Geldbußen sich nach Natur und Schwere der jeweiligen Fälle des Berichtsjahrs richten, ist ein Vorjahresvergleich hier nur bedingt aussagekräftig. Seit Anwendungsbeginn der DSGVO können Geldbußen im Datenschutzbereich deutlich höher ausfallen. Bis zu 20 Millionen Euro beziehungsweise 4 Prozent des weltweiten jährlichen Umsatzes sind möglich – je nachdem, welcher Betrag höher ist.

5 Bußgeldhöhen können gegebenenfalls aufgrund von Einsprüchen im Zwischenverfahren in Zweitbescheiden angepasst werden.

6 Siehe hierzu auch Kapitel H.

D.2 Beteiligung an Gesetzgebungsverfahren

Datenschutz ist kein situatives oder isoliertes Thema. Datenschutz ist auch kein Selbstzweck. Vielmehr sollte Datenschutz in allen relevanten Lebensbereichen als ein selbstverständlicher Bestandteil, als ein durchgängiges Prinzip und wie eine logische Struktur mitgedacht werden – auch bei der Gesetzgebung.

Datenschutz beginnt beim Gesetzgeber. Die wesentlichen datenschutzrechtlichen Grundsätze sind auf allen Ebenen regelmäßig dieselben:

- Wer darf die konkreten Daten verarbeiten?
- Unter welchen Voraussetzungen dürfen diese Daten verarbeitet werden? Hier ist grundsätzlich die Frage angesprochen, ob die Verarbeitung erforderlich ist.
- Unter welchen Voraussetzungen ist möglicherweise eine Weiterleitung der Daten an eine andere verantwortliche Stelle erlaubt?
- Zu welchen Zwecken darf diese Stelle die Daten (weiter)verarbeiten?
- Sind besondere technische und organisatorische Maßnahmen des Verantwortlichen erforderlich?
- Können die Betroffenenrechte gewährleistet werden?

Insbesondere im sogenannten öffentlichen Bereich, in dem die Datenschutz-Grundverordnung (DSGVO) grundsätzlich nationale Regelungen fordert[1], kommt es neben der DSGVO zusätzlich auf die entsprechenden Bundesgesetze oder Landesgesetze an. Denn bei der Rechtsanwendung kann nur so viel Datenschutz erwartet werden, wie das jeweilige Fachgesetz an Datenschutz vorsieht – beispielsweise durch klare Tatbestandsvoraussetzungen für Verarbeitungssituationen und Zweckbestimmungen. Ein Gesetz wird dadurch zum „Schaltplan" für gelebten Datenschutz. Wie bei allen Verarbeitungssituationen ist der Datenschutz auch bei der Gesetzgebung kein Gegenspieler zum fachlichen Ziel des jeweiligen Gesetzes. Vielmehr sind normenklare, zweckorientierte Regelungen des jeweiligen Gesetzes und der Datenschutz lediglich zwei Seiten derselben Medaille.

1 Vgl. Art. 6 Abs. 2, 3 DSGVO.

Frühzeitige Beteiligung unseres Hauses ist zu begrüßen

Es ist daher zu begrüßen, dass wir vom niedersächsischen Gesetzgeber oftmals frühzeitig eingebunden werden, um Gesetzesentwürfe auf die oben skizzierten Grundsätze gegenlesen zu können. Gleichwohl könnte die Beteiligung noch häufiger und oft vor allem noch ein wenig frühzeitiger erfolgen.

Aber: Auch im Jahr 2023 waren wir an Landesgesetzen sowie an Verordnungen und Verwaltungsvorschriften der Ministerien beteiligt. Als Beispiel ist das Gesetzgebungsverfahren zur Änderung des Niedersächsischen Datenschutzgesetzes (NDSG) zu nennen.[2] Hierzu fand im Sommer 2023 die Verbandsbeteiligung statt. Das Gesetz befand sich zum Ende des Berichtszeitraums noch im parlamentarischen Verfahren. Im Jahr 2023 haben wir außerdem diverse weitere Rechtssetzungsvorhaben begleitet.

Gesetze des Landes

Gesetz über das Klinische Krebsregister Niedersachsen (GKKN)
Niedersächsisches Maßregelvollzugsgesetz (Nds. MVollzG)
Niedersächsisches Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke (NPsychKG)
Niedersächsisches Gesetz zur Umsetzung des Pakts für den Öffentlichen Gesundheitsdienst (NUmGPöGD)
Niedersächsisches Kommunalverfassungsgesetz (NKomVG)
Niedersächsisches Architektengesetz (NArchtG)
Niedersächsisches Ingenieurgesetz (NIngG)
Niedersächsische Bauordnung (NBauO)
Niedersächsisches Gleichberechtigungsgesetz (NGG)
Niedersächsisches Gesetz über das Halten von Hunden (NHundG)

2 Die Änderungen des NDSG sind Teil eines „Gesetzgebungspakets"– des Entwurfs eines Gesetzes zur Beschleunigung kommunaler Abschlüsse sowie zur Änderung des Niedersächsischen Kommunalverfassungsgesetzes, des Niedersächsischen Gesetzes über die kommunale Zusammenarbeit, des Niedersächsischen Datenschutzgesetzes und des Niedersächsischen Ausführungsgesetzes zum Wasserverbandsgesetz.

Niedersächsisches Ausführungsgesetz zum Wasserverbandsgesetz (Nds. AGWVG)
Niedersächsisches Sicherheitsüberprüfungsgesetz (Nds. SÜG)
Niedersächsisches Personalvertretungsgesetz (NPersVG)
Niedersächsisches Rettungsdienstgesetz (NRettDG)

Verordnungen, Richtlinien, Erlasse und sonstige Regelungen des Landes

Richtlinie über die Gewährung von Zuwendungen zur Förderung von Angeboten zur Unterstützung im Alltag sowie Modellvorhaben zur Erprobung neuer Versorgungskonzepte und Versorgungsstrukturen (UstARdErl 2024)
Niedersächsische Verordnung über Hygiene und Infektionsprävention in medizinischen Einrichtungen (NMedHygVO)
Verordnung über die „Stiftung Gottfried Wilhelm Leibniz Universität Hannover“ (StiftVO-LUH)
Niedersächsische Beihilfeverordnung (NBhVO)
Niedersächsische Heilverfahrens- und Pflegeverordnung (NHPVO)
Niedersächsische Laufbahnverordnung (NLVO)
Verordnung über die Einreichung und Führung der Tabellen über die angemeldeten Forderungen gemäß § 175 Insolvenzordnung in maschineller Form (NMInsoTabVO)
Vereinbarung gemäß § 81 NBG über die Anwendung eines Personalmanagementverfahrens (PMV) in der niedersächsischen Landesverwaltung
Ausnahmeerlass zur Änderung der „Richtlinien für die Überwachung des fließenden Straßenverkehrs durch Straßenverkehrsbehörden“
6. Bericht der Niedersächsischen Landesregierung nach § 25 Absatz 1 NGG

Gesetze und Verordnungen des Bundes oder anderer Länder

Gesetz zur verbesserten Nutzung von Gesundheitsdaten (GDNG)
Gesetz zur Modernisierung des Pass-, des Ausweis- und des ausländerrechtlichen Dokumentenwesens (PassAuswModG)
Gesetz zur Ermöglichung des Bodycam-Einsatzes nach § 184a LVwG (Landesverwaltungsgesetz Schleswig-Holstein) in Wohnungen[3]
Gesetz zur Änderung des Onlinezugangsgesetzes sowie weiterer Vorschriften zur Digitalisierung der Verwaltung (OZG-Änderungsgesetz – OZGÄndG)[4]
Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (Einwilligungsverwaltungsverordnung – EinwV)[5]

Fazit

Wenn die Datenschutzaufsicht frühzeitig eingebunden wird, insbesondere auf Arbeitsebene, kommt dies nicht nur der Datenschutzkonformität des Vorhabens, sondern auch dem Zeitlauf des anschließenden förmlichen Gesetzgebungsverfahrens regelmäßig zugute. Hintergrund ist, dass etwaige Bedenken frühzeitig ausgeräumt werden können und die entsprechenden normenklaren Regelungen von Anbeginn in das förmliche Gesetzgebungsverfahren eingebracht werden.

3 Auf Bitte des Innenausschusses des Schleswig-Holsteinischen Landtages haben wir im Rahmen des dortigen Gesetzgebungsverfahrens Stellung genommen.
4 Siehe ausführlich Kapitel I.9.
5 Siehe ausführlich Kapitel I.4.

E Schlaglicht: Künstliche Intelligenz

Künstliche Intelligenz beschäftigt die Datenschutzaufsicht

Spätestens seit der KI-basierte Dienst ChatGPT in Deutschland nutzbar ist, ist das Thema Künstliche Intelligenz in der praktischen Arbeit der niedersächsischen Datenschutzaufsicht angekommen. Es ist ein Querschnittsthema, das uns 2023 aus verschiedenen Richtungen, in unterschiedlichen Zusammenhängen und mit unterschiedlichen Zielsetzungen erreicht hat.

Künstliche Intelligenz (KI) ist der Ansatz, dass Maschinen menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität imitieren können. KI-Systeme analysieren frühere Aktionen, passen zukünftige Entscheidungen und Handlungen daran an und entwickeln sich autonom weiter. Im Ende 2023 vorliegenden Entwurf der europäischen KI-Verordnung soll ein KI-System definiert werden als „ein maschinengestütztes System, das für explizite oder implizite Ziele aus den empfangenen Eingaben ableitet, wie es Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugen kann, die physische oder virtuelle Umgebungen beeinflussen können".

KI wird daher als zukunftsweisende technische Entwicklung gewertet, die das Potenzial aufweist, in nahezu allen Lebens- und Anwendungsbereichen eingesetzt zu werden und massive Veränderungen zu bewirken.[1] Bei Künstlicher Intelligenz wird häufig zwischen einer sogenannten schwachen und starken Künstlichen Intelligenz unterschieden. Eine starke KI setzt die universale Einsetzbarkeit für die Erfüllung von Aufgaben und Lösung von Problemen voraus. Starke KI soll jede intellektuelle Aufgabe, die ein Mensch beherrscht, eigenständig und vorausschauend erfüllen können. Starke KI ist bisher nur aus der Science-Fiction bekannt. Aktuelle KI-Systeme sind der schwachen Künstlichen Intelligenz zuzuordnen, da sie für die Erfüllung spezifischer Aufgaben trainiert werden.

1 Siehe z. B. die Übersicht des EU-Parlaments „Was ist künstliche Intelligenz und wie wird sie genutzt?", https://t1p.de/ep-ki (Kurzlink) sowie LfD Niedersachsen, Presseinformation vom 18. März 2021 „Einsatz von künstlicher Intelligenz im Justizvollzug nur unter Wahrung der Persönlichkeitsrechte", https://lfd.niedersachsen.de/198588.html

Erste Anwendungsbereiche von KI sind beispielsweise KI-Sprachmodelle (englisch Large Language Models) wie GPT-4, PaLM 2, Llama 2 und Luminous. Einfach gesagt ist ein Large Language Model eine Textvorhersagemaschine. Technisch ist es ein neuronales Netz für maschinelles Lernen, das mit enormem Daten-Input in Form von Texten und Daten-Output, der bei der Nutzung des Sprachmodelles entsteht, trainiert wird. Das Large Language Model kann mittels wahrscheinlichkeitsbasierter Algorithmen auf ein vorgegebenes Wort ein passendes Folgewort voraussagen. So können Wort für Wort Antworten auf Fragen oder umfassende Texte produziert werden.

Large Language Models können in ganz unterschiedliche KI-Anwendungen eingebunden werden, wie zum Beispiel Chatbots. Zudem sind sehr unterschiedliche Einsatzzwecke und Anwendungsbereiche möglich. Personen können sich über alle möglichen Themen mit einen Chatbot unterhalten, es können Fragen beantwortet, Texte zusammengefasst oder geschrieben oder Softwarecode erstellt werden. Das aktuelle wohl bekannteste Beispiel ChatGPT steht grundsätzlich Privatpersonen, Unternehmen und Behörden für alle Bereiche zur Verfügung, in denen Texte relevant sind – Reden, studentische Abschlussarbeiten, Arbeitszeugnisse, Gesetzesentwurfe, Musikstücke, Bedienungsanleitungen, Wetterprognosen und vieles mehr.

ChatGPT macht bereits absehbar, dass der Einsatz von KI die Gesellschaft verändern wird.[2] Der Deutsche Ethikrat formuliert in einer umfassenden Stellungnahme die Kernfrage: „Werden menschliche Autorschaft und die Bedingungen für verantwortliches Handeln durch den Einsatz von KI erweitert oder vermindert?" Die ethische Bewertung orientiert sich an den Grundsätzen, dass der Einsatz von KI menschliche Entfaltung vergrößern, nicht verringern soll und den Menschen nicht ersetzen darf. Die Gewährleistung dieser Grundsätze kann durch rechtliche Vorgaben flankiert werden. Bereits jetzt sichert die Datenschutz-Grundverordnung das Recht jedes Einzelnen, keiner rein automatisierten Entscheidung unterworfen zu werden, die rechtliche Wirkung entfalten oder eine erhebliche Beeinträchtigung darstellen kann.[3] Umgekehrt bedeutet es, dass in diesen Fällen eine endgültige Entscheidung von einem Menschen getroffen werden muss. Darüber hinaus gibt es in Europa weit fortgeschrittene Bestrebungen, spe-

2 Siehe auch Kapitel G.2.1.

3 Nach Art. 22 DSGVO.

zifische Regelungen für KI zu erlassen, um wünschenswerte Entwicklungen und Auswirkungen zu fördern sowie unerwünschte zu verhindern.

Entwurf einer europäischen KI-Verordnung

Ende 2023 befanden sich die Trilog-Verhandlungen[4] über die europäische Verordnung zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) in einer entscheidenden Phase. Die KI-Verordnung verfolgt einen risikobasierten Ansatz: Es sollen bestimmte Praktiken im Bereich der Künstlichen Intelligenz verboten sowie differenzierte Anforderungen an Hochrisiko-KI-Systeme und bestimmte KI-Systeme festgelegt werden. Daran anknüpfend sollen abgestufte rechtliche Anforderungen für die wichtigsten Beteiligten, zum Beispiel Anbieter, Einführer, Händler, Bevollmächtigte, Nutzer, über die gesamte KI-Wertschöpfungskette gelten. Das Europäische Parlament hat in seiner Position[5] vom 14. Juni 2023 wesentliche Abänderungen des Entwurfstexts der Europäischen Kommission gefordert. Ausdrücklich in die Verordnung eingeschlossen werden sollten danach KI-Basismodelle. Dabei handelt es sich um KI-Modelle, die auf einer breiten Datenbasis trainiert wurden, auf eine allgemeine Ausgabe ausgelegt sind und an eine breite Palette unterschiedlicher Aufgaben angepasst werden können.

Nach dem Vorschlag des EU-Parlaments sollen Anbieter von Basismodellen bestimmte Mindestanforderungen erfüllen, etwa im Hinblick auf Transparenz, Datenqualität, Erklärbarkeit und Cybersicherheit. Im Dezember 2023 konnte nach langen Verhandlungen im Trilog-Verfahren eine Einigung hinsichtlich der Regulierung der Basismodelle in der KI-Verordnung erreicht werden. Es wurde sich auf einen abgestuften Ansatz verständigt, der zwischen Basismodellen und Basismodellen mit systemischen Risiken unterscheidet und entsprechend abgestufte Anforderungen definiert. Aus datenschutzrechtlicher Sicht ist dies ein wichtiger Schritt, um die Forderung der Datenschutzkonferenz (DSK) nach klaren Verantwortlichkeiten für Hersteller und Betreiber in der KI-Verordnung umzusetzen.[6]

4 Informelle interinstitutionelle Verhandlungen als etablierter Bestandteil des Europäischen Gesetzgebungsprozesses.

5 Kurzlink: https://t1p.de/ki-vo

6 Siehe DSK, Regulierung von KI: DSK fordert klare Verantwortlichkeit für Hersteller und Betreiber, Pressemitteilung vom 29. November 2023, Kurzlink: https://t1p.de/dsk-ki (PDF).

Künstliche Intelligenz und Datenschutz

Der Einsatz von Künstlicher Intelligenz bedingt zwar nicht immer, aber sehr häufig die Verarbeitung von personenbezogenen Daten. Immer wenn personenbezogene Daten verarbeitet werden, ist das Datenschutzrecht zu berücksichtigen. Nicht in den Anwendungsbereich kann beispielsweise KI für die Bereiche Geologie, Umweltschutz, Meteorologie oder industrielle Wartung fallen.

Es ist Aufgabe der Aufsichtsbehörden, datenschutzrechtliche Bewertungen von KI-Systemen vorzunehmen, sei es um Beratungsanfragen von Behörden, öffentlichen Einrichtungen oder Unternehmen zu beantworten oder Beschwerden von Bürgerinnen und Bürgern gegen den Einsatz von KI zu bearbeiten. Dabei ist zu beachten, dass in den unterschiedlichen Phasen – von der KI-Entwicklung bis zum Einsatz des KI-Systems – teils in sehr großem Umfang personenbezogene Daten verarbeitet werden. Die benötigte Menge an Trainingsdaten stammt zum Beispiel aus dem Internet, aus Videoüberwachung von belebten Plätzen oder am Verkehr teilnehmende Fahrzeuge oder aus medizinischen Datenbanken. Zudem werden bei der Nutzung von KI weitere Daten produziert, die für das maschinelle „Weiter"-Lernen verwendet werden. So werden beispielsweise bei der Nutzung einer KI-basierten Lernplattform im schulischen Bereich personenbezogene Daten eingegeben und auch der Output des KI-Systems in Form von Aufgabenstellungen und Bewertungen an Schülerinnen und Schüler sowie Lehrerinnen und Lehrer kann personenbezogene Daten umfassen.

KI-Systeme müssen die Grundsätze des Datenschutzes einhalten. Hierbei stehen insbesondere die Grundsätze der Datenminimierung, der Transparenz, der Zweckbindung und der Richtigkeit von personenbezogenen Daten im Widerspruch zu den Grundlagen der Entwicklung, Zielsetzung und Anwendung vieler KI-Systeme. Diesen Grundkonflikt erkannte die DSK bereits frühzeitig: Im Frühjahr 2019 beschloss sie mit der sogenannten „Hambacher Erklärung zur Künstlichen Intelligenz" sieben datenschutzrechtliche Anforderungen an Systeme der Künstlichen Intelligenz.[7] Ein halbes Jahr später

KI-Systeme müssen die Grundsätze des Datenschutzes einhalten.

7 Siehe DSK, Hambacher Erklärung zur Künstlichen Intelligenz, 19. April 2019, https://lfd.niedersachsen.de/download/142595 (PDF).

folgte die Veröffentlichung des Positionspapiers der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen.[8]

Im April 2021 hat der europäische Gesetzgeber den Erlass eines europäischen Gesetzes über Künstliche Intelligenz – die KI-Verordnung – initiiert. Der Verordnungsentwurf umfasst auch Datenschutzvorschriften vor allem zur Verwendung von KI-Systemen zur biometrischen Identifizierung. Es ist daher zu erwarten, dass den Datenschutzaufsichtsbehörden durch die KI-Verordnung neue und zusätzliche Aufsichtsbefugnisse zugewiesen werden.

KI-Themen bei der Datenschutzaufsicht

2023 hat die niedersächsische Datenschutzaufsicht begonnen, die in den genannten DSK-Papieren abstrakt formulierten datenschutzrechtlichen Anforderungen bei konkreten Anwendungen zu überprüfen. Der dargestellte sehr breite Anwendungsbereich von KI-Systemen spiegelte sich hier deutlich wider.

Ausgelöst durch das von der italienischen Datenschutzaufsichtsbehörde ausgesprochene Verbot von ChatGPT in Italien hat sich in Deutschland die Taskforce KI der DSK des Themas angenommen. Niedersachsen ist hierüber an der datenschutzrechtlichen Bewertung von ChatGPT intensiv beteiligt. Ein grundlegendes Problem ist, dass der Anbieter OpenAI für die Entwicklung des Large Language Models GPT-4 überwiegend Trainingsdaten von Webseiten verwendet hat. Das Internet stellt zweifellos die größte und umfassendste allgemein verfügbare Informationsquelle dar. Allerdings führt die öffentliche Abrufbarkeit nicht automatisch dazu, dass alle enthaltenen personenbezogenen Daten zu beliebigen Zwecken (weiter)verarbeitet werden dürfen. OpenAI konnte bisher den Nachweis nicht erbringen, dass die Verarbeitung personenbezogener Daten zum Training von GPT-4 rechtmäßig erfolgt ist.

Das Thema KI begegnet uns ebenso beim autonomen Fahren: Dessen stetige Weiterentwicklung erfordert es aus Sicht der deutschen Automobilindustrie fortlaufend, KI-Systeme mit weiteren Trainingsdaten aus dem re-

8 Siehe DSK, Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen, 6.11.2019, https://lfd.niedersachsen.de/download/150867 (PDF).

alen Straßenverkehr zu trainieren. Im ersten Schritt waren diese zunächst aus dem realen Straßenverkehr von speziellen Testfahrzeugen der Automobilhersteller generiert worden.[9] Im zweiten Schritt beabsichtigen die Hersteller, Trainingsdaten aus den verkauften Kundenfahrzeugen zu verwenden. Diese erfassen die Umgebung mittels Kameras und zahlreicher Sensoren und verarbeiten somit nicht nur personenbezogene Daten der Fahrzeugnutzer, sondern auch von anderen Verkehrsteilnehmern, einschließlich Passanten. Auch hierbei müssen die Datenschutzgrundsätze der Rechtmäßigkeit, Transparenz, Datenminimierung und Zweckbindung beachtet werden und stellen aktuell eine große Herausforderung dar.

Nicht nur von Unternehmen, sondern auch im öffentlichen Sektor wird intensiv über die Einführung von KI nachgedacht. Das Land Niedersachsen gründete im Februar 2023 das Kompetenzzentrum für Künstliche Intelligenz in der niedersächsischen Verwaltung (KiKoN), um den Einsatz von KI zu fördern und zu beschleunigen.[10] Das Niedersächsische Ministerium für Inneres und Sport (MI) hat uns gebeten, das KiKoN in Bezug auf die datenschutzrechtlichen Aspekte von KI zu beraten – eine Aufgabe, der wir sehr gerne nachkommen.

Darüber hinaus haben uns im vergangenen Jahr zwei konkrete Themen beschäftigt. Das Niedersächsische Justizministerium hat den Auftrag für die Entwicklung einer KI-gestützten Richterassistenz erteilt.[11] Aufgrund unserer eingeschränkten Aufsichtsbefugnisse für die justizielle Tätigkeit kommt uns bei diesem Projekt allerdings lediglich eine beratende Funktion zu.[12]

Im Rahmen einer 2023 durchgeführten anlasslosen Prüfung stellten wir fest, dass Schulen in Niedersachsen zunehmend KI-basierte Lernsoftware und sogenannte „intelligente Tutorensysteme" einsetzen.[13] Das Niedersächsische Kultusministerium unterstützt den Einsatz dieser Softwarepro-

9 Siehe DSK, Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten, 27.9.2023, Kurzlink: https://t1p.de/dsk-umgebung (PDF).

10 Siehe Niedersächsisches Ministerium für Inneres und Sport, Land Niedersachsen gründet Kompetenzzentrum für künstliche Intelligenz in der Verwaltung, Presseinformation vom 7.2.2023, https://www.mi.niedersachsen.de/219423.html

11 Siehe Niedersächsisches Justizministerium, Einsatz Künstlicher Intelligenz in der Verwaltung, Presseinformation vom 22. Juni 2023, https://mj.niedersachsen.de/223207.html

12 Siehe Kapitel G.8.1.

13 LfD Niedersachsen, Presseinformation vom 17. Mai 2023, Licht und (digitaler) Schatten, https://lfd.niedersachsen.de/222362.html

dukte in erheblichem Umfang durch die Bereitstellung entsprechender Lizenzen für die Schulen. Es wäre aus Sicht des Datenschutzes und zur Steigerung der Akzeptanz des Vorhabens sinnvoll gewesen, wenn das Kultusministerium die datenschutzrechtliche Unbedenklichkeit der erworbenen Software vorab überprüft hätte. Das Ministerium hätte sich dabei mit der Bitte an uns wenden können, dass wir mit unserer fachlichen Expertise unterstützen. So ist zum Beispiel bereits die Rechtsgrundlage unklar für eine zwangsläufig erfolgende Verarbeitung der Daten von Kindern und Lehrkräften durch die Bildungsverlage.

Ausblick

Technische Entwicklungen datenschutzrechtlich zu begleiten ist eine wichtige Aufgabe der Aufsichtsbehörden, um einerseits deren Datenschutzkonformität zu gewährleisten und andererseits deren Potenzial zu fördern. Daher ist es notwendig und spannend zugleich, dass wir uns so früh wie möglich mit KI-Systemen vertraut machen, Impulse für die Entwicklung des Datenschutzrechts setzen und uns zu konkreten Gesetzgebungsverfahren positionieren. Dieser proaktive Ansatz ist unabdingbar, um öffentliche und nicht-öffentliche Stellen in Niedersachsen beim Einsatz von KI-Systemen zu beraten und die bei stetig zunehmender Verbreitung zu erwartenden Beschwerden und Datenpannenmeldungen zu bearbeiten. KI und KI-Systeme sind aufgrund ihrer Vielfalt und Komplexität ein anspruchsvolles datenschutzrechtliches Thema, das uns auch in den kommenden Jahren intensiv beschäftigen wird.

F Schlaglicht: Das IT-Labor des LfD

Das IT-Labor der niedersächsischen Datenschutzaufsicht

Unsere Behörde ist nicht nur juristisch, sondern auch technisch gut aufgestellt. Die Expertinnen und Experten unseres IT-Labors überprüfen Server auf datenschutzrechtlich relevante Lücken und damit auf die Angreifbarkeit von außen, analysieren den Cookie-Einsatz auf Medienportalen und entwickeln Datenschutz-Prüfverfahren für digitale Plattformen wie Apps und Webseiten.

Seit 2016 baut die Datenschutzaufsicht Niedersachsen kontinuierlich ihr IT-Labor aus, das inzwischen von einem Team aus vier Personen betreut und genutzt wird. Es verfügt über einen umfassenden technischen Apparat aus Servern, Computern und Forensikwerkzeugen. Die Kolleginnen und Kollegen agieren als interne Dienstleister für die juristischen Fachreferate: Mit Hilfe des IT-Labors führt unsere Behörde eigenständig IT-forensische Beweissicherung bei Beschwerden, Datenschutzpannen und anlasslosen Prüfungen durch. Darüber hinaus entwickelt das Team der IT-Forensik eigene Testverfahren.

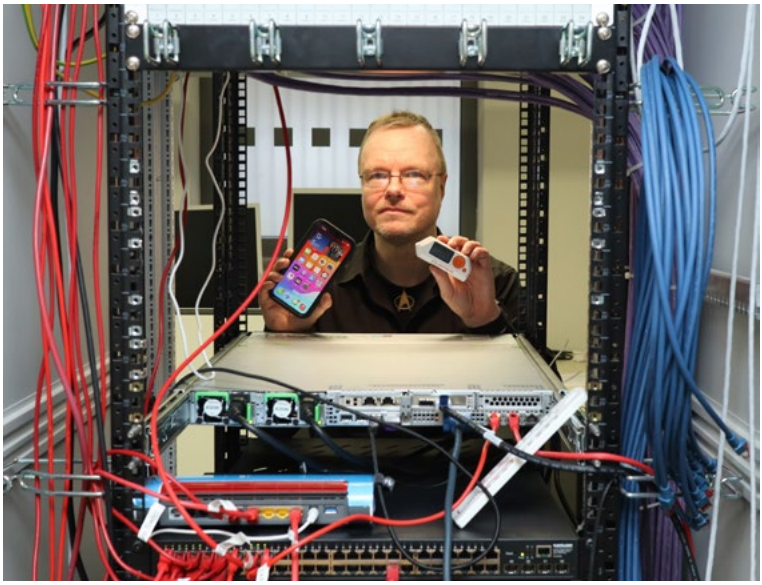
Das Team unseres IT-Labors ist gut vernetzt mit den Kolleginnen und Kollegen anderer Landesdatenschutzbehörden. Durch die intensive Zusammenarbeit und den kontinuierlichen Erfahrungsaustausch auf nationaler und europäischer Ebene wirken wir auf die Entwicklung gemeinsamer Standards in der forensischen Untersuchung von Datenschutzverstößen hin.

IT-Security- und Datenschutzanalysen

Im Jahr 2023 setzten wir unser Projekt der proaktiven Prüfung von Microsoft-Exchange-Servern fort. Im IT-Labor identifizierten wir unter Nutzung von Internet-Wide-Scanning-Datenbanken in einem teilautomatisierten Prozess Verantwortliche aus Niedersachsen, deren Server trotz der bereits seit 2021 publizierten Warnungen des Bundesamts für Sicherheit in der Informationstechnik (BSI)[1] weiterhin bekannte kritische Microsoft-Exchange-Sicherheitslücken aufwiesen. Beim Betrieb von E-Mail-Systemen, die mit

1 Kurzlink: https://t1p.de/bsi-exchange

solchen kritischen Schwachstellen behaftet sind, besteht ein sehr hohes Datenschutzrisiko. Sollte ein Angriff diese Schwachstellen ausnutzen, führt das mit einer sehr großen Wahrscheinlichkeit zur Verletzung des Schutzes personenbezogener Daten.



IT-Experte Patrick Gersmeyer im Serverraum unserer Behörde. Für datenschutzrechtliche Prüfungen kommen auch Smartphones und Spezialtools zum Einsatz.

Wir unterzogen jedes so ermittelte System in unserem IT-Labor einer zusätzlichen Verifikation, um veraltete oder falsch positive Einträge in den Internet-Wide-Scanning-Datenbanken auszuschließen. Dazu haben wir bei den ermittelten Verantwortlichen mit Hilfe eines Schwachstellenscanners die E-Mail-Server in Echtzeit geprüft und im zutreffenden Fall damit aktuelle Nachweise darüber erstellt, dass die von den Verantwortlichen zum Zeitpunkt unserer Prüfung betriebenen Microsoft-Exchange-Server diese Sicherheitslücken auch wirklich aufgewiesen haben.

Nach der Benachrichtigung der betroffenen Verantwortlichen stand unser IT-Labor bei Bedarf den federführenden juristischen Fachreferaten unserer Behörde beratend zur Seite. Zum Abschluss der datenschutzrechtlichen Prüfungen testeten wir, ob die zuvor ermittelten Lücken tatsächlich von

den Verantwortlichen nach unserer Aufforderung geschlossen, also die Schwachstellen in den Exchange-Servern behoben worden sind.

Für Forensik-Analysen verwendet die Datenschutzaufsicht Niedersachsen in einigen Fällen Pentesting-Gadgets.

Das IT-Labor war darüber hinaus intensiv an weiteren Projekten wie der Prüfung von Medienwebseiten[2] beteiligt. Auch bei der Analyse der von Microsoft bereitgestellten Auftragsverarbeitungsverträge[3] unterstützte das IT-Labor bei der Bewertung der in diesem Zusammenhang relevanten technisch-organisatorischen Maßnahmen.[4] Auf dieser dargelegten generischen Grundlage müssen Verantwortliche die konkretisierenden Detailfestlegungen zu technischen und organisatorischen Maßnahmen mit Microsoft aushandeln.

2 Prüfung von Medienseiten: https://www.lfd.niedersachsen.de/223637.html
3 Sogenannte DPAs (Data Processing Agreements).
4 Siehe Kapitel G.5.4.

Im operativen Tagesgeschäft haben unsere IT-Expertinnen und -Experten neben der Projektarbeit allein im Berichtszeitraum 2023 technische Prüfungen im Rahmen von über 60 datenschutzrechtlichen Verfahren durchgeführt.

Europaweiter Austausch

Im Juni 2023 nahmen Mitarbeitende unseres IT-Labors am EDPB-bootcamp[5] teil. An diesem zweitägigen Arbeitstreffen in Brüssel wurden mehrere von europäischen Datenschutzaufsichtsbehörden entwickelte und in der Praxis bereits von uns eingesetzte Tools wie der „Web Evidence Collector"[6] sowie Audit-Anwendungen vorgestellt und im Rahmen eines Workshops gemeinsam erprobt.

Zusammen mit weiteren nationalen und europäischen Aufsichtsbehörden sowie dem Europäischen Datenschutzbeauftragten beteiligten wir uns an der Expertengruppe „Mobile Audit Exchange", die ein europaweit abgestimmtes Vorgehen für technische Untersuchungen der auf Smartphones installierten Apps erarbeitet.

Nationale Zusammenarbeit

Darüber hinaus prägte der intensive Austausch mit den technischen Bereichen einiger Datenschutzaufsichtsbehörden anderer Länder sowie die Nutzung von Schulungsangeboten der Niedersächsischen Polizeiakademie die Arbeit des vergangenen Jahres. Die Mitarbeiter des IT-Labors haben zu mehreren Anlässen den Aufbau sowie die technische Ausstattung des IT-Labors vorgestellt und sich intensiv über aktuelle Prüfungsabläufe und -techniken mit den Kolleginnen und Kollegen anderer Datenschutzaufsichten ausgetauscht.

5 Vgl. Mitteilung des EDSA auf Twitter am 13.6.2023: https://twitter.com/EU_EDPB/status/1668515478002712576

6 Das Tool Website Evidence Collector (WEC) automatisiert das Sammeln von Beweisen für die Speicherung und Übertragung von personenbezogenen Daten. Verfügbar bei GitHub: https://github.com/EU-EDPS/website-evidence-collector

Durch die „Mobile Audit Exchange"-Expertengruppe sind wir auf die Arbeit von Datenanfragen.de e. V.[7] sowie pts-project.org[8] aufmerksam geworden. Diese Gruppen beschäftigen sich mit Analysemöglichkeiten von Apps auf Smartphones für die beiden auf dem Markt dominierenden Smartphone-Betriebssysteme Android und iOS. Die für die Analyse notwendigen Tools sind Open-Source-Projekte. In Zusammenarbeit mit anderen deutschen Datenschutzaufsichtsbehörden arbeiten wir aktuell daran, die sich damit eröffnenden Möglichkeiten in die Prüfverfahren unseres IT-Labors zu integrieren.

Ausblick

Unser Ziel ist es, möglichst von allen Datenschutzaufsichtsbehörden mitgetragene einheitliche Prüfverfahren zu entwickeln und umzusetzen, sodass auch der Austausch von Prüfergebnissen einfacher wird. Zusätzlich gewinnen die Analyse und die Bewertung von technischen Sachverhalten durch die Digitalisierung praktisch aller Lebensbereiche immer mehr an Bedeutung, sodass auch die Anforderungen an die Methoden der IT-Forensik ständig steigen.

Unsere IT-Labor-Mitarbeiterinnen und -Mitarbeiter haben durch ihre Prüfaktivitäten bereits vielfältige Erfahrungen gesammelt und Fachwissen aufgebaut. Der etablierte nationale und EU-weite Austausch über Konzepte, Tools und Methoden der IT-Laborarbeit wird auch in Zukunft die Fortentwicklung und den Ausbau unseres IT-Labors bereichern und damit unser personelles und finanzielles Engagement in diesem Bereich ergänzen.

7 Datenanfragen.de e.V. aus Braunschweig ist eine Zivilinitiative, die als gemeinnütziger Verein insbesondere eine Plattform zur Unterstützung von Selbstdatenschutz und informationelle Selbstbestimmung betreibt: https://www.datenanfragen.de

8 Das Tool PiRogue Tool-Suite (PTS) wird hauptsächlich von Defensive Lab Agency auf Open-Source-Basis entwickelt und gepflegt und bietet eine Router-Plattform für Analysetools, Wissensmanagement, Incident-Response-Management und Artefaktmanagement, mobile Forensik und Netzwerkverkehrsanalyse an mobilen Geräten unter Android und iOS: https://pts-project.org/about/

G Aktuelle Themen

Videoüberwachung

G.1.1 Prüfung von Fitnessstudios: Kameras in Sauna und Umkleide?

Bereits im schriftlichen Prüfverfahren entdeckten wir bei einer Stichprobe von Fitnessstudios teils gravierende Datenschutzverstöße durch Videoüberwachung. Einige Unternehmen müssen nun mit Bußgeldern rechnen und sich auf Vor-Ort-Kontrollen einstellen.

Regelmäßig erreichen uns Beschwerden über Videokameras in Fitnessstudios. Anlässe für die Beschwerden sind zumeist die Überwachung von Trainingsräumen, aber auch von Umkleiden und sogar Saunabereichen. Eine laufende Kamera an solchen Stellen stellt einen besonders intensiven Grundrechtseingriff dar. Denn grundsätzlich hat jeder Mensch Anspruch darauf, seine Freizeit frei von Überwachungsmaßnahmen gestalten zu können. Als Besonderheit kommt bei Fitnessstudios hinzu, dass teilweise bis in den hochsensiblen Bereich der Intimsphäre hinein überwacht wird.

Aus diesem Grund prüften wir 2023 zehn stichprobenartig ausgewählte Fitnessstudio-Unternehmen mit insgesamt 17 Filialen in Niedersachsen. Im ersten Schritt führten wir ein schriftliches Verfahren durch und ermittelten per Fragebogen, ob sie Bereiche in ihren Studios mit Kameras überwachen. Zudem prüften wir außer der Rechtmäßigkeit der eigentlichen Videoüberwachung, ob die Anbieter gesetzliche Informationspflichten erfüllen und ein Verzeichnis der Verarbeitungstätigkeiten führen. Zudem kontrollierten wir, ob sie – sofern erforderlich[1] – eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten benannt und gemeldet sowie – sofern erforderlich[2] – einen Auftragsverarbeitungsvertrag abgeschlossen haben.

1 Siehe dazu Art. 37 DSGVO und § 38 BDSG.
2 Siehe dazu Art. 28 DSGVO.

Zwischenstand: Licht und Schatten

Bis Ende 2023 haben wir die Prüfung der schriftlichen Unterlagen von fast allen Unternehmen abschließen können. Im Ergebnis haben wir bei den verschiedenen Anbietern zu gleichen Teilen keine, geringe und leider auch schwere Datenschutzverstöße festgestellt.

Als Folge der Prüfung haben wir je nach Schwere der Verstöße aufsichtsbehördliche Maßnahmen in Form von Hinweisen oder Verwarnungen ergriffen. Diese kamen etwa bei einer unzureichenden Hinweisbeschilderung in Betracht.

In einigen Fällen war die Einleitung eines Bußgeldverfahrens erforderlich.

In einigen Fällen war außerdem die Einleitung eines Bußgeldverfahrens erforderlich, weil wir unzulässige Videoüberwachungen von Arbeits-, Sitz-, Verzehr- oder Trainingsbereichen festgestellt hatten. Eines dieser Verfahren konnten wir bereits im Berichtszeitraum abschließen.[3]

Nächster Schritt: Vor-Ort-Kontrollen

Im zweiten Schritt werden wir 2024 die Fitnessstudios, bei denen sich besondere Auffälligkeiten oder gravierende Datenschutzverstöße gezeigt haben, im Rahmen einer Vor-Ort-Kontrolle prüfen.

3 Siehe dazu Kapitel H.

G.1.2 Videoüberwachung in Bars und Restaurants

Im Jahr 2023 meldeten uns Polizei und andere Behörden viele datenschutzrechtliche Verstöße beim Einsatz von Videokameras in Gaststätten und Bars. Auffällig werden diese Verstöße häufig im Rahmen von Gewerbe- und Gaststättenkontrollen.

Viele Gastronomen installieren Videokameras in ihren Betrieben, aber auch im Hinterhof oder Eingangsbereich, meist um bei Einbrüchen oder Vandalismus Beweise zu sichern. Häufig ist die Überwachung an den vorgesehenen Stellen nicht zulässig oder Wirte haben dabei nicht alle Vorgaben berücksichtigt, die sich aus der Datenschutz-Grundverordnung (DSGVO) ergeben.

Die Vielzahl an gemeldeten Fällen aus ganz Niedersachsen stellt unsere Behörde vor eine große Herausforderung – zumal uns nicht bloß tatsächliche, sondern auch viele vermeintliche Datenschutzverstöße übermittelt werden, deren Prüfung ebenfalls Zeit kostet. Wir müssen deshalb im Bereich der Videoüberwachung durch Unternehmen stark priorisieren, in welchen Fällen wir wie intensiv vorgehen. So beenden wir Verwaltungsverfahren seit Dezember 2023 vermehrt ohne detaillierte Untersuchung, sondern weisen in einem ersten Schritt lediglich die Verantwortlichen auf einen möglichen Datenschutzverstoß[1] hin.

Das machen wir jedoch nur bei Fällen, bei denen wir aufgrund der ursprünglichen Mitteilungen, Beschwerden oder Meldungen[2] von einem allenfalls geringen Eingriff in das Grundrecht auf informationelle Selbstbestimmung[3] ausgehen. Ähnlich gehen wir bereits regelmäßig bei Videoüberwachung durch Privatpersonen vor.

Dadurch haben wir mehr Zeit, um tiefgehende Grundrechtseingriffe im Bereich der Videoüberwachung zeitnah und umfassend zu untersuchen. Dieses sind etwa Fälle von anlasslosen Videoüberwachungen von Beschäf-

1 Art. 57 Abs. 1 Buchst. d DSGVO.
2 Art. 33 DSGVO.
3 Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.

tigen in Produktions- oder Pausenbereichen oder wenn Kinder beispielsweise auf Spielgeräten in Einkaufszentren betroffen sind.

Hinweiserteilung bei Videoüberwachung in Bars und Gaststätten

Darüber hinaus sehen wir dann vorerst nur einen Hinweis vor, wenn „unbeteiligte" Dritte wie etwa die Polizei nach straf- oder gewerberechtlichen Durchsuchungen die Datenschutzverstöße melden. Denn in diesen Fällen beenden die Betreiber regelmäßig nach entsprechender polizeilicher oder behördlicher Aufforderung die Videoüberwachung, sodass sich der datenschutzrechtlich relevante Grundrechtseingriff nicht weiter fortsetzt.

Situation bei anderen Aufsichtsbehörden

Wie ein Austausch der Aufsichtsbehörden im Rahmen des Arbeitskreises Videoüberwachung der Datenschutzkonferenz ergab, sehen sich die anderen Aufsichtsbehörden in ähnlicher Weise wie wir der Herausforderung gegenüber, extrem hohe Fallzahlen im Bereich der Videoüberwachung zu bewältigen. Auch dort reagieren die Kolleginnen und Kollegen vermehrt mit Hinweisschreiben, um die Verwaltungsverfahren zu beenden – und arbeiten verstärkt mit präventiven Maßnahmen, etwa in Form der Veröffentlichung von Informationsmaterialien.[4]

Ausblick

Bei Besonderheiten im Einzelfall oder im Fall von Wiederholungen wird selbstverständlich weiterhin der gemeldete Sachverhalt vollumfänglich überprüft. Bei einem entsprechend auffälligen Ergebnis, der Feststellung eines Datenschutzverstoßes, erfolgen ordnungsbehördliche Abhilfemaßnahmen[5], um den Verstoß abzustellen.

Die geänderte Vorgehensweise werden wir Mitte 2024 einer Evaluierung unterziehen.

4 Siehe auch Video zur privaten Videoüberwachung unter https://lfd.niedersachsen.de/205509.html

5 Nach Art. 58 Abs. 2 DSGVO.

G.1.3 Videoüberwachung im Fahrgastraum gestoppt

Im Zuge eines Verwaltungsverfahrens stellte ein Beförderungsunternehmen die Überwachung von Fahrerinnen und Fahrern sowie Kundinnen und Kunden mit Videokameras ein. Der Fall zeigt, dass auch bei schwerwiegenden Verstößen die Kooperation mit der Aufsichtsbehörde positive Effekte auf das weitere Verfahren haben kann.

Bei einem Beförderungsunternehmen in Niedersachsen hatte unsere Behörde eine unzulässige Videoüberwachung festgestellt. Das Unternehmen hatte im Innenraum seiner Fahrzeuge Videokameras angebracht und damit dauerhaft sowohl die Kundinnen und Kunden als auch die Fahrerinnen und Fahrer überwacht.

Damit wollte sich das Unternehmen absichern, um bei möglichen Schadensfällen straf- oder zivilrechtliche Ansprüche geltend machen zu können. Dafür gab die weit überwiegende Mehrzahl der Betroffenen jedoch überhaupt keinen Anlass. Diese dauerhafte und anlasslose Überwachung des Fahrzeuginnenraums, dem die Betroffenen nicht ausweichen können, stellt einen schwerwiegenden Verstoß dar.[1]

Unternehmen kooperiert mit Behörde

Häufig stellen sich Unternehmen erst einmal quer, wenn unsere Behörde bei solch schweren Grundrechtseingriffen ein Verwaltungsverfahren einleiten muss.

Nicht so in diesem Fall: Das Unternehmen war während der gesamten Überprüfung ausgesprochen kooperativ und teilte abschließend mit, dass es die Videoüberwachung in den Fahrzeugen vollständig abgestellt und die gespeicherten Aufnahmen vernichtet habe.

1 Siehe dazu auch die DSK-Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", September 2020, Kurzlink: https://t1p.de/video2020 (PDF).

DSK

Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen[1]

Stand: 17. Juli 2020

Redaktion: Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

[1] Unter dem Begriff der „nicht-öffentliche Stellen" sind natürliche Personen, juristische Personen des Privatrechts unabhängig von ihrer Rechtsform und der Art ihrer Betätigung, z. B. eingetragene Vereine, Genossenschaften, Kapital- und Personengesellschaften des Privatrechts (z. B. GmbH, AG, OHG, KG, GmbH und Co. KG, GbR), und andere privatrechtlich organisierte Personenvereinigungen (z. B. Genossenschaften, nichteingetragene Vereine, Gewerkschaften, Parteien, Berufsverbände, Gruppierungen ohne Rechtspersönlichkeit) zu verstehen.

DSK

Inhalt

2

Hinweise zum datenschutzkonformen Einsatz von Videoüberwachung bietet die entsprechende Orientierungshilfe der Datenschutzkonferenz.

Das Verwaltungsverfahren konnte daraufhin beendet werden. Im wegen der hohen Eingriffsintensität eröffneten und noch laufenden Bußgeldverfahren wird dieses kooperative Verhalten Berücksichtigung finden und sich auch auf die Höhe des zu verhängenden Bußgeldes positiv für das Unternehmen auswirken.

G.1.4 Enge Grenzen für die Videoüberwachung an Schulen

Videoüberwachung im Bereich von Schulen ist nur dann erlaubt, wenn eine wirksame Einwilligung vorliegt oder eine Rechtsvorschrift dies vorsieht. Beides ist im Schulbereich besonders heikel – die Datenschutzbehörde Niedersachsen hat dazu eine Orientierungshilfe veröffentlicht.

Um die Zulässigkeit einer Videoüberwachung an öffentlichen Schulen zu beurteilen, ist es entscheidend, ob diese während oder außerhalb der Schulzeit und in einem öffentlich oder in einem nicht öffentlich zugänglichen Bereich erfolgen soll. Rechtsgrundlage für den Einsatz von Videoüberwachungstechnik in öffentlich zugänglichen Bereichen in Schulen ist § 14 des Niedersächsischen Datenschutzgesetzes (NDSG), für nicht öffentlich zugängliche Bereiche kann in Ausnahmefällen auf ein berechtigtes Interesse gemäß Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DSGVO) zurückgegriffen werden. Wichtig: Die Erlaubnis für Videoüberwachungen umfasst regelmäßig keine Tonaufnahmen. Sollten dennoch Audiofunktionen benutzt worden sein, sind etwaige Tonaufnahmen unverzüglich zu löschen.

Videoüberwachung in öffentlich zugänglichen Bereichen während der Schulzeiten

Öffentlich zugängliche Bereiche sind Gebäude und Freiflächen, die dazu bestimmt sind, von einer unbestimmten Zahl von Menschen betreten oder genutzt zu werden. Hierzu gehören in der Regel das Schulgebäude selbst, insbesondere Eingangsbereich, Flure und Pausenhallen – aber nicht die Lehrerzimmer. Im Außenbereich zählen meist Fahrradständer, Parkplätze, Schulhof und Sportgelände dazu.

Während der Schulzeiten ist eine Videoüberwachung in öffentlich zugänglichen Bereichen aufgrund der schutzwürdigen Interessen der von der Videoüberwachung betroffenen Personen grundsätzlich ausgeschlossen.[1]

1 § 14 Abs. 1 NDSG.

In Schulen ist eine Videoüberwachung in der Regel ausgeschlossen (Symbolbild).

Sie stellt regelmäßig einen schweren Eingriff in die Persönlichkeitsrechte von Schülerinnen und Schülern, Lehrkräften und anderen an der Schule tätigen Personen dar.

Auch Argumente der Aufsichtspflicht können hier nicht ins Feld geführt werden: Das Niedersächsische Schulgesetz (NSchG) sieht keine Rechtsgrundlage für den Einsatz technischer Mittel vor, um so die Aufsichtspflicht auszuüben. Vielmehr ist darin ausdrücklich die persönliche Aufsichtspflicht enthalten.[2]

Eine Ausnahme kann die Überwachung der Fahrradständer beziehungsweise des Fahrradkellers und des Parkplatzes sein, sofern überwachungsfreie Ausweichmöglichkeiten zur Verfügung stehen. Die Nutzung im überwachten Bereich ist damit „freiwillig". Aufgrund dieser „Freiwilligkeit" steht der Videoüberwachung dieser Bereiche auch nicht mehr die Schulpflicht oder das Dienst- beziehungsweise Arbeitsverhältnis (Über-/Unterordnungsverhältnis) entgegen. Denn die Schülerinnen, Schüler und Lehrkräfte sind nicht gezwungen, die überwachten Fahrradständer und Parkplätze zu nutzen. Insofern fällt dann die Abwägung gemäß § 14 NDSG zugunsten der Videoüberwachung aus.

2 § 62 Abs. 1 NSchG.

Videoüberwachung in öffentlich zugänglichen Bereichen außerhalb der Schulzeiten

Schulen sind außerhalb der Schulzeiten in der Regel nicht dazu bestimmt, von einem unbestimmten Personenkreis betreten und genutzt zu werden. Sie sind somit dann keine öffentlich zugänglichen Räume. Sofern jedoch Räume oder Flächen der Schule für die Öffentlichkeit freigegeben werden, sind sie öffentlich zugänglich. Dazu zählen beispielsweise:

- die Aula bei öffentlichen Konzerten,
- die Sporthalle, wenn sie von Vereinen benutzt wird,
- die Klassenräume, wenn dort etwa Volkshochschulkurse stattfinden,
- der Zugang zu diesen Bereichen sowie
- bei einer entsprechenden Freigabe der Nutzung die Außenanlagen wie Schulhof, Parkplatz oder Sportgelände.

Die Videoüberwachung dieser öffentlich zugänglichen Bereiche ist unter strengen Voraussetzungen zulässig, unter anderem wenn sie zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.[3] Das kann zum Beispiel der Schutz von Personen sein, die der beobachtenden Stelle (in diesem Fall der Schule) angehören oder diese aufsuchen, oder aber der Schutz von Sachen, die zu der beobachtenden Stelle oder zu den zu schützenden Personen gehören. Ein anderes Beispiel ist die Wahrnehmung des Hausrechts der beobachtenden Stelle.

Videoüberwachung stellt regelmäßig einen schweren Eingriff in die Persönlichkeitsrechte von Schülerinnen, Schülern und Lehrkräften dar.

Zudem müssen weitere Voraussetzungen (legitimer Zweck, Eignung, Erforderlichkeit, Angemessenheit) erfüllt sein. Weitere Einzelheiten dazu finden Sie in unserer Orientierungshilfe zu dem Thema.

Videoüberwachung in nicht öffentlich zugänglichen Bereichen

Während der Schulzeiten ist eine Videoüberwachung in nicht öffentlich zugänglichen Bereichen genauso wie in öffentlich zugänglichen Räumen

3 § 14 Abs. 1 S. 1 und S. 2 NDSG.

grundsätzlich ausgeschlossen. In Ausnahmefällen kann eine Videoüberwachung in nicht öffentlich zugänglichen Bereichen während der Schulzeit möglich sein, beispielsweise in Server-, Tresor- und Archivräumen. Da §14 NDSG nur den Einsatz im öffentlichen Bereich umfasst, kommt dann als Rechtsgrundlage eine Rechtmäßigkeit der Verarbeitung nach DSGVO in Betracht.[4] Dies gilt ebenso für den Einsatz außerhalb der Schulzeiten in nicht öffentlich zugänglichen Bereichen.

Fazit

Bis auf wenige Ausnahmen ist die Videoüberwachung im Schulbereich ausgeschossen. Mehr dazu lesen Sie in unserer ausführlichen Orientierungshilfe zur Videoüberwachung an Schulen, die wir Ende 2023 aktualisiert und komplett überarbeitet haben.[5]

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

5 Orientierungshilfe zur Videoüberwachung an Schulen: https://lfd.niedersachsen.de/download/201751.pdf (PDF).

Digitale Medien

G.2.1 Datenschutzrechtliche Bewertung von ChatGPT

Seit November 2022 ist der Dienst ChatGPT auch in Europa kostenlos verfügbar und in aller Munde. Über keine andere Künstliche Intelligenz wurde so viel von den Medien berichtet und in der Öffentlichkeit diskutiert. Die erste datenschutzrechtliche Bewertung des Dienstes kam von der italienischen Datenschutzaufsichtsbehörde GPDP, die im Februar 2023 die Bereitstellung von ChatGPT aufgrund von datenschutzrechtlichen Mängeln in Italien untersagte. Aus diesem Anlass haben auch wir zusammen mit anderen deutschen Aufsichtsbehörden eine Bewertung von ChatGPT vorgenommen.

ChatGPT ist ein Chatbot[1], der auf dem KI-Sprachmodell (englisch: Large Language Model) GPT-4 basiert. Technisch gesehen ist es ein neuronales Netz für maschinelles Lernen, das mit enormen Datenmengen trainiert wird (mehr dazu in Kapitel E). Personen können sich über verschiedenste Themen mit ChatGPT unterhalten und Fragen stellen. Der Chatbot generiert Texte, Softwarecode und seit der Integration des Bildgenerators Dall-E inzwischen auch Fotos und Bilder.

Die öffentliche Debatte dreht sich insbesondere um die Nutzung von ChatGPT durch Schülerinnen und Schüler und Studentinnen und Studenten, um von der KI Hausaufgaben und Hausarbeiten schreiben zu lassen.[2] In der Arbeitswelt reicht das Spektrum von durch Medienschaffende mit-

1 Ein Chatbot ist ein Computerprogramm, das künstliche Intelligenz (KI) und natürliche Sprachverarbeitung nutzt, um Dialog zwischen Mensch und einem technischen System zu ermöglichen.

2 Die Fakultät für Betriebswirtschaft der Wirtschaftsuniversität Prag hat aus diesem Grund Bachelorarbeiten abgeschafft, siehe FAZ, Erste Uni schafft Bachelorarbeiten ab, 1.12.2023, https://t1p.de/faz-ki (Kurzlink)

tels ChatGPT erstellte Artikel, über Vertragsentwürfe und Schriftsätze in gerichtlichen Verfahren, die vermeintlich von Rechtsanwälten stammen, bis hin zu einem Verordnungsentwurf, der ohne Änderungen übernommen worden ist.[3] In diesem Zusammenhang geht es in der öffentlichen Debatte um die Korrektheit und Wahrheit der Ergebnisse von ChatGPT ebenso wie die Transparenz in Bezug auf die Herstellung der Texte.

Datenschutzrechtliche Erkenntnisse

Die datenschutzrechtliche Bewertung von ChatGPT erfordert es, unterschiedliche Phasen der Verarbeitung zu differenzieren. Bevor ChatGPT von der Öffentlichkeit genutzt werden konnte, sind bereits für das Training des Large Language Models in sehr großem Umfang personenbezogene Daten verarbeitet worden, die auch besonders sensible Daten („besondere Kategorien personenbezogener Daten"[4]) umfassen. Die Trainingsdaten für ChatGPT stammen nach Angaben des Unternehmens OpenAI überwiegend aus dem Internet. Genaue Details über die einzelnen Datensätze und ihre Quellen wurden allerdings nicht öffentlich bekanntgegeben.

Laut OpenAI werden in dem neuronalen Netz von GPT-4 keine personenbezogenen Daten verarbeitet: Es ist allerdings nicht bekannt, welche Daten in der sogenannten verdeckten Schicht des neuronalen Netzes verarbeitet werden. Nutzt eine Person ChatGPT, ist zwischen den Eingabe- und Ausgabedaten zu unterscheiden. In den Fragen und Aufgaben, die bei ChatGPT eingegeben werden, können ebenso wie in den Ausgaben, die die KI liefert, personenbezogene Daten enthalten sein.

Personenbezogene Trainingsdaten

Bei der abstrakten datenschutzrechtlichen Bewertung von ChatGPT steht die Rechtmäßigkeit der Verarbeitung von personenbezogenen Trainingsdaten im Fokus. Es gibt Filtertechniken, die den Umfang von personenbezogenen Trainingsdaten aus dem Internet reduzieren – insbesondere durch den Ausschluss von Webseiten wie checkpeople.com oder gnomecat.net, die gezielt Daten über Personen sammeln. Allerdings werden selbst mit

3 Siehe heise online, Brasilien: Erste vollständig von KI geschriebene Verordnung, 4.12.2023, https://heise.de/-9548331

4 Art. 9 DSGVO.

diesen Filtern allein aufgrund des sehr großen Umfangs der Trainingsdaten aus dem Internet immer noch eine hohe Anzahl personenbezogener Daten verarbeitet.

Für diese Verarbeitung kommt als einzig mögliche Rechtsgrundlage Artikel 6 Absatz 1 Buchstabe f der Datenschutz-Grundverordnung (DSGVO) in Betracht, also die Abwägung des berechtigten Interesses des Verantwortlichen mit den Interessen der Betroffenen. Selbst wenn ein berechtigtes Interesse von OpenAI anerkannt würde, kann aber weder pauschal davon ausgegangen werden, dass die Interessen der Betroffenen überwiegen, noch dass dies nicht der Fall ist.

Allein die Tatsache der Veröffentlichung im Internet führt nicht dazu, dass die personenbezogenen Daten von jedem zu jedem beliebigen Zweck verarbeitet werden dürfen. Dieser Annahme steht schon der Grundsatz der Zweckbindung in der DSGVO[5] entgegen. Auch dem Grundsatz der Datensparsamkeit wird in Bezug auf den Umfang personenbezogener Trainingsdaten keine Rechnung getragen, da sich die Qualität des Large Language Modells gerade durch die Anzahl der Parameter bestimmt.

In vielen Fällen ist nicht prüfbar, ob die besonders sensiblen personenbezogenen Daten vom Betroffenen selbst[6] oder mit seinem Einverständnis[7] im Internet veröffentlicht worden sind. Einmal im Internet veröffentlichte Daten können nicht vollständig wieder gelöscht werden und entziehen sich grundsätzlich der Kontrolle durch den Betroffenen. Es gibt keine Mechanismen, durch die die Aktualität im Sinne der Richtigkeit der Daten gewährleistet wird.

Ob spezifische Filter eingesetzt werden, um den Anteil besonders geschützter Daten wie Gesundheitsdaten, politische Meinungen oder eine Gewerkschaftszugehörigkeit in den Trainingsdaten gezielt zu reduzieren, ist nicht bekannt. Bei besonderen Kategorien personenbezogener Daten wird eine Einwilligung der betroffenen Person[8] aus den bereits genannten Gründen in vielen Fällen als Rechtsgrundlage ausscheiden. Weiterhin ist

5 Art. 5 Abs. 1 Buchst. b DSGVO.
6 Art. 9 Abs. 2 Buchst. e DSGVO.
7 Art. 9 Abs. 2 Buchst. a DSGVO.
8 Art. 9 Abs. 2 Buchst. e DSGVO.

nicht davon auszugehen, dass die Voraussetzungen einer anderen Rechtsgrundlage gemäß DSGVO[9] erfüllt werden.

Solange es dem Unternehmen OpenAI nicht gelingt, nachzuweisen, dass das Training des Large Language Models von ChatGPT datenschutzkonform erfolgt ist, wirkt sich dieser Mangel auf die Möglichkeit der datenschutzkonformen Nutzung aus. Öffentliche und nicht-öffentliche Stellen, die ChatGPT oder KI-Anwendungen auf Basis des Large Language Models GPT-4 nutzen wollen, müssen als Verantwortliche die Datenschutzkonformität gewährleisten können.

Personenbezogene Eingabe- und Ausgabedaten

Werden bei der Nutzung von ChatGPT personenbezogene Daten eingegeben, muss auch dies auf eine Rechtsgrundlage gestützt werden können. Dabei ist zu prüfen, ob die Ein- und Ausgabedaten über die Beantwortung der Fragen und Aufgaben hinaus vom Anbieter des Dienstes für das weitere Training des Large Language Modells genutzt werden. Dieser weitere Zweck muss ebenfalls durch eine Rechtsgrundlage gedeckt sein oder die Verarbeitung zu Trainingszwecken muss zuverlässig unterbunden werden.

Sind von den Ausgabedaten auch personenbezogene Daten umfasst, ist zu berücksichtigen, dass ChatGPT nicht gewährleistet, dass diese Daten richtig sind. Der Dienstanbieter weist an mehreren Stellen in der Webanwendung und der App darauf hin, dass ChatGPT falsche Informationen geben kann und sich Nutzende nicht auf die Ergebnisse des Dienstes als alleinige Quelle von Wahrheits- oder Tatsacheninformationen oder als Ersatz für professionelle Beratung verlassen sollten.

Aufgrund der Architektur von Large Language Models bestehen nur eingeschränkte Möglichkeiten der Umsetzung der Betroffenenrechte.

Betroffenenrechte

Werden personenbezogene Daten in den Dienst bei den Frage- und Aufgabenstellungen eingegeben und enthalten die Ausgaben personenbezogene Daten, so ist zu berücksichtigen, dass die Betroffenenrechte gewährleistet werden müssen. Aufgrund der Architektur von Large Language Models

9 Art. 9 Abs. 2 DSGVO.

bestehen nur eingeschränkte Möglichkeiten der Umsetzung der Betroffenenrechte auf Korrektur oder Löschung der personenbezogenen Daten. Dies ist immer problematisch, wird aber besonders deutlich bei der Ausgabe von falschen personenbezogenen Daten.

Neben diesen Schwerpunkten werden noch weitere Datenschutzaspekte in Bezug auf ChatGPT von den Datenschutzaufsichtsbehörden wie beispielsweise die Angemessenheit der technischen und organisatorischen Maßnahmen geprüft.

Fazit

ChatGPT ist aufgrund des hohen Bekanntheitsgrades das erste von der Allgemeinheit niedrigschwellig nutzbare KI-System, auf das auch die Datenschutzaufsichtsbehörden ihre Aufmerksamkeit gerichtet haben. Die datenschutzrechtliche Bewertung wird mit dem Ziel vorgenommen, potenziellen Nutzenden in Deutschland – insbesondere Unternehmen, Behörden, Vereinen und anderen Organisationen – Handlungsempfehlungen für die Nutzung zu geben. Es ist davon auszugehen, dass die in Bezug auf ChatGPT gewonnenen datenschutzrechtlichen Erkenntnisse auf andere Large Language Models wie Google Bard beziehungsweise Gemini übertragen werden können.

Prüfung von Medienwebseiten deckt Datenschutzmängel auf – sind Abo-Modelle Teil der Lösung oder Teil des Problems? G.2.2

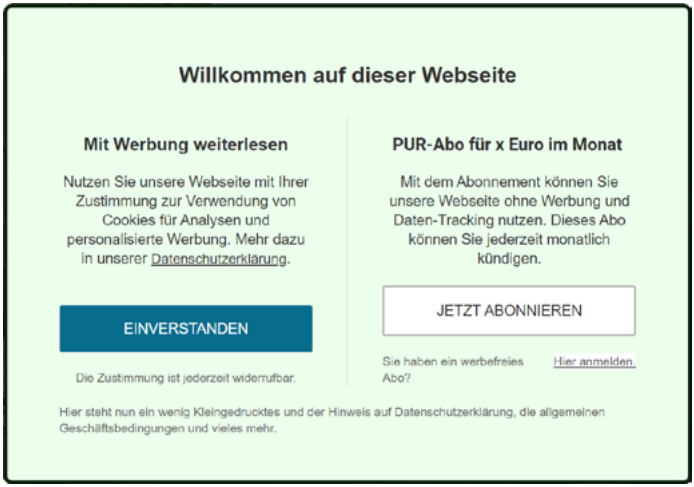
Seit 2021 prüfen Datenschutzaufsichten bundesweit die Webangebote von Medienunternehmen. Vor allem in Bezug auf Nutzertracking zu Werbezwecken und dem Einsatz von Cookies gab es viel zu beanstanden – auch bei den fünf in Niedersachsen untersuchten Unternehmen. Infolge unserer Untersuchung verbesserten die Firmen den Datenschutz auf ihren Medienportalen, sodass wir die Prüfung im Jahr 2023 abschließen konnten.

Im Rahmen einer bundesweiten Prüfung haben die Datenschutzbeauftragten von 11 Bundesländern seit 2021 insgesamt 49 Webangebote von Medienunternehmen untersucht und das Verfahren im Jahr 2023 abgeschlossen. Die Datenschutzbehörde Niedersachsen hatte dabei insgesamt fünf in Niedersachsen ansässige Medienunternehmen mit ihren Angeboten im Blick. Über die ersten Ergebnisse hatten wir in unserem Tätigkeitsbericht 2021 bereits berichtet.[1]

In Folge der Analyse mussten die Anbieter auf ihren Webseiten aufgrund verschiedenster datenschutzrechtlicher Mängel teils erheblich nachbessern. Eine augenfällige Entwicklung in diesem Zusammenhang ist die Einführung sogenannter Pur-Abo-Modelle bei vielen publizistischen Webangeboten.

Zu Beginn der niedersächsischen Prüfung hatten die geprüften Medienunternehmen auf ihren Webseiten eine sehr hohe Anzahl von bis zu 760 Cookies und Drittdiensten eingebunden. Diese dienten mehrheitlich dem Tracking der Nutzerinnen und Nutzer und der Ausspielung von personalisierter Werbung auf Basis der in Echtzeit stattfindenden Auktionierung von Werbeplätzen (Real Time Bidding). Alle fünf in Niedersachsen geprüften Webseiten entsprachen nicht den rechtlichen Anforderungen für den

1 Siehe Tätigkeitsbericht 2021, J.8.2.



Beispiel für ein Einwilligungsbanner mit Pur-Abo-Modell.

Einsatz von Cookies und anderen Trackingtechniken.[2] Auf den Webseiten fanden sich Einwilligungsbanner, über die keine wirksamen datenschutzrechtlichen Einwilligungen der Nutzer eingeholt worden waren. Die Einwilligungsbanner waren unter anderem irreführend in ihrer Gestaltung (sogenannte Dark Patterns), sodass Nutzerinnen und Nutzer gar nicht in der Lage waren, ihre Einwilligungen freiwillig erteilen zu können, und die Informationen waren völlig unzureichend oder zu wenig differenziert. Über die datenschutzrechtlichen Defizite informierte unsere Behörde die Medienunternehmen in umfassenden Auswertungsschreiben und gab ihnen Gelegenheit, zu den geplanten aufsichtsbehördlichen Maßnahmen Stellung zu nehmen.

Neues Gesetz und Abo-Modelle

Vor Abschluss der Prüfung kamen zwei wesentliche Entwicklungen zum Tragen. Erstens trat am 1. Dezember 2021 das Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) in Kraft. In die rechtliche Prüfung mussten wir daher den neuen § 25 TTDSG einbeziehen. Konkrete rechtliche

2 Siehe Pressemeldung des LfD Niedersachsen vom 30.6.2021: https://lfd.niedersachsen.de/201900.html

Bewertungsmaßstäbe hatte die Datenschutzkonferenz (DSK) zuvor in der neuen Orientierungshilfe für Anbieter von Telemedien 2021 festgelegt.[3]

Zweitens begannen die Medienunternehmen sukzessive in ihre Einwilligungsbanner sogenannte Pur-Abo-Modelle zu integrieren. Bei einem Pur-Abo-Modell können Nutzer einer Webseite über den Einwilligungsbanner zwischen zwei Möglichkeiten wählen, die Inhalte zu lesen. Entweder schließen sie ein Pur-Abonnement ab, um die Webseite ohne Nutzertracking, individuelle Profilbildung und personalisierte Werbung zu nutzen, oder sie willigen ohne Pur-Abonnement in diese Vorgänge ein. Im Rahmen der koordinierten Medienprüfung erfolgte eine umfassende rechtliche Bewertung von Pur-Abo-Modellen, die in einem entsprechenden Beschluss der DSK veröffentlicht worden sind.[4]

Die Medienunternehmen haben die Forderungen in Bezug auf die datenschutzkonforme Ausgestaltung der Einwilligungsbanner einschließlich des integrierten Pur-Abo-Modells anerkannt und weitgehend umgesetzt. Auf noch verbleibende datenschutzrechtliche Defizite haben wir die Medienunternehmen in umfassenden Abschlussschreiben verbunden mit dem Vorbehalt einer erneuten Überprüfung hingewiesen.

Fazit

Der länderübergreifende, koordinierte Ansatz dieser Prüfung hat sich bewährt, denn eine einheitliche und abgestimmte Bewertung der Webseiten der Medienbranche, der vor allem gesellschaftlich ein hohes Gewicht zukommt, war hier geboten. Die Prüfung hat uns allerdings auch deutlich vor Augen geführt, wie schnelllebig das Web ist. Bereits unmittelbar nach dem Abschluss der Medienprüfung hatten die Unternehmen ihre Webseiten erneut geändert.

Damit die mit der Medienprüfung erreichten Verbesserungen der Datenschutzkonformität nachhaltig wirken, beabsichtigen wir, in absehbarer Zeit von dem Vorbehalt Gebrauch zu machen, eine Nachprüfung vorzunehmen.

3 Kurzlink zur Orientierungshilfe: https://t1p.de/telemedien (PDF).
4 Kurzlink zum Beschluss: https://t1p.de/pur-abo (PDF).

G.2.3 Daten nach Streit ins Netz gestellt – behördliche Maßnahmen notwendig

Im Tätigkeitsbericht 2022 haben wir von einem Trend berichtet, komplette Gesprächsverläufe und andere persönliche Daten nach Konflikten mit Bekannten, Unternehmen oder Kunden rechtswidrig im Internet zu veröffentlichen. Zu unserem Bedauern hält dieser Trend an, weshalb wir auch im Berichtszeitraum Maßnahmen gegenüber den für die Veröffentlichung Verantwortlichen ergriffen haben.

Auch im Jahr 2023 erreichten uns zahlreiche Beschwerden von Personen, deren personenbezogene Daten nach einem Streit im Internet veröffentlicht worden sind. Die Verantwortlichen stellten in diesen Fällen persönliche Fotos, E-Mail-Korrespondenzen oder andere Inhalte ohne eine entsprechende Rechtsgrundlage[1] ins Netz, sie haben dadurch personenbezogene Daten rechtswidrig verarbeitet.

Besonders häufig ging es um Kommentare auf Rezensionsplattformen – insbesondere bei der Bewertung von Unternehmensprofilen in der Google-Suchmaschine. In einem dieser Fälle etwa hatte die Inhaberin eines Sportfachhandels als Reaktion auf eine negative Unternehmensbewertung die vollständigen E-Mail-Korrespondenz zwischen dem Betroffenen und dem Unternehmen veröffentlicht. Da hierdurch Klarname, Wohnort und E-Mail-Adresse des Betroffenen einer nicht einschätzbaren Anzahl von Personen öffentlich zugänglich waren, haben wir die Verantwortliche[2] kostenpflichtig verwarnt.

In einem anderen Fall hatte die Betreiberin eines privaten Blogs personenbezogene Daten von einem in einem Gerichtsverfahren beteiligten Justizbediensteten ins Netz gestellt. Da sich die Verantwortliche hinsichtlich Ihres Verstoßes gegen die Datenschutz-Grundverordnung auch nach einer er-

1 Siehe Art. 6 Abs. 1 DSGVO.
2 Gemäß Art. 58 Abs. 2 Buchst. b DSGVO.

gangenen Anordnung zur Löschung uneinsichtig gezeigt hat, mussten wir ein zusätzliches Zwangsgeld[3] verhängen.

Vor dem Hintergrund dieses Trends haben wir bereits im Jahr 2022 ein Informationsschreiben[4] veröffentlicht, mit dem wir die Öffentlichkeit sensibilisieren wollen – und hoffentlich dazu beitragen, solche Datenschutzverstöße künftig zu vermeiden.

Veröffentlichungen personenbezogener Daten im Internet ohne Rechtsgrundlage gehen mit schwerwiegenden Grundrechtseingriffen bei den Betroffenen einher, da Beiträge im Internet eine nicht einschätzbare Reichweite haben und häufig nicht wieder lückenlos gelöscht werden können. Vor diesem Hintergrund werden wir in ähnlichen bereits anhängigen Verfahren sowie bei weiteren 2024 zu erwartenden Fällen entsprechende aufsichtsbehördliche Maßnahmen ergreifen.

Schwerwiegende Grundrechtseingriffe bei den Betroffenen

3 Gemäß Art. 58 Abs. 2 Buchst. j DSGVO.

4 Abrufbar unter https://lfd.niedersachsen.de/218440.html

G.2.4 Einwilligungsbedürftige Verarbeitungen in Webshops

Wer in Online-Shops ohne Registrierung über einen Gastzugang bestellt, tut etwas für den Selbstdatenschutz. Die eigentliche Nutzung der Bestellformulare hält in manchen Fällen jedoch eine Überraschung bereit – auch für den Shop-Betreiber.

Wenn ein Webshop mehr Daten verarbeitet als für den Bestellvorgang selbst erforderlich ist, dann ist in der Regel für diese zusätzliche Verarbeitung eine Einwilligung des Nutzers einzuholen.

Anlegen eines registrierten Nutzerzugangs

Webshops müssen in der Regel die Möglichkeit eröffnen, eine Bestellung über einen Gastzugang aufzugeben. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat dies in ihrem diesbezüglichen Beschluss aus Anfang 2022 klargestellt.[1] Diese grundsätzliche Anforderung wird durch viele Webshops eingehalten, gleichwohl erreichten uns einige Beschwerden, die einen Verstoß speziell gegen diese Anforderung rügten.

In einem herauszuhebenden Fall wurden die Zugangsdaten zu einem Nutzerkonto durch den Webshop bereits zu einem Zeitpunkt versandt, in dem die Neukundin oder der Neukunde den Bestellprozess noch nicht abgeschlossen hatte. Nach entsprechenden Hinweisen durch die niedersächsische Datenschutzaufsicht kam es zu einer technischen Umstellung. Eine E-Mail mit den Zugangsdaten wurde nun erst nach Abschluss des Bestellprozesses versandt. Der Verantwortliche stellte dar, dass ein Nutzerzugang erst dann registriert würde, wenn die Zugangsdaten tatsächlich genutzt würden. Dies ging aus der E-Mail jedoch nicht hinreichend deutlich hervor, sodass eine Einwilligung durch Nutzung der Zugangsdaten nicht informiert und damit unwirksam erfolgt wäre. Nach einer weiteren Intervention stellte der Verantwortliche diese Praxis schließlich ein.

1 Siehe DSK, Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang, März 2022, Kurzlink: https://t1p.de/gastzugang (PDF).

E-Mails zur Erinnerung an den Warenkorb

Im Tätigkeitsbericht 2021[2] hat unsere Behörde die allgemeine Rechtslage zu E-Mail-Werbung durch Online-Händler dargestellt. Webshops versenden E-Mails mit werbendem Charakter aber auch, um an einen gefüllten, jedoch nicht bestellten Warenkorb zu erinnern. Dies ist in der Regel nur mit Einwilligung rechtmäßig. In einem Fall machte der Verantwortliche als Ursache für seinen Verstoß einen eigenen Organisationsfehler aus: Die Funktion des Webshops zum Versenden derartiger E-Mails war bereits aktiviert, nicht jedoch die beabsichtigte Funktion zum Einholen entsprechender Einwilligungen.

In einem berichtenswerten Fall befüllten Neukundinnen und Neukunden den Warenkorb, füllten das Bestellformular aus und entschieden sich sodann für den Abbruch der Bestellung. Gleichwohl wurden die angegebenen Daten erfasst und die Betroffenen erhielten Warenkorb-Erinnerungs-E-Mails. Bei demselben Verantwortlichen war zudem eine Irreführung der Nutzer festzustellen: Beim Speichern eines Produktes in den Warenkorb erschien ein Pop-up, das den Eindruck vermittelte, die Angabe der Telefonnummer oder der E-Mail-Adresse sei erforderlich, um das Produkt in den Warenkorb abzulegen. Tatsächlich war dies aber nicht notwendig. Auch in diesem Fall führten unsere Hinweise dazu, dass dieser Verantwortliche die rechtswidrige Praxis abstellte, die Erinnerungsfunktion transparent darstellte und eine Einwilligung einholte.

Verantwortliche müssen die technische Umsetzung im Blick behalten.

Fazit

Verantwortliche müssen neben der Rechtmäßigkeit ihrer Verarbeitungen auch die technische Umsetzung, insbesondere bei der Einführung neuer Funktionen dauerhaft im Blick behalten. Organisatorisch erfordert dies einen Prozess, der bei Produktivsetzung des Webshops und neuer Funktionen beginnt, und die regelmäßige Überprüfung über den gesamten Lebenszyklus des Shops hinweg einschließt.

2 Siehe Tätigkeitsbericht 2021, J.6.4.

G.2.5 Gefährliche Bequemlichkeit – Cyber-Kriminelle verschaffen sich Zugang zu über 20.000 Onlinekonten

Im Jahr 2023 haben uns drei niedersächsische Unternehmen den unbefugten Zugang zu insgesamt über 20.000 Onlinekonten durch sogenannte Credential-Stuffing-Angriffe gemeldet.

Bei Credential Stuffing greifen Kriminelle auf zuvor abhandengekommene, zumeist gestohlene Zugangsdaten (Credentials) von Nutzerinnen und Nutzer zurück. Die Angreifenden versuchen mit Hilfe der zuvor erbeuteten Zugangsdaten wie beispielsweise der Kombination aus E-Mail-Adresse und Passwort auch auf anderen Plattformen, vor allem in Online-Shops, Zugang zu den Nutzerkonten zu erhalten. Die Angriffe laufen automatisiert und meist in großem Ausmaß ab.

Dabei machen sich Cyber-Kriminelle die Bequemlichkeit vieler Nutzerinnen und Nutzer zunutze, dieselben Zugangsdaten bei mehreren Konten zu verwenden. Diese Bequemlichkeit ist gefährlich, denn sie erhöht bei einem gestohlenen Passwort den potenziellen Schaden. Die erbeuteten Zugangsdaten nutzen die Angreifer entweder selbst oder bieten sie im Darknet zum Verkauf an – oft als Listen mit Tausenden erbeuteter Credentials.

Die Meldungen der Unternehmen an unsere Behörde[1] aus dem vergangenen Jahr zeigen, dass diese Angriffsmethode immer wieder erfolgreich ist und eine zunehmende Gefahr für die Daten von Onlinekonten darstellt. So konnten sich die Angreifenden allein bei drei niedersächsischen Unternehmen durch diese Angriffsstrategie in Summe Zugang zu über 20.000 Onlinekonten verschaffen. Hierdurch können die im Konto gespeicherten Daten wie beispielsweise Name, Anschrift, Geburtsdatum, E-Mail-Adresse oder auch Kaufhistorie und gegebenenfalls Kreditkartendaten eingesehen werden.

Mit diesen Daten können die Kriminellen ihre bestehenden Listen mit weiteren Informationen über die jeweiligen Personen anreichern und für be-

1 Meldungen von Datenschutzverletzungen nach Art. 33 DSGVO durch Verantwortliche.

trügerische Absichten nutzen – zum Beispiel für weitere Credential-Stuffing-Angriffe. In den gemeldeten Fällen haben die Verantwortlichen nach Bekanntwerden der Angriffe die betroffenen Kundinnen und Kunden informiert. Durch Änderung der Passwörter konnten die Hacker an einem weiteren Zugriff auf die betroffenen Onlinekonten gehindert werden. Die Kundinnen und Kunden hatten in der Folge zeitnah die Möglichkeit, die Passwörter zurückzusetzen und dadurch wieder vollen Zugang zu ihren Konten zu erlangen.

Schutzmaßnahmen

Damit es gar nicht so weit kommt, können Unternehmen, aber auch Nutzerinnen und Nutzer Maßnahmen ergreifen, um sich vor Passwortattacken wie dem Credential Stuffing zu schützen. Grundsätzlich sind zunächst die Unternehmen in der Pflicht, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Als effektivste Maßnahme gegen Credential Stuffing empfiehlt das Open Web Application Security Project (OWASP) die Implementierung einer Multi-Faktor-Authentifizierung.[2] Auch nach unserer Auffassung ist dies derzeit ein geeigneter Schutz.

Daneben können auch die Nutzerinnen und Nutzer zur Sicherheit ihrer Onlinekonten beitragen. Zunächst sollten sie niemals dasselbe Passwort für mehrere Dienste verwenden. Die Grundregel lautet: Für jeden Dienst ein eigenes Passwort. Um den Überblick über die unterschiedlichen Zugangsdaten zu behalten, empfehlen wir das Verwenden eines Passwortmanagers. Dieser hilft in der Regel außerdem beim Erzeugen guter Passwörter.[3] Wir raten außerdem dazu, Multi-Faktor-Authentifizierung auf denjenigen Webseiten zu aktivieren, die dies anbieten. Ferner sollten Nutzerinnen und Nutzer ihre Passwörter so schnell wie möglich ändern, wenn ein Verantwortlicher sie über einen Sicherheitsvorfall informiert.

Grundregel: Für jeden Dienst ein eigenes Passwort.

2 Siehe OWASP zur Authentifizierung, Kurzlink: https://t1p.de/owasp

3 Zu sicheren Passwörtern siehe auch die Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI): https://bsi.bund.de/dok/6596574

Wirtschaft

G.3.1 Weiterhin kein ausreichender Beschäftigtendatenschutz bei Amazon in Winsen

Im Berichtszeitraum erließ das Verwaltungsgericht Hannover ein Urteil gegen die niedersächsische Datenschutzaufsicht, das sowohl bundes- als auch europaweit auf viel Kritik und Unverständnis stieß.

Im Tätigkeitsbericht der niedersächsischen Datenschutzaufsicht aus dem Jahr 2020 stellten wir die Situation der Beschäftigten bei der Amazon Logistik Winsen GmbH dar: Um online bestellte Waren an Kundinnen und Kunden zu zugesagten Terminen liefern zu können, erhebt und nutzt die Amazon Logistik Winsen GmbH ununterbrochen Beschäftigtendaten.[1]

Wir haben deshalb der Amazon Logistik Winsen GmbH die ununterbrochene Erhebung und Verwendung von bestimmten Beschäftigtendaten untersagt.[2] Dagegen erhob das Unternehmen Klage vor dem zuständigen Verwaltungsgericht Hannover.

Das Verwaltungsgericht Hannover entschied Anfang 2023, dass die Amazon Logistik Winsen GmbH weiterhin ununterbrochen Beschäftigtendaten erheben und verwenden darf.[3]

Begründet wurde diese Entscheidung hauptsächlich damit, dass die erhobenen Daten in erster Linie der Steuerung logistischer Prozesse dienen würden. Weil es sich dabei „nur" um Leistungsdaten der Beschäftigten handele, sei das Vorgehen den betroffenen Beschäftigten zumutbar, so das Verwaltungsgericht Hannover.

1 Siehe Tätigkeitsbericht 2020, J.6.5.
2 Art. 58 Abs. 2 Buchst. f DSGVO.
3 Verwaltungsgericht Hannover, Urteil vom 9. Februar 2023, Aktenzeichen 10 A 6199/20.

Pflicht zur Datenminimierung

Diese Auffassung teilen wir nicht: Eine Steuerung der Logistikprozesse kann auch bei der Amazon Logistik Winsen GmbH mit weniger Beschäftigtendaten erfolgen.

Eine Verarbeitung von Daten[4], also zum Beispiel das Erheben und Verwenden von diesen, muss immer auf das notwendige Maß beschränkt sein. Dies folgt bereits aus dem Grundsatz der Datenminimierung.[5] Dieser ist bei der Verarbeitung von Daten als einzuhaltende Pflicht gesetzlich festgelegt.[6]

Eine ununterbrochene Erhebung und Nutzung von personenbezogenen Daten ist niemandem zumutbar.

Vor diesem Hintergrund rechtfertigen auch die weiteren für die ununterbrochene Datenverarbeitung vorgebrachten Gründe das Vorgehen nicht, auch wenn sie das Verwaltungsgericht Hannover anerkannt hat. Genannt hatte die Amazon Logistik Winsen GmbH unter anderem Entscheidungen über Qualifizierungsmaßnahmen, Personalentscheidungen und Feedbackerteilungen.

Recht auf informationelle Selbstbestimmung

Anders als es das Verwaltungsgericht Hannover vertritt, ist eine ununterbrochene Erhebung und Nutzung von personenbezogenen Daten niemandem – auch nicht im Beschäftigtenkontext – zumutbar.

Die Betroffenen sind nicht nur durch die Datenschutz-Grundverordnung, sondern auch durch ihr Grundrecht auf informationelle Selbstbestimmung[7] geschützt. Darunter ist die Befugnis des Einzelnen zu verstehen, grundsätzlich selbst über die Preisgabe und Verwendung seiner „persönlichen Daten“ zu bestimmen.[8] Vor dem Hintergrund der modernen Datenverarbeitungsmöglichkeiten schützt es den Menschen insbesondere ge-

4 Art. 4 Abs. 2 DSGVO.
5 Art. 5 Abs. 1 Buchst. c DSGVO.
6 Art. 5 Abs. 1 Buchst. c DSGVO.
7 Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.
8 Kühling/Buchner, DS-GVO BDSG, A. Einführung Rn. 122m, beck-online.

gen eine – wie hier erfolgende – nahezu unbegrenzte Verarbeitung seiner „persönlichen Daten".[9]

Berufungsverfahren vor dem Oberverwaltungsgericht Lüneburg

Weil wir die durch das Verwaltungsgericht Hannover vorgenommene rechtliche Einschätzung im vorliegenden Fall nicht teilen, haben wir gegen dieses Urteil vor dem Oberverwaltungsgericht Lüneburg Berufung eingelegt. Das Berufungsverfahren war bei Redaktionsschluss noch nicht abgeschlossen. Wir gehen davon aus, dass es in der zweiten Instanz zu einer Korrektur der erstinstanzlichen Entscheidung kommt.

Fazit

Die seitens Amazon Winsen betriebene extrem eingriffsintensive Datenverarbeitung ist aus datenschutzrechtlicher Sicht nicht zu rechtfertigen. Verantwortliche und Datenschutzbeauftragte[10] sollten sich im Klaren sein, dass wir bei einer ununterbrochenen Erhebung und Nutzung von personenbezogenen Daten – aus welchem Grund auch immer das erfolgen mag – stets die Möglichkeit aufsichtsrechtlicher Maßnahmen prüfen werden.

9 Vgl. Kühling/Buchner, DS-GVO BDSG, A. Einführung Rn. 122m, beck-online.

10 Datenschutzbeauftragte haben nach Art. 39 Abs. 1 Buchst. a DSGVO eine Beratungspflicht gegenüber den Verantwortlichen.

Kontrollen der Immobilienwirtschaft: Erhebliche datenschutzrechtliche Defizite G.3.2

Vermietende, Makler und Immobilienverwaltungen erheben regelmäßig eine Vielzahl personenbezogener Daten, um Vermietungs- und Verkaufsprozesse abzuwickeln. Bereits im Jahr 2022 haben wir anlasslose Prüfungen von Unternehmen aus der Immobilienwirtschaft durchgeführt und 2023 fortgesetzt. Dabei stellten wir zahlreiche Verstöße beim Umgang mit personenbezogenen Daten fest.

Siebzehn Immobilienmakler und Wohnungsunternehmen haben wir im Rahmen einer angekündigten Vor-Ort-Kontrolle aufgesucht. Ziel der Kontrolle: Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) in Bezug auf Kundendaten der Immobilienbetriebe.

Die Kontrollen haben wir stichprobenhaft durchgeführt und dabei speziell datenschutzrechtliche Belange geprüft, in denen erfahrungsgemäß Versäumnisse oder Nachlässigkeiten von Unternehmen der Immobilienbranche zu erwarten waren.

Im Schwerpunkt konzentrierten wir uns bei den Kontrollen auf die Verarbeitung personenbezogener Daten von Kauf- und Mietinteressenten. Dabei haben wir gezielt die verschiedenen Phasen des Vermittlungs-, Vermietungs- und Verkaufsprozesses in den Blick genommen. Von der ersten Kontaktaufnahme für einen Besichtigungstermin über den Vertragsabschluss beziehungsweise die Absage an nicht berücksichtigte Interessentinnen und Interessenten bis hin zur fortlaufenden Mietverwaltung haben wir den gesamten Prozess geprüft.

Verstöße bei Nachweisen und Aufbewahrungsfristen

Bei den Vor-Ort-Kontrollen haben wir eine Reihe von datenschutzrechtlichen Verstößen festgestellt. Neun der geprüften Unternehmen verarbeiteten personenbezogene Daten der Mietinteressentinnen und Mietinteressenten rechtswidrig, indem sie Kopien von Ausweisdokumenten, Gehaltsabrechnungen oder Bonitätsnachweisen erhoben und archivierten,

ohne dass dies zum jeweiligen Stand des Verfahrens erforderlich gewesen wäre.

So dienen Ausweisdokumente beispielsweise lediglich dazu, die Identität festzustellen. Dies kann bereits durch Inaugenscheinnahme des Dokuments erfolgen, ohne dass es dazu einer Kopie oder Speicherung bedarf. Diese Daten zu archivieren ist daher nach der DSGVO weder für die Vertragsanbahnung[1] noch als Ergebnis einer Interessenabwägung[2] erforderlich. Eine rechtliche Verpflichtung personenbezogene Daten zu verarbeiten[3] besteht bei Vermietungen im Regelfall ebenfalls nicht. Ausweisdokumente sind daher weder vollständig noch mit Schwärzungen durch Makler, Hausverwaltungen oder Vermietende zu kopieren und zu archivieren.

Neun der geprüften Unternehmen verarbeiteten personenbezogene Daten der Mietinteressenten rechtswidrig.

Das Gleiche gilt für Gehaltsnachweise und Bonitätsauskünfte: Um das Nettoeinkommen zur Bestreitung der Wohnkosten zu überprüfen, reicht es aus, sich einen Nachweis vorlegen zu lassen und die Angaben der Mieterselbstauskunft zu prüfen. Kopien anzufordern oder anzufertigen beziehungsweise derlei Nachweise zu archivieren, ist für die Durchführung des Mietverhältnisses nicht erforderlich.

Speichern der Kontaktdaten nach Vergabe des Mietobjekts

Sieben Unternehmen speicherten regelmäßig die Namen und E-Mailadressen von Mietinteressentinnen und Mietinteressenten noch mehrere Jahre nach Vergabe einer Wohnung und damit deutlich länger als erforderlich.

Nach der DSGVO sind personenbezogene Daten zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind.[4] Dies greift bei Daten der Interessentinnen und Interessenten grundsätzlich dann, wenn ein Objekt vermittelt wurde. Unabhängig vom jeweiligen Vermittlungsobjekt ist ein Speichern für weitere sechs Monate unter Berücksichtigung des Allgemeinen Gleichbehandlungsgesetzes zulässig. Bei

1 Nach Art. 6 Abs. 1 Buchstabe b DSGVO.
2 Nach Art. 6 Abs. 1 Buchstabe f DSGVO.
3 Nach Art. 6 Abs. 1 Buchstabe c DSGVO.
4 Nach Art. 17 Abs. 1 Buchstabe a DSGVO.

Kaufobjekten ist eine Speicherdauer von 15 Monaten erlaubt, wenn der Maklervertrag ohne Verkauf beendet wurde, um gegebenenfalls Provisionsansprüche geltend machen zu können.

Umfangreiche Datenerhebung zur Anbahnung eines Besichtigungstermins

Sechs Unternehmen erhoben im Vorfeld von Besichtigungsterminen umfangreiche Daten mittels einer sogenannten Mieterselbstauskunft. Abgefragt wurden etwa Einkommen, Beruf und Bonität.

Zur Organisation von Besichtigungsterminen ist dies nicht erforderlich und deshalb nicht datenschutzkonform. Vielmehr reicht es aus, Angaben zur Identifikation, also Name, Vorname und Anschrift und gegebenenfalls Informationen zu einem Wohnberechtigungsschein zu erfragen.[5] Generell darf eine Mieterselbstauskunft nur von Interessentinnen und Interessenten angefordert werden, die bereits erklärt haben, die angebotene Immobilie anmieten zu wollen.

Unzulässige Fragen und unzureichende Information

Vier Unternehmen verwendeten Fragebögen zur Mieterselbstauskunft, die nicht den datenschutzrechtlichen Anforderungen entsprechen. Diese fragten etwa Kontaktinformationen aktueller oder früherer Vermieter sowie die Angabe des Familienstands ab, obwohl diese Angaben für die Entscheidung über ein Mietverhältnis nicht erforderlich sind. Zudem stellten wir fest, dass sechs der geprüften Unternehmen ihren Informationspflichten[6] hinsichtlich der Erhebung und Verarbeitung von Daten nur unzureichend nachkamen.

Abschluss der Kontrollverfahren

Mit den durchgeführten Prüfungen wollten wir die betroffenen Unternehmen einerseits beraten und ihnen Hinweise geben, andererseits erteilten wir auch Sanktionen im Fall von festgestellten Verstößen.

5 Weiterführende Informationen in der Orientierungshilfe der Datenschutzkonferenz zur Einholung von Selbstauskünften bei Mietinteressenten, einzusehen unter https://t1p.de/mietinteresse (Kurzlink).

6 Nach Art. 12 Abs. 1 i.V.m. Art. 13 DSGVO.

Infolge der Verstöße haben wir gegenüber fünf Unternehmen ein Bußgeld festgesetzt. Vier Unternehmen haben wir aufgrund der datenschutzrechtlichen Verstöße verwarnt.[7] Zudem ist gegenüber weiteren sechs Unternehmen anlässlich der im Rahmen der Kontrollen zutage getretenen datenschutzrechtlichen Versäumnissen ein feststellender Bescheid ergangen. Lediglich bei zwei Unternehmen hatten wir keine Datenverarbeitungen zu beanstanden.

Fazit

Die stichprobenartigen Kontrollen der Immobilienwirtschaft haben gezeigt, dass in Teilen erhebliche datenschutzrechtliche Defizite im Umgang mit den Daten der Kundinnen und Kunden bestehen.

Insbesondere die verschiedenen Phasen der Datenverarbeitung, die im Rahmen eines Vermittlungs- oder Vermietungsprozesses auftreten, erfordern eine stetige Prüfung des Verantwortlichen, ob es zum jeweiligen Zeitpunkt und für den jeweiligen Zweck wirklich erforderlich ist, Daten zu erheben. Zudem haben die Verantwortlichen sicherzustellen, dass sie personenbezogene Daten ihrer Kundschaft löschen, wenn diese nicht mehr notwendig sind.

Aufgrund der gewonnenen Erkenntnisse behalten wir uns vor, auch künftig anlasslose Prüfungen im Bereich der Immobilienwirtschaft durchzuführen.

7 Gemäß Art. 58 Abs. 2 Buchst. b DSGVO.

Smart-Data-Verfahren bei Genossenschaftsbanken weiterhin problematisch G.3.3

Kreditinstitute verarbeiten sensible Daten ihrer Kunden. Wollen sie diese Daten für Werbezwecke nutzen, müssen alle Anforderungen des Datenschutzrechts eingehalten werden. In 2023 haben wir daher in diesem Bereich weitere Prüfungen durchgeführt. Bei der Kooperationsbereitschaft der Kreditinstitute gab es Licht und Schatten.

Im Tätigkeitsbericht 2022 haben wir bereits umfassend über Smart-Data-Verfahren bei Genossenschaftsbanken berichtet.[1] Es handelt sich um Verfahren, bei denen die Banken aus den Daten ihrer Kundinnen und Kunden Scorewerte bilden, um diese anschließend passgenau werblich anzusprechen. Im Jahr 2022 hatten wir die Genossenschaftsbanken in Niedersachsen vor der Durchführung dieser Verfahren gewarnt und weitere Überprüfungsverfahren eingeleitet. Grund hierfür war, dass die Verarbeitung weder auf eine Interessenabwägung[2] noch auf die verwendete Einwilligungserklärung[3] gestützt werden konnte und dementsprechend ohne Rechtsgrundlage erfolgte. Im Nachgang zu der Warnung wurde uns mitgeteilt, die Smart-Data-Verfahren seien bundesweit zunächst nicht mehr im Einsatz und würden überarbeitet werden.

Neue Einwilligungen

Im Berichtszeitraum sollten die Smart-Data-Verfahren nun auf eine tragfähige Rechtsgrundlage gestellt werden. Dafür entwarfen die Banken neue Einwilligungserklärungen und rollten sie aus. Insbesondere im Online-Banking fragten die Anbieter nun Kundinnen und Kunden nach ihrem Einverständnis zur Berechnung von Scorewerten für Werbezwecke.

Was bereits Kundinnen und Kunden verärgert und zu Beschwerden geführt hat, ist die fehlende Möglichkeit, die Einwilligung endgültig und vor

1 Siehe Tätigkeitsbericht 2022, J.5.1.
2 Art. 6 Abs. 1 Buchst. f DSGVO.
3 Art. 6 Abs. 1 Buchst. a DSGVO.

allem dauerhaft abzulehnen. Es gibt lediglich die Möglichkeit, die Einwilligung durch einen Klick auf den Button „Jetzt nicht zustimmen“ nicht abzugeben. Dies führt dazu, dass die Kundinnen und Kunden in regelmäßigen Abständen erneut nach dem Einloggen in das Online-Banking dazu aufgefordert werden, die Einwilligung abzugeben.

Eine Bedingung für die Wirksamkeit einer Einwilligung ist die Freiwilligkeit. Diese ist jedoch nicht gegeben, wenn die betroffene Person sich zur Einwilligung gedrängt fühlt oder unangemessener Druck auf die betroffene Person ausgeübt wird.[4] Wird betroffenen Personen ein künstlich erzeugter, sachlich nicht zu begründender, Mehraufwand auferlegt um die Einwilligung nicht zu erteilen, können sie sich zur Vermeidung dieses Mehraufwandes gedrängt fühlen, in eine Verarbeitung einzuwilligen.[5]

Freiwilligkeit ist nicht gegeben, wenn die betroffene Person sich zur Einwilligung gedrängt fühlt.

Auf die Beschwerden hin haben wir Verfahren gegen die betroffenen Kreditinstitute eingeleitet um die Wirksamkeit der neuen Einwilligungen zu beurteilen und detailliert zu ermitteln, welche Verarbeitungsprozesse nunmehr auf Grundlage dieser Einwilligungen durchgeführt werden.

Weitere Überprüfungsverfahren

Wie im Tätigkeitsbericht 2022 angekündigt, haben wir weitere Untersuchungen zu den Smart-Data-Verfahren, die bereits vor unserer Warnung genutzt wurden, durchgeführt. Wir haben dabei insbesondere Informationen zur Anzahl der betroffenen Personen und zur Anzahl der genutzten Verfahren angefordert, um den Umfang der Verarbeitung durch die jeweiligen Banken zu ermitteln und Vor-Ort-Kontrollen durchgeführt. In einem Fall wurde das Verfahren mit der Verhängung eines Bußgeldes abgeschlossen.[6] Weitere Verfahren sind noch offen.

4 EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 55.
5 Vgl. DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien, Dezember 2021, S. 17, Kurzlink: https://t1p.de/telemedien (PDF).
6 Siehe Kapitel H zu Bußgeldverfahren.

Kooperationspflichten

Banken sind nach der Datenschutz-Grundverordnung dazu verpflichtet, mit uns zu kooperieren.[7] Verantwortliche müssen auf Anforderung der Aufsichtsbehörde wahrheitsgemäße und vollständige Angaben zu ihren Verarbeitungstätigkeiten machen. Verstößt ein Verantwortlicher gegen die Kooperationspflicht, kann auch allein dies mit einer Geldbuße geahndet werden.[8]

Verstößt ein Verantwortlicher gegen die Kooperationspflicht, kann dies mit einer Geldbuße geahndet werden.

Während einige Banken umfassend kooperieren, sind andere dieser Pflicht nicht ausreichend nachgekommen. Daher ergingen gegen vier Banken Auskunftsheranziehungsbescheide, mit denen die Kreditinstitute zur Auskunft uns gegenüber verpflichtet und Zwangsgelder angedroht wurden. Die vier Kreditinstitute haben Unterlagen vorgelegt und trotzdem gegen diese Bescheide Klage vor dem Verwaltungsgericht erhoben. Die Klagebegründungen lagen zum Zeitpunkt dieses Berichts noch nicht vor.

Zwischenfazit und Ausblick

Smart-Data-Verfahren bei genossenschaftlichen Kreditinstituten haben sich zu einem Dauerbrenner in unserer aufsichtsbehördlichen Tätigkeit entwickelt. Kreditinstitute verfügen insbesondere in den Zahlungsverkehrsdaten über tiefe Einblicke in die Lebensführung ihrer Kundinnen und Kunden. Um den Schutz der betroffenen Kundinnen und Kunden sicherzustellen, schauen wir als Aufsichtsbehörden in diesem sensiblen Bereich sehr genau hin und werden das auch weiterhin tun.

7 Art. 31 DSGVO.
8 Art. 81 Abs. 4 Buchst. a DSGVO.

G.3.4 Prüfung der Auftragsverarbeitungsverträge von niedersächsischen Lohnbüros

Die niedersächsische Datenschutzaufsicht führte im Jahr 2023 eine Kontrolle der Musterverträge zur Auftragsverarbeitung von Lohnbüros durch. Ziel war es, Lohnbüros und Verantwortliche beim Abschluss rechtskonformer Auftragsverarbeitungsverträge zu unterstützen und Rechtskonformität zu erreichen.

Viele Unternehmen und Organisationen lassen ihre Lohnbuchhaltung durch einen externen Dienstleister, sogenannte Lohnbüros, durchführen. Dabei werden personenbezogene Daten von Beschäftigten verarbeitet. Diese Datenverarbeitung findet im Auftrag des Verantwortlichen, also des Unternehmens, statt. Daher handelt es sich bei dem jeweiligen in Anspruch genommenen Lohnbüro um einen Auftragsverarbeiter.[1] Um einen konkreten Rahmen für diese weisungsgebundene Tätigkeit festzulegen, müssen der Verantwortliche und der Auftragsverarbeiter einen Auftragsverarbeitungsvertrag (AVV) schließen. Die Datenschutz-Grundverordnung (DSGVO) beschreibt dafür im Detail, welche Rechte, Pflichten und Maßnahmen im AVV geregelt werden müssen.[2]

Die niedersächsische Datenschutzaufsicht kontrollierte 2023 die datenschutzrechtlichen Musterverträge zur Auftragsverarbeitung zwischen Anbietern für die Lohn- und Gehaltsabrechnung aus Niedersachsen und deren Kundinnen und Kunden. Auf der Grundlage einer Checkliste schrieb die Aufsichtsbehörde zehn niedersächsische Lohnbüros an und bat um Auskunft zur Ausgestaltung ihrer AVV. Die Checkliste wurde den Lohnbüros zur Verfügung gestellt.

Die Auswertung der Rückmeldungen der Unternehmen ergab erfreulicherweise, dass den Unternehmen grundsätzlich bekannt war, welche Anforderungen die DSGVO an die Ausgestaltung eines AVV stellt. Außerdem zeigte die Prüfung, dass nur noch geringer Verbesserungsbedarf bestand,

1 Bei der Prüfung ging es um die Lohn- und Gehaltsabrechnung durch Personen und Gesellschaften, die nicht gemäß § 11 Abs. 2 i.V.m. § 3 StBerG weisungsfrei sind.

2 Art. 28 Abs. 3 DSGVO.

um die Verträge in Einklang mit den Anforderungen der DSGVO zu bringen und die Rechte und Freiheiten der Betroffenen zu schützen. Die meisten Defizite lagen im Bereich der Unterstützung der Verantwortlichen bei der Erfüllung ihrer Pflichten aus Betroffenenrechten.[3]

Die identifizierten Defizite konnten im kooperativen Dialog beseitigt werden.

Die identifizierten Defizite konnten sämtlich im kooperativen Dialog mit den Unternehmen beseitigt und somit die Rechtmäßigkeit der AVV-Muster hergestellt werden. Die Prüfung wurde im August 2023 abgeschlossen.

3 Gemäß Art. 28 Abs. 3 UAbs. 1 Satz 2 Buchst. e DSGVO.

G.3.5 LfD kontrolliert Datenoffenlegung an externe Auditoren

Bei einer Prüfung durch externe Auditoren müssen Unternehmen in der Regel große Mengen an internen Daten übergeben, darunter häufig personenbezogene Daten von Beschäftigten oder Kunden. In einem Fall in Niedersachsen hatte ein Unternehmen zwar datenschutzrechtliche Aspekte von vornherein umgesetzt, dennoch stellte die niedersächsische Datenschutzaufsicht einige Punkte fest, die sie als datenschutzrechtliche Mängel bewertete. Deshalb verhängte sie ein Bußgeld und sprach Verwarnungen aus.

Hintergrund des Falles war, dass ein Unternehmen gegen bestimmte rechtliche Bestimmungen eines Landes verstoßen hatte. Infolgedessen hatte das Unternehmen im Rahmen von gerichtlichen Verfahren zugestimmt, seine Compliance-Strukturen durch unabhängige externe Stellen überprüfen zu lassen. Für diese „Compliance-Audits" (Konformitätsprüfungen) musste das Unternehmen große Mengen an Unternehmensinformationen gegenüber den externen Auditoren offenlegen, die potenziell auch personenbezogene Daten enthielten. Das Unternehmen implementierte vor der Offenlegung deshalb einen Prozess zur datenschutzrechtlichen Prüfung, Freigabe und zur Schwärzung nicht erforderlicher personenbezogener Daten. Die Offenlegung personenbezogener Daten an die Auditoren wurde unter anderem auf berechtigte Interessen des Unternehmens[1], Rechtsverteidigung[2] sowie auf Zwecke des Beschäftigungsverhältnisses gestützt.

Unzureichende Informationserteilung an Beschäftigte

Die Offenlegung personenbezogener Beschäftigtendaten an die Auditoren war aus Sicht des Landesbeauftragten für den Datenschutz (LfD) als Zweckänderung im Sinne der Datenschutz-Grundverordnung (DSGVO)[3]

1 Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO.
2 Art. 49 Abs. 1 UAbs. 1 Satz 1 Buchst. e DSGVO.
3 Art. 13 Abs. 3 DSGVO.

anzusehen, über welche das Unternehmen seine Mitarbeitenden gesondert und detailliert hätte informieren müssen.

Zwar hatte das Unternehmen die Audits in Datenschutzerklärungen etwa im Intranet erwähnt, allerdings handelte es sich nach der Rechtsansicht des LfD dabei um allgemeine generische Informationen zur Offenlegung bestimmter Datenkategorien ohne Bezug zu konkreten Daten oder Betroffenen. Eine weitergehende, individualisierte Mitteilung an die einzelnen Beschäftigten über die zweckändernde Weiterverarbeitung erfolgte nicht. Die Beschäftigten hätten mithin anhand dieser Information aus Sicht der Aufsichtsbehörde nicht erkennen können, ob sie überhaupt zum Kreis der Betroffenen gehörten, um sodann gegebenenfalls ihr Handeln danach ausrichten zu können. Überdies ist der LfD bei der Prüfung zu der Überzeugung gelangt, dass das Unternehmen zum Teil weitergehende personenbezogene Daten offenlegte als dies zuvor in den zuvor kommunizierten Datenschutzerklärungen mitgeteilt war.

Zwar geht das Unternehmen davon aus, hinreichende Informationen erteilt zu haben, jedoch wird diese Auffassung vom LfD nicht geteilt. Daher wurde unter Berücksichtigung der Zahl der betroffenen Personen und des Umsatzes des Unternehmens wegen unzureichender Informationserteilung gegenüber den Beschäftigten eine Geldbuße in Höhe von 4,3 Millionen Euro festgesetzt. Das Unternehmen hat Einspruch gegen den Bußgeldbescheid eingelegt; dieser ist nicht rechtskräftig. Einzelne dem Bescheid zugrunde gelegte Rechtspositionen sind höchstrichterlich noch nicht entschieden. Bis zu einer rechtskräftigen Entscheidung gilt die Unschuldsvermutung.

Verwaltungsrechtliche Verwarnungen bezüglich weiterer Verstöße

Im Rahmen der Überprüfung des bereits genannten und eines weiteren Compliance-Audits sprach unsere Behörde wegen der nicht ordnungsgemäßen Unterrichtung der Beschäftigten über die zweckändernde Datenverarbeitung[4] eine Verwarnung im Verwaltungsverfahren aus.

4 Art. 13 Abs. 3 DSGVO.

Weiter sprach der LfD in einem konkreten Einzelfall eine Verwarnung wegen der Offenlegung bestimmter personenbezogener Beschäftigtendaten an einen der Auditoren aus, bei denen das Unternehmen aus Sicht der Behörde keine überwiegenden berechtigten Interessen des Unternehmens als Rechtsgrundlage nach DSGVO[5] nachweisen konnte. Die Datenschutzaufsichtsbehörde konnte in diesen Fällen die vorgenommene Interessenabwägung nicht nachvollziehen, weil aus ihrer Sicht wesentliche Gesichtspunkte nicht in die Abwägung einbezogen oder nicht nachvollziehbar gewichtet wurden.

Außerdem wurde eine Verwarnung wegen eines Verstoßes gegen Artikel 32 DSGVO ausgesprochen, weil in einem separaten Teilprozess personenbezogene Beschäftigtendaten ab Schutzstufe D im Sinne des LfD-Schutzstufenkonzepts[6] per E-Mail ohne eine aus Sicht des LfD erforderliche hinreichende Ende-zu-Ende-Verschlüsselung an den außerhalb des Europäischen Wirtschaftsraums befindlichen Auditor übermittelt wurden. Die vom Unternehmen eingesetzte Pseudonymisierung und Transportverschlüsselung erachtete der LfD insoweit nicht als ausreichenden Schutz der personenbezogenen Daten.

Ferner sprach der LfD eine Verwarnung aus, weil das Unternehmen bezüglich eines der Audits zunächst kein gesondertes Verarbeitungsverzeichnis[7] errichtet hatte.

Das Unternehmen hat gegen die Abhilfemaßnahmen des LfD Klage beim Verwaltungsgericht erhoben, über die noch nicht entschieden ist. Die Abhilfemaßnahmen sind daher noch nicht bestandskräftig.

5 Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO.
6 Kurzlink: https://t1p.de/schutzstufen
7 Art. 30 DSGVO.

Dauerbrenner Auskunftsrecht – Unklarheiten und Fehler auf beiden Seiten G.3.6

Viele Beschwerden an unsere Behörde richten sich gegen Unternehmen, die auf ein Auskunftsersuchen nach der Datenschutz-Grundverordnung nicht oder nur ungenügend reagieren. Zudem streiten sich Betroffene mit Unternehmen über die Versandart und Verschlüsselung der Auskunftsdaten.

Insbesondere Klein- und Kleinstunternehmen oder Einzelunternehmer reagieren auch fünf Jahre nach Einführung der Datenschutz-Grundverordnung (DSGVO) noch häufig falsch, wenn ein Betroffener bei ihnen Auskunft bezüglich seiner Daten verlangt. Vielfach ignorieren die Unternehmen dieses Auskunftsersuchen oder beantworten sie nur widerwillig und unzureichend mit dem Verweis auf die Datenschutzhinweise: Dort stünde alles Notwendige drin.

In solchen Fällen sensibilisieren wir die Verantwortlichen mittels eines Hinweisschreibens, das auf das Auskunftsrecht sowie die Form- und Inhaltserfordernisse einer Auskunft aufmerksam macht. Rückblickend hat sich diese Praxis überaus bewährt. In der überwiegenden Zahl der Fälle antwortet die verantwortliche Stelle anschließend zeitnah und umfassend auf das Auskunftsersuchen.

Bei ausbleibender Antwort auf ein Auskunftsersuchen schalten wir regelmäßig, soweit vorhanden, die Datenschutzbeauftragten der Unternehmen ein. Mit dieser Vorgehensweise haben wir gute Erfahrungen gemacht, die Auskunft wird in aller Regel erteilt und es macht bei den betroffenen Personen einen besseren Eindruck, wenn das Unternehmen schlussendlich selbst antwortet.

Häufig gehen bei einem Auskunftsersuchen mit anschließender Beschwerde Konflikte voraus.

Häufig gehen bei einem Auskunftsersuchen mit anschließender Beschwerde Konflikte oder Unstimmigkeiten zwischen den Beteiligten voraus, zum Beispiel ein Streit über die Rückgabe der Mietkaution bei Auszug oder eine abgelehnte Kreditanfrage. Dann fordern die Betroffenen gelegentlich, dass unsere Behörde

unbedingt ein Bußgeld gegen das Unternehmen verhängen müsse. Unterschwellig schwingt mit, dass sich der Betroffene auf diese Weise eine Genugtuung bezüglich der vorausgegangenen Auseinandersetzung verspricht, wenn die Aufsichtsbehörde sein Gegenüber wegen einer nicht oder nur unzureichend erteilten Auskunft bestraft.

In einem Fall verwendete ein Betroffener eine Mustervorlage für Auskunftsersuchen und ergänzte sie mit dem Hinweis, dass bei nicht fristgerechtem Erhalt einer Auskunft „automatisiert eine Beschwerde an den (Landes-) Datenschutzbeauftragten ergeht und anschließend wegen Persönlichkeitsverletzung Klage erhoben […] wird".

Große Unternehmen gut aufgestellt

Wir beobachten, dass größere Unternehmen in der Regel die Auskunft zügig und fristgerecht erteilen. Schwierig wird es meist, wenn das Unternehmen eine allumfassende Auskunft erstellen soll (Recht auf Kopie).[1] In solchen Fällen gehen bei uns vermehrt Beschwerden ein, dass die erhaltene Auskunft nicht vollständig erteilt ist.

Zumeist enthalten solche Beschwerden keine weiteren Erläuterungen. Als Datenschutzaufsicht können wir allerdings nicht beurteilen, ob eine Auskunft alle personenbezogenen Daten einer Beschwerdeführerin oder eines Beschwerdeführers enthält. Insofern verweisen wir die Person dann an das Unternehmen mit dem Hinweis, die fehlenden Dokumente oder Daten konkret zu benennen, damit das Unternehmen die Auskunft vervollständigen kann.

Dokumente bei Auskunft korrekt übermitteln

Viele Unternehmen stehen an diesem Punkt vor der Frage, wie sie eine Auskunft gemäß der DSGVO[2] mit zahlreichen Dokumenten, die ja schließlich eine Vielzahl personenbezogener Daten enthalten, datenschutzkonform an die Beschwerdeführer übermitteln.

In der Regel melden sich die Betroffenen gegenüber der verantwortlichen Stelle auf elektronischem Weg, also als transportverschlüsselte E-Mail-

1 Art. 15 Abs. 3 DSGVO.
2 Art. 15 Abs. 3 DSGVO.

Anfrage zum Beispiel an ein Funktionspostfach (betroffenenrechte@xyz-gmbh.de). Unternehmen kommen an dieser Stelle regelmäßig in Schwierigkeiten, denn die DSGVO verpflichtet die verantwortliche Stelle, die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern die oder der Betroffene nichts anderes angibt.[3]

Einige Unternehmen übersenden die Auskunft dann als PDF-Anhang über eine transportverschlüsselte E-Mail an die Absenderadresse des Betroffenen. Dieses Vorgehen führte im Jahre 2023 wiederum zu einigen Beschwerden. Die Beschwerdeführer beklagen in diesem Fall, dass die Auskunft unverschlüsselt und für jedermann lesbar übermittelt wurde. Dass zumindest eine Transportverschlüsselung im Einsatz ist, ist den meisten für gewöhnlich nicht bewusst oder wird als nicht ausreichend erachtet.

In diesem Zusammenhang ist eine Beschwerde aus dem zurückliegenden Berichtsjahr erwähnenswert, bei der ein Großunternehmen eine Auskunft in einem mehr als 100 Seiten umfassenden PDF an einen Kunden als E-Mail-Anhang übermittelt hat. Das PDF war weder passwortgeschützt noch war die E-Mail Ende-zu-Ende verschlüsselt. Unmittelbar nach Erhalt beschwerte sich die fachkundige betroffene Person bei uns, unter anderem weil die PDF-Datei eine Personalausweiskopie, diverse Gehaltsabrechnungen, eine Selbstauskunft und Vertragsunterlagen enthielt und in diesem Fall die Transportverschlüsselung nicht für ausreichend erachtet wurde.

Das eingeleitete aufsichtsbehördliche Prüfverfahren hierzu ist noch nicht abgeschlossen. Das Unternehmen hat zwischenzeitlich allerdings sein Verfahren zur erweiterten Auskunftserteilung umgestellt: Auskünfte sendet es zwar weiterhin per E-Mail und PDF-Anhang an die vorher verifizierte E-Mail-Adresse des Betroffenen, dieses PDF ist allerdings nun mit einem (sicheren) Passwort geschützt. Das Passwort schickt das Unternehmen anschließend auf einem anderen Weg, in diesem Fall postalisch, an die betroffene Person. Dies ist eine zweckdienliche Lösung, um dem Recht auf Auskunft nachzukommen.

3 Art. 15 Abs. 3 Satz 3 DSGVO.

Varianten der Übermittlung beim Recht auf Kopie

Darüber hinaus begegnen uns in der Praxis weitere Varianten, wie Unternehmen Auskünfte verschicken. In einigen Fällen missachtete die verantwortliche Stelle die DSGVO und sendete trotz eines elektronischen Antrags die Auskunft postalisch an die Adresse der betroffenen Person im Papierformat zu.[4] In der Regel stand der verantwortlichen Stelle in diesen Fällen kein (sicheres) elektronisches Verfahren zur Verfügung, um die Auskunft zu übermitteln. Oder sie war sich unsicher, ob ihre elektronischen Übermittlungsmöglichkeiten ausreichend datenschutzkonform sind.

In der Praxis wird dieses Verfahren bisher auch bei einem elektronischen Antrag nicht als schwerwiegender Verstoß gegen die DSGVO gewertet, da aus unserer Sicht die sichere Übermittlung der Auskunft im Vordergrund steht, für die der Absender verantwortlich zeichnet.

In anderen Fällen stellen verantwortliche Stellen die Daten auf einem sogenannten Portal zur Verfügung. Nach Eingang des elektronischen Antrags erstellt das Unternehmen für die Auskunft dabei ein Datenpaket und legt es temporär in einer abgesicherten und passwortgeschützten Cloud zum Download ab. Die betroffene Person erhält anschließend per Mail einen Benutzernamen für den Login an ihre verifizierte Absenderemailadresse. Das erforderliche Passwort bekommt sie auf einem zweiten Wege (postalisch).

Insbesondere bei besonders sensiblen personenbezogenen Daten wie Finanzdaten, Steuerbescheiden oder Gehaltsabrechnungen halten wir das – gemeinsam mit der Ende-zu-Ende verschlüsselten E-Mail – derzeit für die beste Methode für den Versand einer Auskunft.

4 Art. 15 Abs. 2 Satz 3 DSGVO.

Gesundheit und Soziales

Apotheken zu Corona-Daten und Kundenkarten geprüft G.4.1

Im Rahmen einer Serie von anlasslosen Prüfungen im Gesundheitswesen haben wir in einer Stichprobe fünf Apotheken hinsichtlich des datenschutzkonformen Umgangs mit personenbezogenen Daten untersucht. Eher zufällig haben wir dabei eine für alle Verantwortlichen wichtige Erkenntnis bezüglich von Daten-Backups gewonnen.

Prüfgegenstand bei den fünf Apotheken waren die Einwilligungserklärungen von Kundinnen und Kunden in Bezug auf die Kundenkarte, die Löschkonzepte für personenbezogene Daten und die Aufbewahrung von Berechtigungsscheinen für die Ausgabe von Corona-Schutzmasken.

Mit solchen Berechtigungsscheinen konnten Personen aus Risikogruppen Corona-Masken in Ihrer Apotheke beziehen. Die Scheine verblieben in den Apotheken, müssen dort bis zum 31. Dezember 2024 verwahrt und danach vernichtet werden.

In allen überprüften Apotheken wurden die Berechtigungsscheine den Vorgaben entsprechend getrennt von anderen personenbezogenen Daten aufbewahrt und mit Vernichtungsdatum für Anfang 2025 versehen.

Alle geprüften Apotheken haben zudem sogenannte Kundenkarten im Einsatz. Diese werden vorrangig dazu genutzt, den Betroffenen eine Übersicht über die innerhalb eines Jahres gezahlten Kosten für Medikamente zu erstellen. Diese Übersicht können die Betroffenen für die Befreiung von der Zuzahlung gegenüber der Krankenkasse oder als Nachweis der krankheitsbedingten Mehraufwendungen bei der Steuererklärung nutzen. Gleichzei-

tig können die auf der Kundenkarte gespeicherten Daten den Apotheken dazu dienen, die Beratung zu verbessern.

Die Einwilligungserklärungen für diese Kundenkarten waren rechtlich akzeptabel, aber noch verbesserungsfähig. So wiesen einige Einwilligungstexte Ungenauigkeiten auf. Zudem waren die eingesetzten Softwaresysteme teils so rudimentär, dass manche Vorgänge unnötigerweise händisch nachgetragen werden mussten – eine potenzielle Fehlerquelle. Das jeweils vorhandene Löschkonzept war hingegen nicht zu beanstanden.

Jede geprüfte Apotheke hat einen detaillierten Abschlussbericht erhalten mit Hinweisen auf Stärken und Schwächen ihres Datenschutzkonzepts nebst Optimierungsmöglichkeiten.

Unkenntnis über eigenes Backup-Konzept

Am Rande der Prüfung haben wir uns die Art und Weise der elektronischen Datenverarbeitung näher angeschaut. Alle Apotheken verarbeiten die Kundenkartei und die Warenwirtschaft elektronisch.

In diesem Zusammenhang ist aufgefallen, dass die Verantwortlichen und zum Teil leider auch die jeweiligen Datenschutzbeauftragten nicht in der Lage waren, die elektronische Datenverarbeitung und das Backup-Konzept umfänglich zu beschreiben. Insbesondere hatte uns interessiert, welche Daten bei der täglichen Dateisicherung gespeichert werden und ob eine vollständige Systemwiederherstellung mit diesen Daten möglich ist. Hier haben wir die Verantwortlichen entsprechend sensibilisiert und empfohlen, auf einem getrennten System einen entsprechenden Backup-Wiederherstellungstest durchzuführen. Dabei sollte sie das beauftragte IT-Unternehmen und die oder der Datenschutzbeauftragte unterstützen.

In den geprüften Apotheken werden allerdings alle relevanten personenbezogenen Daten, insbesondere die Daten, welche einer gesetzlichen Aufbewahrungspflicht unterliegen (beispielsweise nach dem Transfusions- oder dem Apothekengesetz), in Papierform gespeichert. Ein potenzieller Systemausfall hätte daher selbst mit unzureichendem Backup keine schwerwiegenden Folgen für die Kundinnen und Kunden.

Sofern zukünftig die Apotheken auch Daten, die einer gesetzlichen Aufbewahrungspflicht unterliegen, elektronisch verarbeiten, muss das gesamte

EDV-System datenschutzkonform und nach den Vorgaben der Informationssicherheit aufgestellt sein. Hierzu sollten die Verantwortlichen die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik zum IT-Grundschutz[1] beachten.

Im Nachgang zur Prüfung haben wir der Apothekerkammer unseren Prüfbericht zukommen lassen und diese gebeten, die Mitgliedsapotheken über die Erkenntnisse aus der Prüfung zu unterrichten sowie insbesondere hinsichtlich der elektronischen Datenverarbeitung zu sensibilisieren.

Fazit

Die Apotheken gehen verantwortungsvoll mit sensiblen Daten um – an einigen Stellen gibt es aber Verbesserungspotenzial.

1 Kurzlink: https://t1p.de/bsi-grundschutz

G.4.2 Massenhafter Fehlversand von elektronischen Arbeitsunfähigkeitsmeldungen

Mitte des Jahres erreichte uns die Information, dass sich in dem elektronischen Postfach einer Arztpraxis insgesamt 116.466 elektronische Arbeitsunfähigkeitsmeldungen befanden, welche für die AOK Niedersachsen bestimmt waren.

Wie konnte es überhaupt zu einem Fehlversand kommen? Ärztinnen und Ärzte wurden gesetzlich[1] verpflichtet, sich bis zum 30. Juni 2020 an die Telematikinfrastruktur (TI)[2] zur digitalen Vernetzung im Gesundheitswesen anzuschließen. Spätestens seit dem 1. Januar 2023 besteht die Verpflichtung[3], mittels elektronischem KIM-Postfach[4] Arbeitsunfähigkeitsbescheinigungen elektronisch an die Krankenkassen zu übermitteln. Die Nutzung von KIM war für diese Zwecke seit dem 1. Juli 2022 möglich.

KIM ist der einheitliche und datenschutzrechtlich sichere Standard für die elektronische Übermittlung medizinischer Dokumente. Diesen E-Mail-Dienst dürfen ausschließlich mittels des elektronischen Heilberufeausweises registrierte und authentifizierte TI-Teilnehmende nutzen.

Einträge in den KIM-TI-Verzeichnisdienst, das E-Mail-Adressbuch aller an der TI teilnehmenden Verantwortlichen, dürfen nur qualitätsgesichert vorgenommen werden. Die einzelnen Verantwortlichen werden im KIM-TI-Verzeichnisdienst mit einer mehrteiligen Identifizierungsnummer gespeichert. Der Hauptteil dieser Nummer muss eine oder einen Verantwortlichen eindeutig identifizieren können und darf nicht mehrfach vergeben werden.

Im vorliegenden Fall war jedoch genau das passiert. Eine Arztpraxis hatte denselben Hauptteil erhalten wie die AOK Niedersachsen. Beide Identifikationsnummern hatten lediglich unterschiedliche Endungen. Einige Praxisverwaltungssysteme waren so programmiert, dass diese für die Zuord-

1 § 291b Abs. 4 Satz 2 Sozialgesetzbuch – Fünftes Buch (SGB V).
2 § 306 Sozialgesetzbuch – Fünftes Buch (SGB V).
3 § 295 Abs. 1 Satz 1 Nummer 1 und Satz 10 Sozialgesetzbuch – Fünftes Buch (SGB V).
4 Kommunikation im Medizinwesen (KIM) – ein TI-Dienst der gematik zur sicheren Übermittlung von Gesundheitsdaten.

nung der KIM-Adresse lediglich den Hauptteil der Identifikationsnummer genutzt haben.

Mehrere Arztpraxen, die eine elektronische Arbeitsunfähigkeitsmeldung (eAU) für die AOK Niedersachsen ausgestellt und den richtigen Adressaten ausgewählt hatten, haben aufgrund des unglücklichen Zusammenspiels dieser beiden Umstände dennoch die eAU unwissend an die unbeteiligte Arztpraxis versendet. In der Zeit vom 1. Juli 2022 bis zum 30. Juni 2023 waren es insgesamt über 116.000 eAU-Meldungen einer Vielzahl von Arztpraxen. Die empfangende Praxis hatte von den unzähligen eAU-Meldungen lediglich durch einen Hinweis des Systems erfahren, dass das Eingangspostfach zu voll sei.

KIM ist modular aufgebaut. Das bedeutet, dass die Arztpraxen zwar das Modul kaufen und nutzen müssen, das die eAU versendet, nicht jedoch das Modul, das auch E-Mails oder Arztbriefe empfangen kann. Da Arztpraxen keine Empfänger von eAU-Meldungen sind, gab es keine Verpflichtung, ein möglicherweise vorhandenes Eingangspostfach regelmäßig zu prüfen. Insofern war der empfangenden Praxis kein datenschutzrechtliches Fehlverhalten vorzuwerfen.

Richtige Reaktion der Praxis

Nachdem die Praxis Kenntnis von den unbefugt erhaltenen eAU-Meldungen hatte, unternahmen deren Verantwortliche unverzüglich alle erforderlichen Schritte, damit dies nicht mehr vorkommt. Sie benachrichtigten die AOK Niedersachsen, die für den KIM-Dienst zuständige Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (Gematik) und den Hersteller der Praxisverwaltungssysteme. Unmittelbar nach Kenntnis des Vorfalls bei der Gematik am 1. Juli 2023 hat die Arztpraxis eine neue KIM-Identifikationsnummer erhalten. Die Gematik hat den Datenbestand des KIM-TI-Verzeichnisdienstes auf mögliche weitere Redundanzen geprüft und die Hersteller der Praxisverwaltungssysteme haben ihr Programm so umgestellt, dass es zukünftig die gesamte Identifikationsnummer abgleicht. Ein derartiger Vorfall sollte sich daher nicht noch einmal wiederholen.

Ein hohes datenschutzrechtliches Risiko für die betroffenen Patientinnen und Patienten hat zu keinem Zeitpunkt vorgelegen, da die Arztpraxis alle

erforderlichen Schritte eingeleitet hatte und nur wenige inhaltliche Daten zur Kenntnis genommen hat.

Vollständige Nutzung von KIM wird Pflicht

Im Rahmen des Digitalgesetzes[5] beabsichtigt der Gesetzgeber, die Leistungserbringer zu verpflichten[6], die Empfangsbereitschaft für elektronische Briefe in der vertragsärztlichen Versorgung sicherzustellen. Es ist davon auszugehen, dass der Bundesrat das Gesetz in seiner Plenarsitzung im Februar 2024 verabschiedet. Mit Inkrafttreten dieser Regelung müssen die Gematik GmbH und Herstellenden von TI Komponenten aus unserer Sicht eine vollständige und durchgehende Verfügbarkeit von KIM für die Nutzenden gewährleisten. Wird dies sichergestellt, ist eine regelmäßige Kontrolle des elektronischen Posteingangs für alle Verantwortlichen unumgänglich.

Ab diesem Zeitpunkt hat aus datenschutzrechtlicher Sicht zudem sämtliche elektronische Kommunikation zwischen Leistungserbringenden über einen datenschutzkonformen Dienst wie beispielsweise KIM zu erfolgen. Die Übermittlung von Patientendaten zwischen Leistungserbringenden über unsichere Kommunikationswege wie Fax oder eine unverschlüsselte E-Mail sind dann nicht mehr zu rechtfertigen. Wir werden solche Übermittlungswege als Datenschutzbehörde dann nicht mehr hinnehmen.

Wir als Datenschutzbehörde werden solche Übermittlungswege dann nicht mehr hinnehmen.

5 Vom Bundestag am 14.12.2023 beschlossen.

6 § 295 Absatz 1c Sozialgesetzbuch – Fünftes Buch (SGB V).

Unzureichender Zugriffsschutz bei E-Mail-Funktionskonten führt zu einem Bußgeld G.4.3

Über unser Beschwerdeformular erhielten wir den Hinweis, dass drei E-Mail-Funktionskonten eines Krankenhauses in Niedersachsen nur unzureichend vor dem Zugriff durch unbefugte Externe geschützt waren.

Es gibt vermutlich nur wenige Unternehmen, die keine E-Mail-Funktionskonten wie „info@…" oder „poststelle@…" verwenden. Dies ist bei datenschutzkonformer Einrichtung nicht zu beanstanden. Wird zudem die Funktion „Outlook im Web" (OWA) verwendet, kann der Nutzer über einen Webbrowser auf das jeweilige Postfach zugreifen. Dafür benötigt er außer der Internetadresse des Unternehmens den Namen der Domäne und ein Passwort. Ein Hinweisgeber teilte uns zwei Namen von Domänen mit, von denen einer aus den Anfangsbuchstaben des Klinikums bestand und damit relativ leicht zu erraten gewesen ist.

Im Gegensatz zu personalisierten Funktionskonten wie „Vorname.Nachname@…" ist das Passwort bei Funktionskonten in der Regel nicht an das Passwort und den Account eines individuellen Nutzenden gebunden, sondern wird zentral vergeben. Bei der erstmaligen Einrichtung von E-Mail-Konten werden durch Administrationen häufig Passwörter wie „123456", „654321" oder „Passwort" vergeben, damit die später für das Postfach zuständigen Beschäftigen sich erstmalig anmelden können. Derartige Passwörter sind nach der ersten Anmeldung in sichere Passwörter entsprechend einer Passwortrichtline zu ändern. Dies war im vorliegenden Fall zunächst unterblieben.

Mittels eines Trivialpasswords war uns ein Zugriff auf mehrere Funktionskonten möglich.

Mittels eines Trivialpasswords war uns ein Zugriff auf mehrere Funktionskonten des Klinikums, unter anderem auf das Haupt-E-Mail-Postfach „info@…" möglich. In diesem Postfach befanden sich zum Zeitpunkt unseres Zugriffs über 7.500 E-Mails aus mehreren Jahren. Auch wenn ein Großteil der E-Mails lediglich Werbung oder Spammails waren, enthielten einige Mails auch sensible Gesundheitsinfor-

mationen. Wir informierten die Klinikleitung unverzüglich telefonisch über den Vorfall, die daraufhin sofort die Zugangspasswörter ändern ließ. Sie sagte eine Überprüfung der übrigen Funktionskonten auf Trivialpasswörter zu.

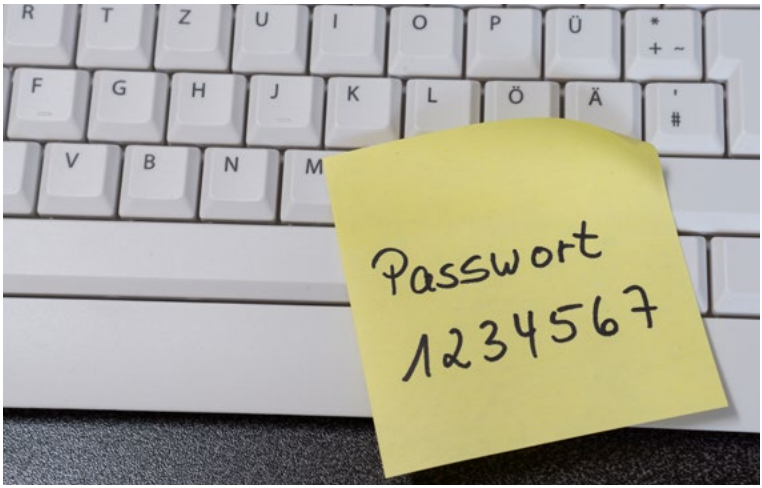
Zweiter Vorfall innerhalb weniger Wochen

Nur wenige Wochen nach dem ersten Vorfall bekamen wir erneut einen anonymen Hinweis, dass bei dem Klinikum mittels Trivialpasswörtern mindestens sieben weitere Funktionskonten über OWA zugänglich waren. Auch diese Meldung konnten wir nachvollziehen. In einer ergänzenden Stellungnahme teilte das Klinikum mit, dass man sich auf die Aussage eines Beschäftigten verlassen habe, der angegeben habe, dass alle Funktionskonten maschinell überprüft wurden.

Aufgrund unserer zweiten Mitteilung an das Krankenhaus stellte sich heraus, dass offenbar aufgrund einer fehlerhaften Konfiguration doch nicht alle E-Mail-Konten von dem maschinellen Verfahren erfasst wurden. Das Klinikum hat daraufhin händisch über 100 Funktionskonten geprüft und sofern erforderlich auf sichere Passwörter umgestellt. Auf die Nutzung der OWA-Funktion will das Klinikum nach Umstellung der Informationstechnik in Zukunft verzichten und hat entsprechende Maßnahmen eingeleitet. Ein weiterer Vorfall wurde seitdem nicht gemeldet und ist in Anbetracht der seitens des Krankenhauses ergriffenen Maßnahmen auch nicht zu befürchten. Hervorzuheben ist die gute Zusammenarbeit des Krankenhauses mit uns im Rahmen der Sachverhaltsaufklärung.

Fazit

Der Betrieb von Funktionspostfächern im Gesundheitswesen, welche lediglich mit einem Trivialpasswort gesichert sind, stellt einen eklatanten Verstoß gegen die nach der Datenschutz-Grundverordnung (DSGVO) vom Verantwortlichen einzurichtenden technisch-organisatorischen Schutzmaßnahmen dar. Erschwerend kommt hinzu, dass das Klinikum nach Bekanntwerden des ersten Vorfalls zwar Maßnahmen ergriffen hatte, diese jedoch nicht mit einer Stichprobe auf ihre Wirksamkeit hin überprüfte. In Anbetracht der besonderen Kategorien personenbezogener Daten wäre eine umfangreiche Stichprobe angezeigt gewesen.



Mit voreingestellten Trivialpasswörtern riskieren Verantwortliche Datenschutzverstöße.

Da uns bei der zweiten Meldung sogar sieben weitere Funktionskonten gemeldet wurden, ist die Wahrscheinlichkeit hoch, dass dem Klinikum bei einer solchen Stichprobe zumindest ein Funktionskonto aufgefallen wäre, bei welchem die elektronischen Maßnahmen nicht erfolgreich waren. Dadurch hätte der zweite Vorfall eventuell verhindert werden können.

Nach Würdigung aller Umstände haben wir als Abhilfemaßnahme den Datenschutzverstoß festgestellt und ein Bußgeldverfahren eingeleitet. Letzteres ist 2024 mit einem Bußgeldbescheid rechtskräftig abgeschlossen worden. Positiv berücksichtigt wurde bei der Bußgeldbemessung insbesondere die konstruktive Zusammenarbeit der Krankenhausleitung mit der Datenschutzaufsicht.

G.4.4 Personaldatenbank mit auffälligen Personen in der Kinderbetreuung – Rechtsgrundlage fehlt

Das Landesamt für Soziales, Familie und Jugend wollte eine Personaldatenbank einführen, die als Zusatzfunktion trägerübergreifend auffällige Personen in der Kindertagesbetreuung speichert. Aus Sicht der niedersächsischen Datenschutzbehörde aber fehlt dafür derzeit eine Rechtsgrundlage.

Vor Einführung einer Personaldatenbank, die Angaben über auffällig gewordene (ehemalige) Beschäftigte aus Einrichtungen der Kindertagesbetreuung speichern sollte, hat sich das Landesamt für Soziales, Familie und Jugend (LS) an uns gewandt und um datenschutzrechtliche Beratung gebeten.

Zum Schutz der Kinder haben die Träger erlaubnispflichtiger Einrichtungen[1] der Kindertagesbetreuung sich von allen Beschäftigten vor der Einstellung und anschließend in regelmäßigen Abständen einen Auszug aus dem polizeilichen Führungszeugnis vorlegen lassen.[2] Personen, die aufgrund einer Straftat in Bezug auf das Wohlergehen von Kindern rechtskräftig verurteilt wurden, dürfen nicht in der Kinderbetreuung eingestellt werden. Das LS hat in diesem Bereich einen Kontrollauftrag gegenüber den Einrichtungen.

Hintergrund für die beabsichtigte Einrichtung dieser Personaldatenbank waren meldepflichtige Vorkommnisse.[3] Die Träger der Einrichtungen sind verpflichtet, dem LS unverzüglich Ereignisse oder Entwicklungen anzuzeigen, die geeignet sind, das Wohl von Kindern und Jugendlichen zu beeinträchtigen. Aufgabe des LS ist es, die seitens der Einrichtungen eingeleiteten Abhilfemaßnahmen zu bewerten. Das LS kann je nach Bedarf weitere Maßnahmen bis hin zu einem Beschäftigungsverbot der betroffenen Person gegenüber der Einrichtung anordnen. Die Meldung eines solchen Vor-

1 § 45 Sozialgesetzbuch – Achtes Buch (SGB VIII).
2 § 72a Sozialgesetzbuch – Achtes Buch (SGB VIII).
3 § 47 Sozialgesetzbuch – Achtes Buch (SGB VIII).

falls an das LS darf dort nach der derzeitigen Rechtslage jedoch nur einrichtungsbezogen gespeichert werden.

In der Praxis kommt es vor, dass eine Einrichtung oder die Eltern erst dann von einem Vorfall erfahren, wenn die Täterin oder der Täter die Einrichtung bereits verlassen hat. Sofern diese auffällig gewordenen, jedoch nicht rechtskräftig verurteilten Personen sich bei einer anderen Einrichtung bewerben, kann weder die neue Einrichtung noch das LS als Aufsichtsbehörde nachvollziehen, ob es in der Vergangenheit bereits Auffälligkeiten in Bezug auf diese Person gegeben hat. Die vom LS geplante landesweite Datenbank sollte dem Zweck dienen, diese Personen bei Aufnahme einer neuen Beschäftigung im Bereich der Kinder- und Jugendhilfe gründlicher zu überprüfen.

Der Gesetzgeber ist in der Pflicht

Als Aufsichtsbehörde für den Datenschutz haben wir die geltenden Gesetze zu beachten und jeden Sachverhalt objektiv zu beurteilen. Wir kamen nach eingehender Prüfung zum Schluss, dass das LS das einrichtungsübergreifende Speichern der Daten auf keine Rechtsgrundlage stützen kann.

Wenngleich das Anliegen der Einführung einer trägerübergreifenden elektronischen Personaldatenbank auffällig gewordener Personen vor dem Hintergrund aktueller Vorfälle gut nachvollziehbar ist, bedarf es einer bundesgesetzlichen Rechtsgrundlage. Eine solche Initiative begleiten wir gerne konstruktiv.

Konsequentes Ausschöpfen der rechtlichen Möglichkeiten

In Anbetracht der fehlenden Rechtsgrundlage haben wir dem LS empfohlen, den Einrichtungen nahezulegen, konsequent Strafanzeige zu erstatten, sobald auch nur der Verdacht einer strafbaren Handlung im Zusammenhang mit der Betreuung von Kindern aufkommt.

G.4.5 EuGH-Urteil: Kopie einer Patientenakte muss kostenfrei ausgehändigt werden

Seit Anwendungsbeginn der Datenschutz-Grundverordnung gab es immer wieder Streit, ob Verantwortliche für eine Kopie der Patientenakte eine Aufwandsentschädigung verlangen können. Der EuGH hat nun die vom LfD Niedersachsen vertretene Rechtsauffassung bestätigt.

Auslöser der Streitigkeiten war eine Regelung im Bürgerlichen Gesetzbuch (BGB), welche mit dem Patientenrechtegesetz[1] im Februar 2013 aufgenommen wurde. Hiernach haben Patientinnen und Patienten ein Recht auf Kopien aus der Patientenakte, sind jedoch verpflichtet, dem Verantwortlichen die entstandenen Kosten zu erstatten. Mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) wurde vom Bundesgesetzgeber versäumt, die Regelung im BGB an die rechtlich vorrangigen Regelungen der DSGVO[2] anzupassen, Verantwortliche haben auf die Kostenerstattung bestanden, selbst wenn diese von den Patientinnen und Patienten auf unsere online veröffentlichten Ausführungen zur Kostenfreiheit hingewiesen wurden.[3] Infolgedessen kam es immer wieder zu Beschwerden und entsprechenden aufsichtsbehördlichen Abhilfemaßnahmen.

Einige Verantwortliche haben sich darauf berufen, dass das kostenfreie Auskunftsrecht nach der DSGVO nur dann Anwendung finden könne, wenn Betroffene interessehalber wissen wollen, welche Daten gespeichert sind. Für eine Vorbereitung etwaiger Klageverfahren gegen die Verantwortlichen sei das Auskunftsrecht nach der DSGVO nicht anzuwenden.

Als Datenschutzaufsichtsbehörde in Niedersachsen haben wir stets die Auffassung vertreten, dass das Auskunftsrecht nach der DSGVO keinen besonderen individuellen Grund voraussetzt, die Vorschrift des BGB verdrängt und daher stets eine kostenfreie erste Kopie ausgehändigt werden muss. Klageverfahren gegen die von uns erlassenen Abhilfemaßnahmen

1 § 630g Absatz 2 BGB.
2 Art. 15 Abs. 3 i.V.m. Art. 12 Abs. 5 DSGVO.
3 Siehe dazu „FAQ DSGVO im Gesundheitsbereich", https://lfd.niedersachsen.de/229071.html

hat es nicht gegeben, allerdings wurden solche Entscheidungen anderer Datenschutzaufsichtsbehörden gerichtlich überprüft.

Am 26. Oktober 2023 hat der Europäische Gerichtshof (EuGH) mit seinem Urteil in der Rechtssache C-307/22 abschließend in drei Leitsätzen festgestellt:

- Die Herausgabe einer Kopie der Patientenakte erfolgt unentgeltlich.
- Der mit der Geltendmachung eines Anspruchs auf Kopie verfolgte Zweck ist unerheblich.
- Eine Reproduktion einer gesamten Akte ist immer dann herauszugeben, wenn dies zum Verständnis der Informationen erforderlich ist.

Nach Entscheidung des EuGHs ist die in der DSGVO geregelte Unentgeltlichkeit einer ersten Kopie[4] der verarbeiteten Daten vorrangig vor dem deutschen Zivilrecht anzuwenden[5], sodass für Auskunftsersuchen und erste Kopien der personenbezogenen Daten keine Kosten zu erheben sind.

Weiter stellte der EuGH fest, dass die betroffene Person nicht verpflichtet ist, ihren Antrag auf Herausgabe einer Kopie zu begründen. Daneben komme es nicht auf den mit dem Antrag tatsächlich verfolgten Zweck an.

Der mit der Geltung eines Anspruchs verfolgte Zweck ist unerheblich.

Das Recht auf Kopie umfasse immer dann eine Reproduktion der vollständigen Akte, wenn dies zum Verständnis der in den Dokumenten enthaltenen personenbezogenen Daten unerlässlich ist. Im Falle einer Patientenakte schließt dies insbesondere Diagnosen, Untersuchungsergebnisse, ärztliche Befunde und Angaben zu Behandlungen oder Eingriffen ein.

4 Art. 12 Abs. 5 DSGVO.
5 Art. 15 Abs. 3 DSGVO.

G.4.6 Antworten auf die häufigsten Fragen zum Datenschutz im Gesundheitsbereich

Der Datenschutz im Gesundheitsbereich bleibt ein zentrales Anliegen der Bürgerinnen und Bürger wie auch der Leistungserbringenden im Gesundheitswesen. Aufgrund aktueller höchstrichterlicher Entscheidungen wie beispielsweise zur Kostenfreiheit von Kopien aus der Patientenakte haben wir unsere FAQ zum Thema aktualisiert.

Auch fünf Jahre nach Anwendungsbeginn der Datenschutz-Grundverordnung (DSGVO) erhalten wir regelmäßig neue Fragen zum richtigen Umgang mit Gesundheitsdaten. Die im Jahr 2018 erstellten FAQ zur DSGVO im Gesundheitswesen konnten bereits viele regelmäßige Fragen beantworten. Gleichwohl konnten längst nicht alle denkbaren Themenkomplexe und Fragen in den ersten Versionen der FAQ berücksichtigt werden. Regelmäßig tauchen auch neue Fragenkomplexe auf.

Die nun in einigen Bereichen vorliegenden höchstrichterlichen Entscheidungen auf Bundes- und Europäischer Ebene, wie beispielsweise zum Auskunftsrecht einerseits und weitgehend bundeseinheitliche Rechtsauffassungen der Datenschutz-Aufsichtsbehörden andererseits, haben wir zum Anlass genommen, die bestehenden FAQ im Jahr 2023 grundlegend zu überarbeiten.

Neue Struktur und aktualisierte Antworten

Die vorgenannten Entscheidungen und zwischenzeitlichen Rechtsänderungen wie beispielsweise im Sozialgesetzbuch wurden ebenso aufgenommen wie einige neue Bereiche. Anhand der vorliegenden Beratungsanfragen wurden in den FAQ Themenblöcke für Bürgerinnen und Bürger auf der einen Seite und für Leistungserbringende auf der anderen Seite gebildet. Alle Antworten der bisherigen FAQ haben wir aktualisiert und neu strukturiert. Dabei haben wir Anregungen von Bürgerinnen und Bürgern, aber auch aus der Praxis der Gesundheits(dienst)berufe und von Seiten der Berufskammern gerne mit aufgenommen.

Neu aufgenommen sind außerdem die Bereiche der digitalen Kommunikation im Gesundheitswesen, digitale Gesundheitsanwendungen sowie das datenschutzkonforme Verhalten bei der Auflösung von Berufsausübungsgemeinschaften.

Bereits in der Vergangenheit wurden die FAQ Datenschutz im Gesundheitswesen sowohl von Bürgerinnen und Bürgern, als auch von Leistungserbringenden dankend angenommen, da durch sie auf allen Seiten Klarheit geschaffen und Zweifel beseitigt werden konnten. Wir beabsichtigen, auch in Zukunft regelmäßig Themenbereiche zu ergänzen und aktuelle Rechtsprechungen einfließen zu lassen.

Auf der Webseite unserer Datenschutzbehörde finden Sie unter dem Link https://lfd.niedersachsen.de/229071.html die aktuelle Version der FAQ zum Datenschutz im Gesundheitsbereich.

Kommunen und Verwaltung

G.5.1 Kommunen: Datenschutzverletzungen durch Hackerangriffe und fehlende Schwärzungen

Im Tätigkeitsbericht 2022 haben wir über unsere anlassunabhängige Prüfung von 50 niedersächsischen Kommunen berichtet. Im Jahr 2023 haben wir bei ausgewählten Stadt- und Gemeindeverwaltungen vor Ort deren Verzeichnis der Verarbeitungstätigkeiten untersucht.

Im Rahmen unserer datenschutzrechtlichen Prüfung von 50 niedersächsischen Kommunen haben wir bei der Auswertung des Verzeichnisses der Verarbeitungstätigkeiten zum Teil große Unterschiede bei der Anzahl der gemeldeten Verarbeitungen zum Melderecht festgestellt.[1] Des Weiteren berichteten uns die Verantwortlichen von melderechtlichen Verarbeitungstätigkeiten im Bürgerbüro durch Mitarbeiterinnen und Mitarbeiter, die auf dem ersten Blick keinen Bezug zum Melderecht haben. Aus diesen Gründen haben wir uns entschlossen, mit einigen Kommunen Gespräche vor Ort zu führen.

Die Stadt- und Gemeindeverwaltungen führen das Bundesmeldegesetz (BMG) sowie das Niedersächsische Ausführungsgesetz zum Bundesmeldegesetz (Nds. AG BMG) aus. Somit ist davon auszugehen, dass die Verarbeitungstätigkeiten im Bereich des Melderechts weitgehend identisch sind. Zielsetzung der Gespräche war es deshalb unter anderem, zu klären, welche melderechtlichen Verarbeitungstätigkeiten die Kommunen erledigen.

Mit Unterstützung der besuchten Kommunen wollen wir nach Abschluss der Untersuchungen eine Hilfestellung zum Anfertigen eines Verzeichnisses der Verarbeitungstätigkeiten veröffentlichen. Diese wird sich auf

1 Siehe Tätigkeitsbericht 2022, J.3.4 und Prüfbericht „Zweite überörtliche Datenschutzprüfung bei Kommunen", abrufbar unter https://lfd.niedersachsen.de/221102.html

melderechtliche Verarbeitungsvorgänge beziehen und die im Melderegister verarbeiteten personenbezogenen Daten und deren unterschiedliche Löschfristen berücksichtigen.

Besuch der Bürgerbüros

Die Termine in den Rathäusern nutzten wir auch zum Besuch der Bürgerbüros. Hier lag ein Augenmerk auf der datenschutzkonformen Gestaltung der Räumlichkeiten. Insbesondere achteten wir in Abhängigkeit von den räumlichen Gegebenheiten darauf, ob der Wartebereich ausreichend vom Arbeitsbereich der Beschäftigten abgegrenzt ist.

Erfreulicherweise bieten alle bisher besuchten Bürgerbüros die Möglichkeit, Gespräche in einem getrennten Raum zu führen. Auf dieses Angebot ist deutlich sichtbar hinzuweisen. Die bisherigen Termine vor Ort gaben keinen Anlass zu Beanstandungen.

Des Weiteren nahmen wir die von den Bürgerbüros genutzte Meldesoftware in Augenschein. Die endgültigen Ergebnisse der Vor-Ort-Termine werden im Laufe des Jahres 2024 vorliegen.

Datenschutzverletzungen

Im vergangenen Jahr waren erneut niedersächsische Kommunen von Hackerangriffen und dadurch auch von Datenschutzverletzungen betroffen. Die Folge dieser Vorkommnisse ist, dass die Landkreise, Städte und Gemeinden während der Abwehr eines Angriffs nicht oder nur eingeschränkt handlungsfähig sind. In diesem Zeitraum sind die IT-Systeme meist nicht verfügbar und die für die Bearbeitung notwendigen personenbezogenen Daten stehen nicht zur Verfügung.

Auswirkungen ergeben sich für Kommunen auch dann, wenn deren Auftragsverarbeiter von Hackern angegriffen werden. Diese können dann den Zugriff auf von ihnen im Auftrag der Kommunen verarbeitete personenbezogene Daten nicht mehr gewährleisten. Insoweit ist es notwendig, dass die Verantwortlichen sich auch aus datenschutzrechtlicher Sicht auf entsprechende Vorfälle vorbereiten. In diesen Fällen greifen Datenschutz und IT-Sicherheit ineinander.

Weitere gemeldete Datenschutzverletzungen betrafen die Offenlegung von personenbezogenen Daten zum Beispiel durch fehlende Schwärzungen bei Veröffentlichungen im Internet oder bei der Gewährung von Akteneinsicht.

Insbesondere beim Bereitstellen von Dokumenten über Bürgerinformationssysteme wurde erneut deutlich, dass sich die Verantwortlichen der damit verbundenen Risiken für die betroffenen Personen nicht hinreichend bewusst waren. Teilweise unterblieben datenschutzrechtlich gebotene Schwärzungen. Immerhin korrigierten sie die Dokumente unverzüglich nach entsprechenden Hinweisen, um die Offenlegung der personenbezogenen Daten zu beenden. In Abhängigkeit von der Art und dem Umfang der betroffenen personenbezogenen Daten sprachen wir aufsichtsbehördliche Maßnahmen aus.

Teilweise unterblieben datenschutzrechtlich gebotene Schwärzungen.

Prüfung der Gewerbeaufsicht: Vorsicht bei Löschfristen G.5.2

Im Jahr 2022 hatte unsere Behörde alle niedersächsischen staatlichen Gewerbeaufsichtsämter in Hinblick auf datenschutzrechtliche Pflichten schriftlich geprüft. Ein Jahr später untersuchten wir stichprobenartig zwei Ämter vor Ort – und stellten Mängel beim Einhalten der Löschfristen fest.

Im ersten Quartal 2023 haben wir zwei zufällig ausgewählte Gewerbeaufsichtsämter vor Ort geprüft. Unsere Prüfung bezog sich auf die organisatorische Absicherung bei der konkreten Bearbeitung von Vorgängen. Hierbei haben wir zwei Themenschwerpunkte gesetzt.

Zum einen haben wir ausgewählte Räumlichkeiten geprüft, nämlich den jeweiligen Empfangsbereich („Tresen"), den Wartebereich und einzelne Großraumbüros. Relevant war, ob hinreichende räumliche und auch im übrigen organisatorische Vorkehrungen getroffen worden waren, damit personenbezogene Daten nicht unbefugten Dritten zur Kenntnis gelangen. Das Ergebnis war erfreulich: Es bestand kein Anlass zu einer Beanstandung.

Der zweite Themenschwerpunkt bezog sich auf die Frage der Löschfristen, und zwar auf den zufällig ausgewählten Bereich der sogenannten Nachbarschaftsbeschwerden. Dies sind Vorgänge, bei denen sich Nachbarn gegen einen nahegelegenen Gewerbebetrieb beim jeweiligen Gewerbeaufsichtsamt beschweren, beispielsweise in Hinblick auf Lärm- oder Geruchsbeeinträchtigung.

Hinsichtlich der Löschfristen führten beide Gewerbeaufsichtsämter die Nachbarschaftsbeschwerden nicht als separaten Vorgang, sondern chronologisch als Teil der gesamten Betriebsakte. Diese Betriebsakte wird dort jeweils solange geführt, wie der Betrieb existiert. Erst bei Stilllegung des Betriebs wird die Akte geschlossen, sodass in den beiden geprüften Gewerbeaufsichtsämtern erst ab dann die Löschfrist beginnen würde.

Beginn der Aufbewahrungsfrist vom Einzelfall abhängig

Gemäß der niedersächsischen Aktenordnung[1] sind nicht nur Akten, sondern als Teilbereich auch „Vorgänge" zu schließen, wenn sie für den Geschäftsbetrieb nicht mehr benötigt werden. Anschließend, konkret ab dem darauffolgenden 1. Januar, beginnt die Aufbewahrungsfrist.[2] Die Aufbewahrungsfrist beträgt in der Regel 15 Jahre. Daher enthält die Aktenordnung eine doppelte Differenzierung: Neben der Akte ist auch ein gesonderter Vorgang mit einer eigenen Aufbewahrungsfrist möglich. Zudem ist der jeweilige Vorgang individuell dann zu schließen, wenn er für den Geschäftsbetrieb nicht mehr benötigt wird.

Vor diesem Hintergrund ist ein Nachbarschaftsbeschwerde-Vorgang separat als gesonderter Vorgang zu behandeln und zudem auf die eigene Erforderlichkeit für den Geschäftsbetrieb, also die Relevanz für die rechtliche Bewertung des Betriebs, zu prüfen. Die in beiden Gewerbeaufsichtsämtern vorgenommene Interpretation der Aktenordnung, bei sämtlichen (Teil-) Vorgängen der Betriebsakte erst ab Stilllegung des Betriebs die Aufbewahrungsfrist beginnen zu lassen, entsprach daher nicht der Aktenordnung.

Bei einem der beiden geprüften Gewerbeaufsichtsämtern bestand zudem kein Löschkonzept und damit keine hinreichende Löschpraxis zu den bereits abgeschlossenen Vorgängen. Als Ergebnis der Prüfung sind beide Gewerbeaufsichtsämter gemäß Datenschutz-Grundverordnung (DSGVO) von unserer Behörde sensibilisiert und auf die Vorgaben der DSGVO in Verbindung mit der niedersächsischen Aktenordnung hingewiesen worden.

Fazit

Die Aufbewahrungsfrist beläuft sich zwar oftmals einheitlich auf 15 Jahre – aber der Beginn dieser Aufbewahrungsfrist kann divergieren. Zu prüfen ist jeweils individuell, ob die Gesamtakte einzelne, abgrenzbare Vorgänge enthält, die für den Geschäftsbetrieb der Behörde, also für den Zweck der Akte, nicht mehr benötigt werden. Sofern solche Vorgänge keine Relevanz mehr haben, sind sie zu schließen und die übliche Aufbewahrungsfrist beginnt ab diesem individuellen Zeitpunkt.

1 9.1/9.2 Aktenordnung und Aktenplan für die niedersächsische Landesverwaltung, RdErl. d. MI v. 18. 8. 2006 – 12-02201/02202.

2 Vgl. Art. 57 Abs. 1 Buchst. d DSGVO.

Wer darf die Akten des Sozialpsychiatrischen Dienstes einsehen? G.5.3

Patientinnen und Patienten des Sozialpsychiatrischen Dienstes befinden sich regelmäßig in einer gesundheitlichen Ausnahmesituation. Anlässlich eines Medienberichts prüften wir im Jahr 2023, wer deren sensible Gesundheitsinformationen zu Aufsichtszwecken überhaupt verarbeiten darf.

Im Sommer 2022 wurde ein Gullydeckel auf die Autobahn A 7 geworfen, der ein fahrendes Auto traf. Zwei Menschen wurden teils schwer verletzt. Zunächst richtete sich der Verdacht gegen eine Person, die vom ärztlichen Fachpersonal des Sozialpsychiatrischen Diensts (SpDi) behandelt wurde.[1] Eine Fraktion eines Kreistages forderte den Landrat auf, Informationen aus der Behandlungsakte des Patienten herauszugeben, um den Vorgang „sachverständig" beurteilen zu können. Da die Zahl der Beratungsanfragen im Verlauf des Jahres 2023 in diesem Bereich zunahm, verschafften wir uns einen Überblick über die Praxis der Aufsichtstätigkeit über den SpDi. Wir befragten unter anderem das Netzwerk Kommunaler Datenschutz, welche Stellen Einsicht in die Behandlungsakte von erkrankten Personen erhalten.

Keine Akteneinsichtsrechte für Mitglieder der kommunalen Vertretung

Einzelne Mitglieder einer kommunalen Vertretung haben auf Antrag einer Fraktion oder eines Viertels der Mitglieder der Vertretung das Recht, Akten einer Kommune einsehen zu können. Der SpDi war im vorliegenden Fall organisatorisch einem Landkreis zugeordnet. Allerdings unterliegen dem Akteneinsichtsrecht der Mitglieder einer kommunalen Vertretung nicht solche Informationen, die geheim zu halten sind.[2] Die ärztliche Schweigepflicht schützt das besondere Vertrauensverhältnis zwischen erkrankten

1 NDR, Gullydeckel-Wurf: Beschuldigter wird psychiatrisch untersucht, abrufbar unter: https://ndr.de/gullydeckel152.html

2 § 58 Abs. 4 S. 4 NKomVG.

Personen und ärztlichem Fachpersonal. Davon umfasst sind auch medizinische Fachgutachten oder die Dokumentation von Betreuungs- und Behandlungsverläufen von Patienten und Patientinnen des SpDi. Daher berieten wir den Landkreis dahingehend, der Fraktion keine Akteneinsicht zu gewähren.

Keine Akteneinsichtsrechte für Hauptverwaltungsbeamte

Hauptverwaltungsbeamtinnen und Hauptverwaltungsbeamte (HVB)[3] repräsentieren die Kommune.[4] Ausweislich eines Presseberichts[5] wurde ein HVB von einer Person bedroht, die vom SpDi behandelt wurde. Dürfen nun HVB Einblick in SpDi-Behandlungsakten nehmen? Schließlich sind sie als kommunale (Wahl-)Beamte zur Geheimhaltung verpflichtet und sie erfüllen Aufgaben, die der Geheimhaltung unterliegen.[6] Man könnte daher argumentieren, dass auch die Akteninhalte geheim bleiben, wenn sie innerhalb der Kommune offenbart werden.

Das medizinische Behandlungsverhältnis stellt ein besonderes Vertrauensverhältnis dar, das nicht durch Aufsichtsmaßnahmen gestört werden darf.

Allerdings stellt das medizinische Behandlungsverhältnis ein besonderes Vertrauensverhältnis dar, das nicht durch Aufsichtsmaßnahmen gestört werden darf.

Denn das Niedersächsische Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke (NPsychKG) unterscheidet bei der Verarbeitung von personenbezogenen Daten nach der Art der betroffenen Daten. In einer Vorschrift des NPsychKG heißt es sinngemäß, dass personenbezogene Daten zur Wahrnehmung von Aufsichts- und Kontrollbefugnissen verarbeitet werden dürfen, wenn dies erforderlich ist.[7] Zwar sind auch Gesundheitsdaten personenbezogene Daten, aber sie unterliegen einem spezielleren Schutz. Im NPsychKG kommt dies dadurch zum Ausdruck, dass eine wei-

3 Samtgemeindebürgermeisterinnen und Samtgemeindebürgermeister, (Ober-)Bürgermeisterinnen und (Ober-)Bürgermeister, Landrätinnen und Landräte sowie der oder die Regionspräsident/in der Region Hannover (§ 7 Abs. 2 NKomVG).

4 § 86 Abs. 1 NKomVG.

5 NDR, Harsums Bürgermeister beantragt Personenschutz, abrufbar unter: https://ndr.de/buergermeister504.html

6 § 85 Abs. 1 Nummer 5 NKomVG.

7 § 32 Abs. 2 NPsychKG.

tere Vorschrift die Datenverarbeitung mit diesen „besonderen" personenbezogenen Daten regelt.[8] In dieser Vorschrift ist aber keine Datenverarbeitung zu Aufsichtszwecken vorgesehen. Damit ist sie nicht erlaubt.

Die Entscheidung des niedersächsischen Gesetzgebers ist richtig. Erkrankte Personen müssen dem ärztlichem Fachpersonal ihre physischen und psychischen Probleme anvertrauen dürfen, ohne befürchten zu müssen, dass Gesundheitsinformationen ungefragt Dritten preisgegeben werden. Andernfalls könnten sich erkrankte Personen entscheiden, ihre gesundheitlichen Probleme für sich zu behalten oder sich gar nicht erst behandeln zu lassen. Insbesondere im Fall einer psychischen Erkrankung kann dies schwerwiegende Folgen für den Betroffenen haben.

Keine Akteneinsichtsrechte für Ministerium

Diese Wertung greift auch im Verhältnis zwischen dem Niedersächsischen Ministeriums für Soziales, Gesundheit und Gleichstellung als Fachaufsichtsbehörde über die Landkreise und kreisfreien Städte. Auch dessen Informationsrechte sind in dieser Hinsicht beschränkt.

Akteneinsichtsrechte der Fachbereichsleitung des SpDi

Unsere Abfrage im Netzwerk kommunaler Datenschutz ergab, dass der SpDi organisatorisch oftmals dem Gesundheitsamt zugeordnet ist. Der Leiter oder die Leiterin des SpDi leitet das Gesundheitsamt und den SpDi. Diese Praxis ist datenschutzrechtlich vertretbar, solange technisch und organisatorisch sichergestellt ist, dass die Datenverarbeitung des Gesundheitsamts und des SpDi nicht miteinander vermengt wird. Die Tätigkeit des SpDi ist vom Umgang mit besonders sensiblen personenbezogenen Daten von erkrankten Menschen geprägt, die nur zur Erfüllung von Aufgaben nach dem NPsychKG verarbeitet werden dürfen.[9] Die öffentlichen Gesundheitsämter fördern und schützen hingegen die Gesundheit der Gesamtbevölkerung. Zur Erfüllung dieser Aufgabe sind sie nicht auf personenbezogene Daten von Patientinnen und Patienten des Sozialpsychiatrischen Dienstes angewiesen.

8 § 33 NPsychKG.
9 § 33 Satz 1 NPsychKG.

Die Fachbereichsleitung des SpDi darf hingegen Einsicht in sämtliche Behandlungsakten nehmen, weil ihre besondere Expertise auch den erkrankten Personen zugutekommen muss.[10]

Fazit

Der SpDi mag binnenorganisatorisch wie ein herkömmliches Amt einer Kommune wirken. Dennoch sind bei der Akteneinsicht andere Maßstäbe anzulegen: Die ärztliche Schweigepflicht des medizinischen Fachpersonals des SpDi überlagert die Verarbeitung von besonderen personenbezogenen Daten zu Aufsichtszwecken. Unsere Prüfung hat sicher die eine oder andere Kommune für diese Besonderheiten nochmals sensibilisiert.

10 Gemäß § 7 Ab. 2 NPsychKG muss der Leiter oder die Leiterin des Gesundheitsamtes eine besondere Fachausbildung haben oder auf besonderes Erfahrungswissen im Bereich der (Jugend-)Psychiatrie zurückgreifen können.

Mühsamer Weg zum rechtmäßigen Einsatz von Microsoft 365 G.5.4

Uns erreichen nach wie vor diverse Beratungsanfragen in Zusammenhang mit dem Einsatz von Software aus der Produktfamilie Microsoft 365. Aus datenschutzrechtlicher Sicht gibt es hier diverse Hürden, die vor dem datenschutzrechtlich unbedenklichen Einsatz der Software genommen werden müssen.

Unter unserer Federführung ist eine Handreichung von insgesamt sieben Datenschutzaufsichtsbehörden entstanden[1], die die Verantwortlichen dabei unterstützt, mit Microsoft eine Auftragsverarbeitungsvereinbarung abzuschließen, die den Anforderungen der Datenschutz-Grundverordnung (DSGVO)[2] entspricht. Eine solche Vereinbarung ist dann nötig, wenn personenbezogene Daten im Auftrag des Verantwortlichen durch einen Dritten verarbeitet werden.

Die Handreichung knüpft an die Problemfelder an, die die Datenschutzkonferenz in ihrem Abschlussbericht vom 2. November 2022 beschrieben hat.[3] Hierzu gehören insbesondere Themen wie der Umgang mit der Verarbeitung durch Microsoft zu eigenen Geschäftszwecken, die Konkretisierung des Inhalts der Auftragsverarbeitung und die Prüfung der Angemessenheit der implementierten technischen und organisatorischen Datenschutzmaßnahmen.

Darüber hinaus haben wir das Niedersächsische Ministerium für Inneres und Sport und den Niedersächsischen IT-Planungsrat im Hinblick auf die uns vorgelegte Rahmen-Datenschutzfolgenabschätzung (DSFA) zum Einsatz der Anwendung Microsoft Teams und bestimmter weiterer Anwendungen aus der Produktfamilie Microsoft 365 beraten. Im Ergebnis hat der niedersächsische IT-Planungsrat den Einsatz der Produkte insbesondere an die Anforderung geknüpft, dass dieser nur nach einer vorherigen individuellen Risikobetrachtung (DSFA-Bericht) in den einzelnen Behörden erfolgt

1 Gemäß Art. 28 Abs. 3 DSGVO.
2 Handreichung zur Auftragsverarbeitungsvereinbarung für Microsoft 365, https://lfd.niedersachsen.de/225721.html
3 Kurzlink zur Zusammenfassung des Berichts: https://t1p.de/dsk-ms (PDF).

und dass die in der Rahmen-DSFA aufgeführten risikominimierenden Maßnahmen umgesetzt werden.

Fazit

Es ist sicherlich nicht einfach, als Verantwortlicher die Anforderungen für die datenschutzkonforme Nutzung von Microsoft 365 umzusetzen. Es wäre deshalb wünschenswert, dass Microsoft seine Standardverträge nachbessert und es seinen Kunden somit erleichtert, ihrer Rechenschaftspflicht nachzukommen und die datenschutzrechtlichen Anforderungen an ein Auftragsverarbeitungsverhältnis zu erfüllen. Das Niedersächsische Ministerium für Inneres und Sport hat sich nach Beratung durch die Datenschutzbehörde auf den Weg gemacht, mit Microsoft über die vertragliche Ausgestaltung in diesem Sinne zu verhandeln. Der Prozess war im Berichtszeitraum allerdings noch nicht abgeschlossen.

Verantwortliche haben auch die Wahl, auf den Einsatz von Microsoft 365 zugunsten von Open-Source-Produkten zu verzichten.

Verantwortliche haben nach allen Abwägungen aber auch die Wahl, auf den Einsatz von Microsoft 365 zum Beispiel zugunsten von Open-Source-Produkten zu verzichten.

Datenschutzaufsicht unterstützt Digitalisierung der Verwaltung G.5.5

Im Rahmen der Verwaltungsdigitalisierung müssen öffentliche Stellen den Datenschutz von vornherein mitdenken. Immer mehr Verantwortliche aus der niedersächsischen Landes- und Kommunalverwaltung wenden sich daher an uns mit der Bitte, sie bei Projekten zu beraten.

Die Bandbreite der von uns im Jahr 2023 bearbeiteten Beratungsanfragen reicht von Rechtsgrundlagen bei der Verarbeitung von Online-Anfragen einer Kommune über die datenschutzrechtlichen Verantwortlichkeiten im Rahmen der bundesweiten Umsetzung des Onlinezugangsgesetzes (OZG) bis hin zur Einschätzung der Rechtslage nach dem in 2024 erwarteten OZG-Änderungsgesetz.[1]

Die begleitenden Beratungsleistungen unterstützen dabei nicht nur die anfragenden Stellen, sondern gewähren auch uns einen wertvollen Einblick in die praktische Seite der OZG-Umsetzung in Niedersachsen.

Wer ist für was verantwortlich?

Weil beim OZG das „Einer-für-Alle"-Prinzip[2] gilt, sind in der Regel mehrere Stellen daran beteiligt, eine Verwaltungsleistung online bereitzustellen. Das ist den Bürgerinnen und Bürgern in vielen Fällen gar nicht ersichtlich, wenn sie einen Antrag elektronisch stellen.

Dabei erhebt eine öffentliche Stelle die Antragsdaten der Bürgerinnen und Bürger mithilfe eines Online-Antragsformulars und leitet diese zur Bearbeitung an die fachlich zuständige Stelle weiter. Im Rahmen unserer Beratung im Jahr 2023 waren insbesondere die datenschutzrechtlichen Rollen der Beteiligten zu beurteilen und einzuordnen. Wir kamen dabei in der Regel zum Ergebnis, dass diejenige Stelle, die den Onlinedienst betreibt und damit lediglich für die Erhebung und Weiterleitung der personenbezogenen

1 Siehe auch das Kapitel I.9 zum OZG-Änderungsgesetz.
2 Siehe hierzu auch Tätigkeitsbericht 2022, G.2.

Antragsdaten verantwortlich ist, als Auftragsverarbeiter handelt.[3] Die für einen Antrag fachlich zuständige Stelle handelt in den uns vorgelegten Fällen als Verantwortlicher.[4] In einigen Fällen kamen noch Unterauftragsverarbeiter hinzu, die den Auftragsverarbeiter bei der technischen Umsetzung unterstützten. Allein diese Auflistung macht deutlich, wie komplex die gegenseitigen (datenschutzrechtlichen) Bezüge zueinander häufig sind.

Nach dem aktuellen Entwurf des OZG-Änderungsgesetzes[5] wird sich die datenschutzrechtliche Rolle der Behörde, die einen Onlinedienst betreibt, ändern. Ihr wird die datenschutzrechtliche Verantwortlichkeit kraft Gesetzes zugewiesen, was zum einen ein hohes Maß an Rechtssicherheit schafft.[6]

Auf diese Änderung müssen sich andererseits die potenziell betroffenen Stellen einstellen, denn die datenschutzrechtliche Verantwortlichkeit bringt auch weitere Pflichten mit sich. Beispielsweise treffen den Verantwortlichen Informationspflichten[7] gemäß der Datenschutz-Grundverordnung, ferner können ihm gegenüber Betroffenenrechte[8] ausgeübt werden. Auch etwaige Datenpannen sind vom Verantwortlichen zu melden.[9]

Für die neu hinzukommenden Pflichten sind beim Verantwortlichen entsprechende Prozesse vorzusehen. In vielen Fällen muss er außerdem eine Datenschutzfolgenabschätzung erstellen.[10]

In einigen uns vorgelegten Fällen waren ferner bereits an der Entwicklung des Onlinedienstes mehrere Stellen beteiligt. Diese Stellen legten zum Beispiel die Funktionen fest, die ein Onlinedienst enthalten sollte. Auch insoweit stellte sich die Frage, ob eine solche Zusammenarbeit zu einer gemeinsamen Verantwortlichkeit der beteiligten Stellen führt. In den uns vorgelegten Fällen konnten wir das verneinen. Die Zusammenarbeit verschiedener Beteiligter bei der Definition der funktionalen Anforderungen führte noch nicht zu einer gemeinsamen Festlegung der Zwecke und der Mittel der Verarbeitung.[11] Insbesondere hatten die während der Entwick-

3 Art. 4 Abs. 8 DSGVO.
4 Art. 4 Abs. 7 DSGVO.
5 Stand 23.8.2023, BT-Drs. 20/8090.
6 Siehe auch Kapitel I.9 zum OZG-Änderungsgesetz.
7 Art. 12 ff. DSGVO.
8 Art. 15 ff. DSGVO.
9 Art. 33 und 34 DSGVO.
10 Art. 35 DSGVO.
11 Art. 4 Abs. 7 und Art. 26 DSGVO.

lung beteiligten Stellen in unseren Fällen nicht entschieden, ob und für wessen konkrete Anträge der Dienst später verwendet werden sollte. Diese Entscheidung traf die Fachbehörde, die den Dienst einsetzte.

Fazit

Es lohnt sich, den Datenschutz bereits zu Beginn der Digitalisierungsprojekte mitzudenken.

Es lohnt sich, den Datenschutz bereits zu Beginn der Digitalisierungsprojekte mitzudenken. Dadurch vermeiden öffentliche Stellen, mitten in der Entwicklung eines Diensts oder im schlimmsten Fall sogar nach Abschluss noch einmal mit viel Aufwand nachbessern zu müssen. Außerdem erleichtert es die Planung für die Verantwortlichen und stärkt das Vertrauen der Bürgerinnen und Bürger in einen modernen Staat.

Schule und Hochschule

G.6.1 Schulen müssen „nachsitzen“ – Vor-Ort-Prüfung an vier niedersächsischen Schulen

Im Anschluss an die 2022 durchgeführte schriftliche Prüfung hat die niedersächsische Datenschutzaufsicht im Sommer 2023 vier Schulen in Niedersachsen im Rahmen von Ortsterminen geprüft.

Wir wählten vier Schulen aus, die im schriftlichen Teil der Prüfung nur unterdurchschnittliche Ergebnisse erzielt haben. Vor Ort ermittelten wir, ob die Schulen Löschkonzepte vorhalten, ob insbesondere die durch Auflagen während der Corona-Pandemie entstandenen Daten (im Folgenden „Corona-Daten“ genannt) gelöscht wurden und wir überprüften die Datenverarbeitung in Klassenbüchern. Auf ein Sonderproblem stießen wir erst vor Ort: Grundschulen übermittelten weiterführenden Schulen im Einzelfall die gesamte Grundschulakte.

Löschkonzepte

Schulen dokumentieren in einem Löschkonzept, wer personenbezogene Daten von Schülerinnen und Schülern in welcher Form[1] nach Ablauf der Aufbewahrungsfrist löscht oder einem Kommunalarchiv anbietet. Das können zum Beispiel Lehrkräfte, das Sekretariat oder die Verwaltungsassistenz sein. Erforderlich ist auch, das Schularchiv zu strukturieren und Akten von Schülerinnen und Schülern regelmäßig um zu löschende personenbezogene Daten zu bereinigen.

1 Zur konkreten Form der Löschung enthält die DIN-Norm 66399 in den Teilen 1, 2 und 3 Hinweise.

Das Niedersächsische Kultusministerium (MK) legt in einem Runderlass[2] konkrete Aufbewahrungs- und Löschfristen fest. So sind zum Beispiel Entwürfe oder Zensurlisten zu Prüfungen 50 Jahre nach Ablauf des Schuljahres, in dem sie entstanden sind, zu löschen. Die Pflicht, vor endgültiger Löschung das Schriftgut einem Kommunalarchiv anzubieten, betrifft laut dem Runderlass nur die Archivschulen. Diese werden vom Niedersächsischen Landesarchiv im Einvernehmen mit den Kommunalarchiven bestimmt. Sofern eine Schule daher nicht als Archivschule benannt ist, sind die personenbezogenen Daten stets nach Ablauf der jeweiligen Aufbewahrungsfrist zu löschen.

Alle überprüften allgemeinbildenden Schulen hatten Nachholbedarf hinsichtlich der technischen und organisatorischen Umsetzung von Löschpflichten. Wir erteilten Hinweise vor Ort und stimmten im Gespräch mit den Regionalen Landesämtern für Schule und Bildung (RLSB) ein Muster für Löschkonzepte ab. Das Löschkonzept der überprüften Berufsbildenden Schule war hingegen weitgehend frei von Mängeln.

Löschung von Corona-Daten

An den niedersächsischen Schulen galten während der Covid-19-Pandemie Zutrittsbeschränkungen, die zwischenzeitlich weggefallen sind. Die Schülerinnen und Schüler mussten sich mehrfach in der Woche auf eine Infektion mit dem Covid-19-Virus testen.[3] Das Testergebnis war im Anschluss der Schule vorzulegen. Alternativ konnten die Schülerinnen und Schüler sich impfen lassen. Der Nachweis über die Auffrischungsimpfung konnte auf Basis der Einwilligung der Lernenden gespeichert werden. Das gleiche Prinzip galt für Befreiungen von der Maskenpflicht und für Genesenennachweise.

Die überprüften Schulen berichteten, dass diese Corona-Daten zeitnah gelöscht oder gar nicht erst zur Akte genommen wurden. In der von uns gezogenen Stichprobe fanden wir nur vereinzelt Covid-19-Testergebnisse, was wir vor Ort rügten. Im Übrigen wurden Impf- und Genesenennachwei-

2 RdErl. d. MK v. 29. Mai 2020 – 15-05410/1.2 (Nds. MBl. Nr. 32/2020 S. 696; SVBl. 8/2020 S. 351) – VORIS 22560.

3 Hierzu und zum Folgenden: § 16 Abs. 3 der Niedersächsische Verordnung über Schutzmaßnahmen zur Eindämmung des Corona-Virus SARS-CoV-2 und dessen Varianten vom 23. Februar 2022.

se sowie Maskenbefreiungsatteste ordnungsgemäß vernichtet. Insgesamt waren alle geprüften Schulen in Bezug auf diese zu löschenden Corona-Daten gut aufgestellt.

Klassenbücher

Die Klassenbücher wurden überwiegend korrekt geführt, gepflegt und aufbewahrt. Klassenbücher dürfen nur die unbedingt erforderlichen Schülerdaten wie Vor- und Nachname, Geburtsdatum oder Vermerke über versäumte Unterrichtsstunden enthalten. Vereinzelt enthielten Klassenbücher Entschuldigungsschreiben, was wir vor Ort beanstandeten.

Die überprüften Schulen bewahren Klassenbücher rechtskonform in Räumen auf, die für die Schülerinnen und Schüler nicht zugänglich sind oder die durchgängig von Lehr- oder Verwaltungskräften beaufsichtigt werden. Ein Klassenbuchdienst durch Schülerinnen und Schülern ist datenschutzrechtlich unbedenklich möglich. Die betreffenden Schülerinnen und Schüler müssen vorab altersgerecht über die Zwecke der Führung des Klassenbuches und dessen Schutzbedürftigkeit gegenüber der unbefugten Einsichtnahme von Dritten aufgeklärt werden.

Übermittlung von der Grundschule an weiterführende Schulen

Die Grundschulen dürfen nicht die gesamten Grundschulakten von Schülerinnen und Schülern an die weiterführenden Schulen übermitteln.[4] Diesen eigentlich bekannten Grundsatz hielten die Schulen teilweise nicht ein.

Grundschulen dürfen nicht die gesamten Grundschulakten an weiterführende Schulen übermitteln.

Die Weitergabe ist offenbar auch überhaupt nicht notwendig: Die Schulleitungen der betreffenden weiterführenden Schule berichteten, man sei auf die darin enthaltenden Informationen gar nicht angewiesen. Auch Informationen über die Schullaufbahn seien nicht erforderlich. Diese Erkenntnisse ließen uns die gesamte Praxis der Übermittlung von personenbezogenen Daten von einer Grundschule an weiterführende Schulen hinterfragen.

4 Vgl. auch die Informationen der RLSB in diesem Kontext, Kurzlink: https://t1p.de/schulakten

Wir diskutierten mit den RLSB, welche personenbezogenen Daten notwendig sind, um der weiterführenden Schule eine möglichst effiziente und effektive Beschulung zu ermöglichen. Das Niedersächsische Schulgesetz ist an dieser Stelle wenig bestimmt. Es dürfen Daten übermittelt werden, die zur Erfüllung des Bildungsauftrags „erforderlich" sind. Schulen müssen die Gründe darlegen, warum sie welche personenbezogenen Daten von Schülerinnen und Schülern zur Erfüllung des Bildungsauftrages benötigen. Nicht erforderlich ist jedenfalls die Übermittlung von Informationen über schulordnungsrechtliche Maßnahmen der Grundschule (Erziehungsmittel, Ordnungsmaßnahmen).

Hingegen ließen wir uns von den RLSB überzeugen, dass die weiterführende Schule mehr benötigt als Schülerstammdaten (Name, Vorname, Adresse, Geburtsdatum). Der Begriff der individuellen Lernentwicklung muss aber im konkreten Einzelfall mit Leben gefüllt werden. Ganz grundsätzlich müssen Grundschulen vor dem Übergang eines Schülers oder einer Schülerin auf eine weiterführende Schule einzelfallbezogen prüfen, welche Informationen aus der Dokumentation der individuellen Lernentwicklung eine weiterführende Schule konkret benötigt, um ihrem Bildungsauftrag nachzukommen.

Fazit

Die Mängel der vor Ort geprüften Schulen wurden abgestellt. Im direkten Gespräch erfuhren wir Hintergründe und Nöte von Schulleitungen, die unter anderem auf fehlendes Personal verwiesen. Da die datenschutzrechtlichen Herausforderungen zunehmen, aber der Grundbedarf an Datenschutzorganisation an Schulen nicht abgedeckt ist, benötigen Schulen von anderer Seite Unterstützung. Wir werden auch in Zukunft in diesem Bereich prüfen, um das Datenschutzniveau an Schulen zu verbessern.

G.6.2 Schweigepflichtentbindung durch „Nudging"-Methoden?

Eine niedersächsische Universität forderte Studierende auf, im Falle des krankheitsbedingten Prüfungsrücktritts Formulare zu nutzen, mit denen die behandelnde Ärztin oder der behandelnde Arzt von der Schweigepflicht entbunden wird. Die Universität hat dabei verkannt, dass die Entbindung von der ärztlichen Schweigepflicht nur auf Einwilligungsbasis erfolgen darf.

Uns erreichten zwei Beschwerden gegen eine niedersächsische Universität, in denen die Betroffenen Folgendes rügten: Die auf der Webseite der Hochschule zur Verfügung gestellten Formulare für den krankheitsbedingten Rücktritt von Prüfungen enthielten pauschal eine Erklärung, welche die behandelnde Ärztin oder den behandelnden Arzt von der ärztlichen Schweigepflicht entbindet. Die Universität suggerierte den Studierenden damit, dass sie diese Erklärungen abzugeben haben, um wirksam von der Prüfung zurücktreten zu können.

Diese Methode wird in der Verhaltensökonomik als „Nudging" (englisch für „Stupsen") bezeichnet.[1] Die Universität setzte den Entscheidungsrahmen auf der Webseite so, dass möglichst alle Studierenden die Formulare nutzen und die Schweigepflichtentbindungserklärungen abgeben.

Übliches Verfahren für Prüfungen

Das an den niedersächsischen Hochschulen übliche Verfahren für den krankheitsbedingten Rücktritt von Prüfungen gestaltet sich wie folgt: Studierende lassen sich von ihrer Ärztin oder ihrem Arzt in einem Formular die gesundheitlichen Einschränkungen attestieren, die zu der Prüfungsunfähigkeit führen. Eine Diagnose wird nicht preisgegeben. Auch wird die ärztliche Schweigepflicht nicht tangiert, da die Studierenden selbst entschei-

1 Vgl. Richter, Frederick, Nudging für mehr Datenschutz, PinG Ausgabe 06.19, S. 256.

den, ob sie das Attest dem Prüfungsausschuss vorlegen oder nicht. Dieses Verfahren wird seitens der höchstrichterlichen Rechtsprechung gebilligt.[2]

Die Einholung einer Schweigepflichtentbindungserklärung im Rahmen des Rücktritts von der Prüfung durch die Universität weicht erheblich von dem sonst üblichen Verfahren ab und bot somit Anlass für eine nähere rechtliche Überprüfung.

Anforderungen an wirksame Schweigepflichtentbindungserklärungen

Bei der Arzt-Patienten-Beziehung handelt es sich um ein besonders geschütztes Vertrauensverhältnis. Dieses darf durch einen faktischen Zwang zur Preisgabe von Gesundheitsdaten nur in explizit geregelten Fällen tangiert werden. Im Übrigen bedarf die Entbindung einer Ärztin oder eines Arztes von der Schweigepflicht einer auf Freiwilligkeit beruhenden Erklärung durch die betroffene Person. Diese Freiwilligkeit setzt außer einer transparenten Information über die Folgen der Erklärung auch eine echte Handlungsalternative voraus. Insbesondere ist zu vermeiden, dass die Betroffenen einem faktischen Zwang zur Abgabe der Erklärung ausgesetzt werden.

Bei der Arzt-Patient-Beziehung handelt es sich um ein besonders geschütztes Vertrauensverhältnis.

Die Beschwerden haben uns veranlasst, die Universität zur Stellungnahme aufzufordern. Die Hochschule hat erläutert, dass es sich nicht um verpflichtende Formulare, sondern um Musterformulare handele und die Studierenden die Prüfungsunfähigkeit auch auf die sonst übliche Weise nachweisen können.

Sie hat zugleich eingeräumt, dass die Entscheidung des Prüfungsausschusses über die Wirksamkeit des Rücktritts von der Prüfung nicht von der Abgabe der Schweigepflichtentbindungserklärung abhängen dürfe. Für den Prüfungsausschuss seien die von der behandelnden Ärztin oder dem behandelnden Arzt attestierten Einschränkungen, die zur Prüfungsunfähigkeit führen, maßgeblich für die Entscheidung über die Wirksamkeit des Prüfungsrücktritts.

2 Regelung über das qualifizierte ärztliche Attest: Bundesverwaltungsgericht, Beschlüsse vom 6. August 1996, Az. 6 B 17/96, und vom 14. Juli 2004, Az. 6 B 30/04.

Sofern der Prüfungsausschuss anhand der vorliegenden Informationen jedoch keine Entscheidung treffen könne, sieht die Hochschule einen Vorteil in der Schweigepflichtentbindungserklärung. Dann sei es dem Prüfungsausschuss möglich, die fehlenden Informationen selbst bei der Ärztin oder dem Arzt einzuholen. Die weitere Kommunikation mit dem Prüfling entfalle und der Prüfungsausschuss könne zügiger zu einem Ergebnis kommen.

Wir haben der Universität die rechtlichen Anforderungen an wirksame Schweigepflichtentbindungserklärungen erläutert. Daraufhin hat die Universität ihre Musterformulare für den Prüfungsrücktritt und die zugehörigen Datenschutzhinweise überarbeitet.

Der Fall Helmut Kentler: Verarbeitung von personenbezogenen Daten für die Sozialforschung G.6.3

Im Rahmen einer Beratungsanfrage berieten wir das Niedersächsische Landesamt für Soziales, Jugend und Familie, ob Akten zu einer Einrichtung der Kinder- und Jugendhilfe an eine Gruppe von Forschenden herausgegeben werden darf.

Der 2008 verstorbene Helmut Kentler vertrat die These, dass eine gleichberechtigte sexuelle Beziehung zwischen einem Kind und einem Erwachsenen nicht schädlich, sondern eher positiv für die Persönlichkeitsentwicklung des Kindes sein könne.[1] Er vermittelte zudem Kinder und Jugendliche an Einrichtungen, die von vorbestraften Pädophilen geleitet wurden.[2] Eine Gruppe von Forschenden fand heraus, dass Helmut Kentler in Niedersachsen eine Organisation gegründet hatte, der das Landesamt für Soziales, Jugend und Familie (LaSo) seinerzeit erlaubte, Kinder und Jugendliche zu betreuen. Außer Sachinformationen enthielt die Betriebserlaubnisakte auch Informationen über Beschäftige des LaSo, der Einrichtung sowie über die betreuten Kinder und Jugendliche.

Das Recht auf informationelle Selbstbestimmung und die Forschungsfreiheit

Die Forschungsfreiheit und das Recht auf informationelle Selbstbestimmung sind Freiheitsgrundrechte. Die Datenschutz-Grundverordnung (DSGVO) sieht an vielfältigen Stellen eine Privilegierung der Nutzung von Daten zu Forschungszwecken vor. So wird das Verarbeiten von Daten zu Forschungszwecken mit dem ursprünglichen Zweck einer Datenverarbeitung für vereinbar erklärt.[3] Zudem bestehen Grenzen für Betroffenenrechte,

1 Vgl. Die Zeit, Der Schatten von 1968, Ausgabe Nr. 42/1996.
2 Vgl. Focus Online, Kentler-Experiment: Pflegekinder wurden jahrzehntelang an Pädophile vermittelt, Kurzlink: https://t1p.de/kentler
3 Art. 5 Abs. 1 Buchst. b Hs. 2 DSGVO.

die im Einklang mit der Forschungsfreiheit ausgelegt werden.[4] Allerdings benötigen auch Forschende für die Datenverarbeitung zu Forschungszwecken eine Rechtsgrundlage. Dies kann einerseits eine Einwilligung der betroffenen Personen sein oder Forschende müssen von Gesetzes wegen eine Interessenabwägung durchführen. Im Rahmen der Interessenabwägung ist zu dokumentieren, dass die Forschungsinteressen höher zu bewerten sind als das Recht auf informationelle Selbstbestimmung der betroffenen Personen.

Die Vielfalt möglicher Rechtsgrundlagen

Die maßgeblichen Rechtsgrundlagen für Forschende sind im Bundesrecht, aber auch im Landesrecht der 16 Bundesländer enthalten. Dies betraf auch die Arbeit der Forschenden im vorliegenden Fall. Die Forschenden fragten einige Jahre zuvor bereits die Berliner Senatsverwaltung für Bildung, Jugend und Familie, ob sie Akten zu Betriebserlaubnisverfahren von Einrichtungen in Berlin zu Forschungszwecken erhalten dürfe. Indes gelten in Berlin andere Vorschriften als in Niedersachsen, sodass das bestehende Datenschutzkonzept der Forschenden nicht eins zu eins auf Niedersachsen übertragen werden konnte.

Die Vielfalt personenbezogener Daten in einer Betriebserlaubnisakte

Eine Betriebserlaubnisakte enthält nicht nur Sachinformationen, sondern auch verschiedene personenbezogene Informationen. Um die einschlägigen Rechtsgrundlagen zu ermitteln, war zu prüfen, zu welchen Zwecken die personenbezogenen Daten in der Betriebserlaubnisakte gespeichert sind.

Dabei war wie folgt zu differenzieren: Die personenbezogenen Informationen des Personals der Einrichtung unterfielen ursprünglich dem Beschäftigtendatenschutz, weil die Einrichtung die Informationen als Arbeitgeber des Personals verarbeitete. Diese Beschäftigtendaten werden durch Übermittlung an das LaSo zu Sozialdaten, weil dieses mit Durchführung des Betriebserlaubnisverfahrens eine Aufgabe nach dem Sozialgesetzbuch

4 Art. 89 Abs. 2 DSGVO i. V. m. § 13 Abs. 5 NDSG (für öffentliche Stellen), Art. 89 Abs. 2 DSGVO i. V. m. § 27 Abs. 2 BDSG (für private Stellen).

wahrnimmt. Für die Verarbeitung von Sozialdaten gelten die besonderen Regelungen des Sozialgesetzbuchs, die die allgemeinen datenschutzrechtlichen Regelungen verdrängen. Statt der Interessenabwägungsklausel des allgemeinen Datenschutzrechts war im Hinblick auf die Sozialdaten § 75 des Sozialgesetzbuchs X (SGB X) anwendbar. Nach dieser Vorschrift benötigt das LaSo (grundsätzlich) eine Einwilligung der Beschäftigten der Einrichtung, um deren personenbezogene Informationen an Forschende übermitteln zu dürfen.

Ausnahmsweise ist keine Einwilligung notwendig, wenn zum Beispiel die Ermittlung des unbekannten Aufenthaltsorts ehemaliger Sachbearbeiterinnen und Sachbearbeiter einen erheblichen Verwaltungsaufwand verursachen würde.[5] Ob dies der Fall ist, war vom LaSo in eigener Verantwortung zu beurteilen. An die Stelle der Einwilligung tritt dann eine Interessenabwägung.[6] Das Datenschutzkonzept der Forschenden musste angepasst werden, weil die Forschenden fälschlicherweise von einer Anwendung des allgemeinen Datenschutzrechts ausgingen.

Die personenbezogenen Daten des (ehemaligen) Personals des LaSo beziehen sich einerseits auf das Beschäftigungsverhältnis zwischen dem LaSo und den Beschäftigten. Andererseits sind es aus Sicht der Forschenden auch Informationen „über" das Betriebserlaubnisverfahren. Wir sind zum Ergebnis gekommen, dass der Schwerpunkt der Verarbeitung darin liegt, diese Informationen als Beschäftigtendaten an die Forscher zu übermitteln. Denn maßgeblich ist im Fall des ersten Schrittes der Verarbeitungskette – die Übermittlung der Daten – nicht die Sicht der Forschenden, sondern die Sicht des LaSo. Das LaSo trägt aber als Dienstherr die Verantwortung für die Verarbeitung von Beschäftigtendaten. Erst im zweiten Schritt, nämlich in den Händen der Forschenden, werden die Beschäftigtendaten zu Forschungsdaten.

Damit musste die Interessenabwägungsklausel des Niedersächsischen Datenschutzgesetzes (NDSG) angewendet werden.[7] Danach dürfen öffentliche Stellen unter anderem personenbezogene Daten an andere Stellen

5 § 75 Abs. 1 S. 2 Sozialgesetzbuch – Zehntes Buch (SGB X): „Eine Übermittlung ohne Einwilligung der betroffenen Person ist nicht zulässig, soweit es zumutbar ist, ihre Einwilligung einzuholen."

6 § 75 Abs. 1 S. 1 Sozialgesetzbuch – Zehntes Buch (SGB X).

7 § 88 Absatz 1 Satz 1 Variante 3, Satz 2 NBG in Verbindung mit § 13 Absatz 1 Satz 1 NDSG.

zur wissenschaftlichen oder historischen Forschung übermitteln, wenn die Art und Verarbeitung der Daten darauf schließen lassen, dass ein schutzwürdiges Interesse der betroffenen Person der Verarbeitung der Daten für das Forschungsvorhaben nicht entgegensteht oder das öffentliche Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse der betroffenen Person überwiegt. Das LaSo ist eine öffentliche Stelle und musste die Interessenabwägung in eigener Verantwortung vornehmen und dokumentieren.

Die Akte des Betriebserlaubnisverfahrens einer Einrichtung könnte auch personenbezogene Daten von Dritten enthalten. Im Datenschutzkonzept der Forschenden wurden diese Dritten als „Privatpersonen" bezeichnet. Sofern Kinder und Jugendliche betroffen sind, sind deren personenbezogene Daten als Sozialdaten einzuordnen. Die Unterbringung und Betreuung von Kindern und Jugendlichen sind Leistungen nach dem Sozialgesetzbuch. Deren Daten an Forschende zu übermitteln ist daher grundsätzlich nur auf Einwilligungsbasis möglich.[8]

Empfehlung

Im vorliegenden Fall mussten die Forschenden ihr bestehendes „Berliner Datenschutzkonzept" an die Rechtslage in Niedersachsen anpassen. Das Forschungsvorhaben konnte gleichwohl auch in Niedersachsen durchgeführt werden, da die landesrechtlichen Regelungen nicht wesentlich voneinander abweichen.

Divergierendes Landes- oder Bundesrecht kann bei übergreifenden Forschungsvorhaben zu rechtlichen Unsicherheiten führen. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder empfiehlt daher, die Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten für Forschungszwecke zu vereinheitlichen.[9]

8 § 75 Sozialgesetzbuch – Zehntes Buch (SGB X).

9 Siehe dazu Kapitel I.7 und DSK-Entschließung, Datenschutz in der Forschung durch einheitliche Maßstäbe stärken, November 2023, Kurzlink: https://t1p.de/dsk-forschung (PDF).

Datenschutzrechtliche Verantwortlichkeit beim Einsatz von Dienstleistern in Hochschulen G.6.4

Die Datenschutz-Grundverordnung sieht unterschiedliche Konstellationen der Verantwortlichkeit vor. Da Hochschulen beim Umgang mit personenbezogenen Daten zunehmend mit Externen zusammenarbeiten, ist auf den ersten Blick nicht immer leicht zu erkennen, wer als Verantwortlicher anzusehen ist.

Uns erreichen jedes Jahr einige Eingaben aus dem Hochschulbereich. Beim Einsatz externer Dienstleister prüfen wir oftmals, wer überhaupt Verantwortlicher im Sinne der Datenschutz-Grundverordnung (DSGVO)[1] ist. Sofern ein Dienstleister personenbezogene Daten verarbeitet, kommt grundsätzlich eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit der Hochschule und des Dienstleisters in Betracht.

Auftragsverarbeitung

Eine Beschwerde betraf ein unrichtiges Datum in dem Informations- und Bewerberportal der Stiftung für Hochschulzulassung. Über dieses Portal können Bewerbungs- und Vergabeverfahren für Studiengänge digital abgebildet werden. Im Rahmen des Bewerbungsprozesses für einen Studiengang wurde das Datum zur Einschreibung einer Person versehentlich mit „eingeschrieben" gespeichert, obwohl diese Person nicht für das Studium zugelassen wurde.

Die Stiftung sowie die Hochschule haben der betroffenen Person unterschiedliche Antworten auf die Frage gegeben, wer die verantwortliche Stelle nach der DSGVO ist. Die zutreffende Beantwortung dieser Frage ist bedeutsam, da der Verantwortliche insbesondere die Korrektur des unrichtigen Datums vornehmen muss.

1 Definition der Verantwortlichkeit siehe Art. 4 Abs. 7 DSGVO. Zur Auftragsverarbeitung siehe Art. 28 DSGVO. Zu gemeinsamen Verantwortlichen siehe Art. 26 DSGVO.

Unsere datenschutzrechtliche Prüfung hat ergeben, dass zwischen den Hochschulen und der Stiftung ein Auftragsverarbeitungsverhältnis besteht. Die Stiftung betreibt im Auftrag der Hochschulen das Portal und verarbeitet die dafür erforderlichen personenbezogenen Daten der Studienbewerberinnen und -bewerber. Die Hochschulen legen jedoch fest, welche Daten hierfür erforderlich sind. Datenschutzrechtlich verantwortliche Stelle für die Einhaltung der datenschutzrechtlichen Vorschriften im Rahmen des Portals ist somit die jeweilige Hochschule.

Gemeinsame Verantwortliche

Im Rahmen zweier Datenpannen haben wir Kenntnis davon erlangt, dass zwei niedersächsische Hochschulen ein Kurssystem nutzen, das über einen Plattformanbieter einer Hochschule eines anderen Bundeslands angeboten wird. Die niedersächsischen Hochschulen übermittelten personenbezogene Daten der Studierenden zu deren Identifikation und Zugangsberechtigung an die andere Hochschule, die das Kurssystem anbietet.

In diesem Fall sind die jeweilige Hochschule, die das Kurssystem nutzt, und die andere Hochschule, die das Kurssystem anbietet, gemeinsame Verantwortliche.[2] Sie verfolgen mit der Ausbildung der Studierenden einen gemeinsamen Zweck und beeinflussen gemeinsam auch die eingesetzten technischen und organisatorischen Maßnahmen der Datenverarbeitung, indem sie den Studierenden Kursinhalte über eine gemeinsam genutzte Plattform zugänglich machen.

Die DSGVO verpflichtet in diesem Fall dazu, eine Vereinbarung über die gemeinsame Verantwortlichkeit zu schließen, in der transparent festgelegt werden muss, welche Stelle welche Verpflichtungen nach der DSGVO erfüllt.[3] Da diese Vereinbarung nicht vorlag, haben wir die Hochschulen auf die Pflicht zum Abschluss dieser Vereinbarung hingewiesen.

Keine eigene Verantwortlichkeit der Hochschule

Eine weitere Meldung einer Datenpanne führte zu der Betrachtung der Verantwortlichkeit zwischen einer Hochschule und einem Anbieter von In-

2 Art. 26 Abs. 1 Satz 1 DSGVO.
3 Art. 26 Abs. 1 Satz 2 DSGVO.

formationen in Form von Statistiken. Die Hochschule stellte den Studierenden das Angebot des externen Anbieters zur Verfügung. Dieses Unternehmen hat für das Nutzen seines Angebotes personenbezogene Daten der Studierenden verarbeitet. Die Hochschule hat jedoch keine personenbezogenen Daten der Studierenden an das externe Unternehmen übermittelt. Die Studierenden haben ihre personenbezogenen Daten vielmehr selbst an das Unternehmen übermittelt. Somit ist nicht die Hochschule, sondern das externe Unternehmen für die Verarbeitung der Studierendendaten Verantwortlicher im Sinne der DSGVO. Die Pflichten für Verantwortliche nach der DSGVO treffen somit lediglich das externe Unternehmen, nicht jedoch die Hochschule.

Fazit

Diese drei Fälle verdeutlichen, dass die Einbindung externer Stellen im Hochschulbereich zu unterschiedlichen datenschutzrechtlichen Verantwortlichkeiten führen kann. Sofern externe Dienstleister eingesetzt werden, ist daher eine sofortige Prüfung der datenschutzrechtlichen Verantwortlichkeit angeraten.

Die Einbindung externer Stellen kann zu unterschiedlichen datenschutzrechtlichen Verantwortlichkeiten führen.

Denn hiervon hängt insbesondere ab, welche Stelle, ob Hochschule oder Externer, welchen Verpflichtungen nach der DSGVO unterliegt. Dies betrifft insbesondere die Pflichten der Erfüllung der Informationspflichten[4] und weiterer Betroffenenrechte[5], der Meldepflicht von Datenpannen[6], des Abschlusses einer Vereinbarung über die gemeinsame Verantwortlichkeit[7] und des Abschlusses eines Auftragsverarbeitungsvertrags.[8]

4 Art. 13 und 14 DSGVO.
5 Art. 15 bis 22 DSGVO.
6 Art. 33 DSGVO.
7 Art. 26 DSGVO.
8 Art. 28 DSGVO.

Polizei

G.7.1 Prüfung der Übermittlung personenbezogener Daten Minderjähriger an Europol

Zusammen mit anderen Datenschutzaufsichtsbehörden haben wir Verfahren deutscher Polizeibehörden geprüft, bei denen personenbezogene Daten Minderjähriger mit der Kennzeichnung „Verdächtige" oder „künftige potenzielle Straftäter" an Europol übermittelt wurden. Für eine unmittelbare Datenübermittlung an Europol seitens des Landeskriminalamts Niedersachsen fehlt derzeit eine Rechtsgrundlage.

Die Überprüfung erfolgte nach einer Anfrage des Europäischen Datenschutzbeauftragten, die sich an alle deutschen Datenschutzaufsichtsbehörden richtete. Für die niedersächsische Polizei haben wir dabei lediglich einen relevanten Datensatz festgestellt. Materiell-rechtlich war die Datenverarbeitung nicht zu beanstanden. Allerdings übermittelte das Landeskriminalamt (LKA) den Datensatz auf Grundlage einer Vereinbarung zwischen den Bundesländern und dem Bundeskriminalamt (BKA) unter Nutzung des Systems SIENA[1] unmittelbar an die Europol National Unit eines Mitgliedsstaats. Das ist problematisch, weil die hier einschlägige Regelung nach dem Niedersächsischen Polizei- und Ordnungsbehördengesetz (NPOG)[2] Datenübermittlungen an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen nur gestattet, soweit die Übermittlung „in einem Gesetz" geregelt ist.

1 SIENA steht für Secure Information Exchange Network Application.
2 § 43 Abs. 2 Nr. 1 NPOG.

Als mögliche Übermittlungsvorschriften kommen § 3 Absatz 3 Satz 2 Nummer 4 BKAG[3] und § 3 Absatz 1 Satz 1 EuropolG[4] in Betracht. Während jedoch letztere Vorschrift eine Datenübermittlung nur über das BKA erlaubt, genügt die Regelung des BKAG[5] nicht den Voraussetzungen des NPOG.[6] Die Bundesvorschrift enthält nämlich nicht die geforderte gesetzliche Regelung zur Datenübermittlung, sondern berechtigt lediglich zur Schaffung einer untergesetzlichen Regelung.

Ausblick

Um direkte Datenübermittlungen durch das LKA an Europol oder die Europol National Unit eines Mitgliedsstaats auf Grundlage des BKAG vornehmen zu können, müsste das NPOG Datenübermittlungen im Rahmen einer Regelung „aufgrund eines Gesetzes" erlauben.

Diese Rechtsauffassung teilten wir dem LKA mit und erhielten von dort die Rückmeldung, dass man unseren Ausführungen folge und die Problemstellung dem Niedersächsischen Ministerium für Inneres und Sport berichten werde. Seitens des LKA gehe man davon aus, dass der Gesetzgeber entsprechende Anpassungen umsetzen werde.

Fazit

Eine Übermittlung personenbezogener Daten an Europol ist derzeit lediglich über das BKA zulässig.

Eine rechtmäßige Übermittlung personenbezogener Daten an Europol ist derzeit lediglich über das BKA, nicht jedoch unmittelbar durch das LKA selbst zulässig. Hierfür wäre der Wortlaut der Regelung des § 43 Absatz 2 Nummer 1 NPOG entsprechend anzupassen.

Wir werden die Entwicklungen hierzu weiter beobachten und das Thema in unserem nächsten Tätigkeitsbericht erneut aufgreifen.

3 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten.

4 Gesetz zur Anwendung der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates.

5 § 3 Abs. 3 S. 2 Nr. 4 BKAG.

6 § 43 Abs. 2 Nr. 1 NPOG.

G.7.2 Falschparker berufen sich auf Datenschutz

Ist es datenschutzwidrig, einen Falschparker zu fotografieren, um diesen anzuzeigen? Datenschutz wird häufig als Täterschutz gebrandmarkt. Auch in diesem Fall stimmt das aber nicht.

Wer sich über Falschparker ärgert, greift schnell mal zum Smartphone, fotografiert das Fahrzeug und erstattet per E-Mail Anzeige. Das dauert nicht einmal fünf Minuten, und über Datenschutz macht sich in diesem Moment wahrscheinlich niemand Gedanken. Kann sich die Falschparkerin oder der Falschparker erfolgreich darauf berufen, dass es sich um einen Datenschutzverstoß handelt? Diese Frage war im Berichtszeitraum Gegenstand von mehreren Beschwerden und Anfragen.

Anwendbarkeit der DSGVO

Grundsätzlich ist beim Anfertigen der Fotografie für den Zweck der Anzeigeerstattung die Datenschutz-Grundverordnung (DSGVO) anwendbar. Beim Kennzeichen eines Fahrzeugs handelt es sich um ein personenbeziehbares Datum.[1] Die Erstatterin oder der Erstatter der Anzeige kann sich zudem nicht darauf berufen, die DSGVO sei nicht anwendbar, weil es sich um eine ausschließlich persönliche Tätigkeit handelt.[2] Um eine persönliche Tätigkeit handelt es sich nach der Rechtsprechung dann nicht, wenn die Verarbeitung, also das Aufnehmen eines Fotos, den öffentlichen Raum betrifft.[3] Wer im öffentlichen Raum geparkte Fahrzeuge mit dem Zweck der Weitergabe der Fotos fotografiert, bewegt sich daher außerhalb der eigenen persönlichen Sphäre.

Abwägung

Für das Fotografieren und die Anzeige bedarf es also einer Rechtsgrundlage.[4] Die Einwilligung stellt natürlich keine praktikable Möglichkeit dar und

1 VG Ansbach, Urteil vom 2.11.2022, Az. AN 14 K 22.00468.
2 Art. 2 Abs. 2 Buchst. c DSGVO.
3 EuGH, Urteil vom 11.12.2014, Az. C-212/13.
4 Art. 5 Abs. 1 Buchst. a DSGVO.

würde im Zweifelsfall auch nicht erteilt werden. In Betracht kommt daher nur die Interessenabwägung.[5] Die Verarbeitung ist danach zulässig, wenn die Verarbeitung einem legitimen Interesse dient, erforderlich ist und bei einer Abwägung die Grundrechte der betroffenen Personen nicht überwiegen.

Die Anzeige von Ordnungswidrigkeiten bei den dafür zuständigen Behörden stellt ein legitimes Interesse dar, welches von unserer Rechtsordnung anerkannt wird.[6] Dabei sollte jedoch darauf geachtet werden, den Behörden nicht Informationen zukommen zu lassen, die nicht erforderlich sind. Es sollte daher nach Möglichkeit vermieden werden, andere Kennzeichen oder Personen zu fotografieren. So kann die Anzahl der betroffenen Personen verringert werden.

Die Grundrechte der Falschparkerin oder des Falschparkers als betroffener Person überwiegen in diesen Fällen grundsätzlich auch nicht. Bei der Abwägung sind insbesondere die vernünftigen Erwartungen der betroffenen Personen zu berücksichtigen. Es wird im Wesentlichen das Nummernschild als personenbezogenes Datum fotografiert und übermittelt. Sinn und Zweck eines Fahrzeugkennzeichens ist es gerade, die Identifizierbarkeit im Straßenverkehr zu gewährleisten. Fahrzeughalter müssen daher damit rechnen, dass das Kennzeichen für eine Anzeige genutzt wird, wenn ihr Fahrzeug nicht ordnungsgemäß geparkt ist. Das Interesse, nicht für ein ordnungswidriges Verhalten belangt zu werden, ist überdies nur von geringem Gewicht.[7]

Fahrzeughalter müssen damit rechnen, dass das Kennzeichen für eine Anzeige genutzt wird, wenn ihr Fahrzeug nicht ordnungsgemäß geparkt ist.

Fazit

Wir haben entsprechende Beschwerden durch Personen, die wegen Falschparkens angezeigt worden waren, als unbegründet abgewiesen. Das Datenschutzrecht verhindert nicht, dass die Bürgerinnen und Bürger Falschparker fotografieren und Anzeige erstatten.

5 Art. 6 Abs. 1 Buchst. f DSGVO.
6 Vgl. Erwägungsgrund 50 Satz 9 DSGVO.
7 VG Ansbach, Urteil vom 2.11.2022, Az. AN 14 K 22.00468.

G.7.3 Telekommunikationsüberwachung: Kritikwürdiges Altverfahren läuft weiter

Die Polizei Niedersachsen kann zur Ermittlung von schweren Straftaten und zur Gefahrenabwehr auch Maßnahmen der Telekommunikationsüberwachung nutzen. Unsere Behörde berät das Land, wie es dabei einen möglichst hohen Schutz der Grundrechte seiner Bürgerinnen und Bürger aufrechterhält. Die Umsetzung unserer Forderungen verzögert sich weiter.

Maßnahmen der Telekommunikationsüberwachung (TKÜ)[1] sind für die polizeiliche Arbeit in bestimmten Aufklärungssituationen unabdingbar, allerdings aus verfassungsrechtlichen Gründen eng reglementiert. Das ist auch notwendig, denn sie sind ein Instrument, das mit erheblichen Eingriffen in die Rechte und Freiheiten der betroffenen Personen verbunden ist. Der Gesetzgeber hat folgerichtig hohe rechtliche Hürden für diese Grundrechtseingriffe gesetzt. Ein wesentlicher Teil dieses Regulierungsmechanismus ist auch das Datenschutzrecht, das Bestimmungen zu notwendigen technischen und organisatorischen Maßnahmen zum Schutz vor Verletzungen der Persönlichkeits- und Freiheitsrechte enthält.

Das seit 2016 geplante gemeinsame „Rechen- und Dienstleistungszentrum Telekommunikationsüberwachung der Polizei im Verbund der norddeutschen Küstenländer" (RDZ-TKÜ) verfolgt das Ziel, die komplexen rechtlichen und technischen Anforderungen sowie die Verfahrensschritte ökonomisch mit einem zentralen Verfahren umzusetzen. Beteiligt sind Bremen, Hamburg, Niedersachsen, Mecklenburg-Vorpommern und Schleswig-Holstein.

Altverfahren kritikwürdig – ablösendes Verfahren in Verzug

Der Aufbau und Betrieb für das neue Verfahren sind erneut erheblich in Verzug geraten. Das bereits im Jahr 2017 von unserer Behörde kritisierte

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

Altverfahren betreibt das Landeskriminalamt Niedersachsen daher faktisch solange weiter, bis das Nachfolgeverfahren der fünf Bundesländer im Produktivbetrieb starten und das Altverfahren ablösen kann.

Im November 2022 wurde unserer Behörde von der Projektleitung auf Nachfrage mitgeteilt, dass sich der ursprünglich für 2020 und zwischenzeitlich für den 10. Oktober 2022 vorgesehene Start des Wirkbetriebs erneut verzögern werde – nach unserem aktuellen Kenntnisstand inzwischen auf das 3. Quartal 2024.

Die fünf beteiligten Länder haben ihre Aufsichtsbehörden daraufhin im April 2023 zu einer weiteren Sachstandspräsentation eingeladen. Bei diesem und weiteren Terminen berieten wir mit dem Schwerpunkt zu methodischen Fragen der Datenschutz-Folgenabschätzung (DSFA) sowie um eine zielgerichtete Vorgehensweise und Dokumentation zu gewährleisten. Seither befindet sich die Projektgruppe in der Umsetzung dessen, was an Nachhol- und Anpassungsbedarf identifiziert worden war.

Das von unserer Behörde kritisierte Altverfahren betreibt das Landeskriminalamt faktisch weiter.

Die Risikobewertung und die DSFA verzögerten sich dadurch weiter. Die finale DSFA hat die Projektleitung den Aufsichtsbehörden nun im Frühjahr 2024 präsentiert. Wir werden beurteilen, ob allen relevanten Risiken durch wirksame und angemessene technisch-organisatorische Maßnahmen begegnet wird und diese so im erforderlichen Maß reduziert werden.

Justiz

G.8.1 Aufsichtsrechtliche Lücke – weiterhin keine besonderen Stellen im Justizsystem

In Fortsetzung zu den Beiträgen in den vorhergehenden Tätigkeitsberichten[1] besteht auch weiterhin eine aufsichtsrechtliche Lücke im Bereich der Justiz. Diese Lücke durch „besondere Stellen im Justizsystem"[2] zu schließen, ist in Deutschland derzeit nicht beabsichtigt.

Initiiert durch das Schreiben der Datenschutzkonferenz (DSK) an die Justizministerkonferenz (JuMiKo) hat sich die Zentralabteilungsleitertagung der Landesjustizverwaltungen mit der Thematik der besonderen Stellen im Justizsystem befasst. Diese kam zu dem Ergebnis, dass zurzeit aus Sicht der Länder kein Bedürfnis gesehen werde, besondere Stellen im Justizsystem einzurichten. Insbesondere bestehe bereits jetzt eine ausreichende Kontrolle durch die Instanzgerichte. Nach unserer Ansicht ist jedoch die Einrichtung dieser besonderen Stellen zur Durchsetzung der europarechtlichen Vorgaben zum Datenschutz zwingend geboten. Die Gerichte sind zwar zur Einhaltung dieser Regelungen vollumfänglich verpflichtet.[3] Es existiert jedoch für den Bereich der justiziellen Tätigkeit der Gerichte keine Aufsichtsbehörde. Unsere aufsichtsrechtliche Zuständigkeit ist (aus gutem Grund) für diesen Bereich ausgeschlossen.[4] Der rechtsstaatliche Grundsatz der Unabhängigkeit der Justiz soll unangetastet bleiben.

In der Folge bezweifelte die DSK in einem Antwortschreiben, ob mit einer Kontrolle durch die Instanzgerichte auf dem Rechtsweg die betreffende

1 Siehe Tätigkeitsbericht 2022, J.2.1.
2 Vorgesehen in Erwägungsgrund 20 der DSGVO.
3 Erwägungsgrund 20 der DSGVO.
4 Art. 55 Abs. 3 DSGVO.

Lücke in der Datenschutzsupervision und -beratung im Bereich der justiziellen Tätigkeit vollständig geschlossen werden kann. Es sei fraglich, ob damit alle Fragen und Anliegen der betroffenen Personen sowie der Gerichte selbst erfasst werden könnten. Zudem bestünden wesentliche Unterschiede zum Beschwerderecht nach der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG)[5] – insbesondere mit Blick auf die Kosten für die betroffenen Personen. Wir werden diese Bedenken auch im weiteren Austausch mit dem Niedersächsischen Justizministerium erneut thematisieren. Auf diesem Wege wollen wir noch einmal für die Thematik sensibilisieren, nicht zuletzt vor dem Hintergrund, dass das Land Niedersachsen ab Januar 2024 den Vorsitz der JuMiKo übernimmt.

Einsatz Künstlicher Intelligenz zur Richterassistenz

Dazu passt auch die Diskussion um eine KI-gestützte Richterassistenz in Niedersachsen.[6] Das Niedersächsische Justizministerium hat einen Auftrag für die Entwicklung einer solchen Richterassistenz erteilt. Das Assistenzsystem solle es ermöglichen, gleich gelagerte Verfahren effektiver zu bearbeiten. Dies beträfe insbesondere Massenverfahren, die die Justiz und die Gerichte seit Jahren belasten würden.

Aufgrund des Umstands, dass die Aufsichtsbefugnisse unserer Datenschutzbehörde für den Bereich der justiziellen Tätigkeit eingeschränkt sind, könnten wir das Justizministerium allenfalls dazu beraten. Die Überwachung und Durchsetzung der DSGVO obliegt der Justiz selbst. Allein anhand dieser Thematik wird deutlich, dass aufsichtsrechtliche Lücken im Justizbereich existieren, die sich nur mit der Einrichtung von besonderen Stellen für Datenschutzaufsicht und -vollzug schließen ließen.

5 Siehe Art. 77 DSGVO und § 60 BDSG.

6 Siehe auch Kapitel E und Pressemitteilung „Einsatz Künstlicher Intelligenz in der Justiz" des Niedersächsischen Justizministerium vom 22. Juni 2023, abrufbar unter https://www.mj.niedersachsen.de/223207.html

G.8.2 Bei Aufsicht über Staatsanwaltschaften keine Einigung in Sicht

Fragen zur aufsichtsrechtlichen Zuständigkeit gegenüber den Staatsanwaltschaften beschäftigen unsere Behörde schon seit einiger Zeit. In einem Fall mussten wir 2023 eine niedersächsische Staatsanwaltschaft förmlich zu einer Auskunft gegenüber der Datenschutzaufsicht verpflichten.

Im Tätigkeitsbericht 2022 berichteten[1] wir über eine Beanstandung, die wir gegenüber dem Niedersächsischen Justizministerium (MJ) betreffend eine Generalstaatsanwaltschaft (GenStA) aussprechen mussten. Dazu hat das MJ Anfang 2023 Stellung genommen.

In dem Fall hatte die GenStA eine richterliche Entscheidung in nicht anonymisierter Form an öffentliche Stellen in Niedersachsen übermittelt. Zugleich gab es dabei mit der GenStA große Unstimmigkeiten hinsichtlich unserer aufsichtsrechtlichen Zuständigkeit für bestimmte Tätigkeitsbereiche der Staatsanwaltschaften. Auf diesen ausführlich diskutierten Punkt ging das MJ in seiner abschließenden Stellungnahme jedoch nicht ein. Laut MJ habe es sich bei dem Vorfall um ein Versehen im Einzelfall gehandelt. Man habe die betreffenden Mitarbeiterinnen und Mitarbeiter im Hinblick auf die Datenschutzvorschriften nochmals sensibilisiert.

Auskunft einer Staatsanwaltschaft

In einem weiteren Fall erfolgte zwar anfangs ein Schriftwechsel mit einer Staatsanwaltschaft (StA), an dem sich auch die GenStA beteiligte. Fallbezogene Nachfragen, die dazu erforderlich waren, um unsere aufsichtliche Zuständigkeit[2] abschließend zu klären, beantwortete die betreffende StA jedoch nicht. Stattdessen teilte die GenStA – ohne auf unsere Fragen einzugehen – ihr Unverständnis mit. Zudem bat sie darum, dass sich unsere Dienststelle nicht mehr unmittelbar an die der GenStA nachgeordneten Staatsanwaltschaften wenden solle. Stattdessen solle in allen Angelegen-

1 Siehe Tätigkeitsbericht 2022, J.2.2. und Tätigkeitsbericht 2021, J.3.2.
2 Siehe § 57 Abs. 3 NDSG.

heiten betreffend die Staatsanwaltschaften die Kommunikation nur noch direkt über die GenStA erfolgen.

Das würde sich jedoch aus datenschutzrechtlicher Sicht als rechtswidrig darstellen. Denn wir haben uns als Aufsichtsbehörde regelmäßig zunächst an den Verantwortlichen selbst zu wenden.[3] Um uns nicht dem Vorwurf eines Verstoßes gegen den Grundsatz der Datenminimierung auszusetzen, leisten wir die Forderung der GenStA dementsprechend nicht Folge.

Zwischenergebnis

Da weder die StA noch die GenStA bislang unsere Fragen beantworteten, haben wir nunmehr gegenüber der StA formal eine sogenannte Auskunftsheranziehung verfügt, um deren Auskunftspflicht gegenüber unserem Haus durchzusetzen. Die Stellungnahme der StA hierzu stand zum Ende des Berichtszeitraums noch aus.

3 Vgl. § 57 Abs. 4 NDSG.

G.9 Datenschutz im Verein: Hoher Beratungsbedarf

Auch im Jahr 2023 haben wir viele Anfragen, Beschwerden und Pannenmeldungen aus den Vereinen in Niedersachsen erhalten. Sie reichen von Fragen zur Mitgliederverwaltung über Probleme nach Hacking-Angriffen bis hin zu vereinsinternen Streitigkeiten, die auf dem Feld des Datenschutzes ausgefochten werden.

Aus dem Vereinsumfeld erreichen uns hauptsächlich Schreiben zu allgemeinen Fragen des Datenschutzes, also zur Mitgliederverwaltung nebst Beitragserhebung und zur Öffentlichkeitsarbeit, aber auch Datenpannenmeldungen.[1] Vereine berichten uns in diesem Zusammenhang zum Beispiel vom Verlust eines Notebooks oder externen Datenträgern mit personenbezogenen Daten der Mitglieder.

Es wird sich aber auch darüber beschwert, wenn jemand aus dem Verein Unterlagen an einen falschen Adressaten verschickt oder E-Mail-Adressen offenlegt, weil er versehentlich einen offenen E-Mail-Verteiler verwendet hat. Die Vereine reagieren in diesen Fällen meist korrekt und fordern beispielsweise erfolgreich die Unterlagen zurück. Bei Verwendung offener Verteiler liegt zumindest in den uns bekannten Fällen selten ein Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) vor. Die Meldungen zeigen uns gleichwohl, dass das Datenschutzrecht für viele (noch) keine vertraute Materie ist und weiterhin Aufklärungs- beziehungsweise Beratungsbedarf besteht.

Hacking, Werbung, Löschfristen

Aufgefallen sind uns in diesem Jahr mehrere Schwerpunkte bei Beschwerden und Datenschutzpannen. Zum einen haben auch bei Vereinen seit Beginn des russischen Angriffs auf die Ukraine Hacking-Versuche zugenommen.

1 Gemäß Art. 33 DSGVO.

Außerdem meldeten uns Vereinsmitglieder Fälle, in denen ihre personenbezogenen Daten von anderen Mitgliedern, sogar von Funktionsträgern, zweckwidrig verwendet wurden. Meist versendete das Mitglied dann Werbung für eigene Angebote an die anderen Vereinsmitglieder. Dies ist im Regelfall unzulässig, denn für die Weitergabe der Mitgliederdaten ist von jedem Mitglied eine Einwilligung notwendig.

Ferner beschwerten sich ehemalige Vereinsmitglieder bei uns, dass ihre Daten nach ihrem Austritt aus dem Verein nicht sofort gelöscht wurden. Der Anspruch auf Datenlöschung ist im Regelfall nicht gegeben, der Verein hat die Daten aus steuerrechtlichen Gründen zehn Jahre aufzubewahren und sie lediglich aus dem aktiven Bestand zu nehmen.

Datenschutz bei Streitereien ins Feld geführt

Ebenfalls auffallend ist es, dass Mitglieder bei Streitigkeiten in einem Verein oder mit einem Verein versuchen, die Probleme mit Mitteln des Datenschutzrechts zu lösen beziehungsweise die Auseinandersetzung auf diesem Rechtsgebiet zu führen. Vielfach wird im Zuge eines Streits um eine Auskunft[2] nachgesucht und im Anschluss daran Beschwerde bei uns wegen fehlender Auskunft oder falscher Auskunft erhoben.

Vielfach wird im Zuge eines Streits um eine Auskunft nachgesucht und im Anschluss daran Beschwerde erhoben.

Das kostet alle Beteiligten viel Zeit und führt in der Regel zu nichts: Der Streit wird einfach nur in das Datenschutzrecht getragen, und selbst wenn dann die datenschutzrechtliche Fragestellung beantwortet oder gar gelöst ist, ist man einer Lösung des eigentlichen Konflikts keinen Schritt nähergekommen.

Hotline, Schulung und Tipps für Vereine

Die an uns herangetragenen Fälle unterstreichen, dass die von uns eingerichtete Vereinshotline auch im sechsten Jahr der Datenschutz-Grundverordnung weiterhin notwendig ist. Über diese Vereinshotline können Vereine sich unmittelbar an unsere Behörde mit datenschutzrechtlichen Fragen wenden und sie mit unseren Mitarbeiterinnen und Mitarbeitern erörtern.

2 Nach Art. 15 DSGVO.

Die Vereinshotline ist wöchentlich an drei Tagen besetzt, die Nachfrage ist ungebrochen.

Darüber hinaus bieten wir interessierten Vereinsmitgliedern die kostenlose Online-Schulung „Datenschutz im Verein" an. In der Schulung stellen Expertinnen und Experten die Grundzüge des Datenschutzrechts mit Fokus auf Vereine dar.

Aufgrund der hohen Nachfrage über die Vereinshotline hatten wir die Veranstaltung im Jahr 2022 konzipiert und eingeführt. Seitdem findet sie mehrmals im Jahr als abendliche Online-Veranstaltung statt, um ehrenamtlich Tätigen im Flächenland Niedersachsen unproblematisch die Teilnahme zu ermöglichen. Die Nachfrage und die Rückmeldungen in den Terminen haben uns darin bestärkt, die Schulung fortzuführen und sie auch im Jahr 2024 anzubieten. Aktuelle Termine finden Sie auf unserer Homepage.[3]

2023 haben wir darüber hinaus eine „Handreichung Datenschutz im Verein" auf unserer Homepage zum Download bereitgestellt.[4] Sie enthält die Grundzüge des Datenschutzes im Verein und ist eine hervorragende Ergänzung zur Online-Schulung.

3 Im Bereich LfD-Infoveranstaltungen, Kurzlink: https://t1p.de/ds-verein

4 Abrufbar unter https://lfd.niedersachsen.de/56043.html

Datenübermittlung in die USA: Neuer Angemessenheitsbeschluss G.10

Die Europäische Kommission hat am 10. Juli 2023 den Angemessenheitsbeschluss für den Datenschutzrahmen EU-USA angenommen. Eine Übermittlung personenbezogener Daten an zertifizierte Unternehmen und Organisationen in den USA ist nunmehr wieder ohne weitere Anforderungen möglich.

Auf Grundlage des neuen Durchführungsbeschlusses über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Data Privacy Framework (Datenschutzrahmen EU-USA) können Verantwortliche und Auftragsverarbeiter wieder personenbezogene Daten an zertifizierte Unternehmen und Organisationen in den USA übermitteln, ohne geeignete Garantien und zusätzliche Maßnahmen ergreifen oder sich auf spezielle Ausnahmetatbestände stützen zu müssen.

Mit Erlass des Angemessenheitsbeschlusses wird eine rund dreijährige Übergangsperiode mit besonderen Anforderungen an Datenübermittlungen in die USA beendet. Diese war entstanden, nachdem der Europäische Gerichtshof (EuGH) mit dem Schrems-II-Urteil vom 16. Juli 2020 den auf das Vorgängerabkommen „EU-US Privacy Shield" gestützten Durchführungsbeschluss für unwirksam erklärt hatte.

Ziele und Inhalte des neuen Datenschutzrahmens

Durch den neuen Datenschutzrahmen EU-USA soll insbesondere der Zugang der US-Nachrichtendienste zu Daten auf das notwendige und verhältnismäßige Maß beschränkt werden. Außerdem wurde ein zweistufiges Beschwerdeverfahren gegen US-Überwachungsmaßnahmen eingeführt. Dieses kann eine Überprüfung durch einen neu eingerichteten „Data Protection Review Court" beinhalten.

Der vom EU-US Privacy Shield bekannte Zertifizierungsmechanismus wird beibehalten. Das US-Handelsministerium hat eine Liste von US-Unterneh-

men veröffentlicht[1], die sich gegenüber dem Ministerium selbst zertifiziert und zur Einhaltung der Grundsätze des Datenschutzrahmens EU-USA verpflichtet haben.

Datenübermittlungen an US-Unternehmen, die nicht in der Liste zum Datenschutzrahmen EU-USA verzeichnet sind, können nicht auf den Angemessenheitsbeschluss gestützt werden. Solche Übermittlungen erfordern weiterhin gemäß der Datenschutz-Grundverordnung geeignete Garantien[2] (zum Beispiel Standardvertragsklauseln), den Rückgriff auf verbindliche interne Datenschutzvorschriften[3] (Binding Corporate Rules) oder das Vorliegen eines Ausnahmetatbestands im Einzelfall.[4]

Ausblick

Die EU-Kommission wird die Funktionsweise des Datenschutzrahmens EU-USA fortlaufend überprüfen. Die erste Überprüfung erfolgt ein Jahr nach Bekanntgabe des Angemessenheitsbeschlusses an die Mitgliedstaaten. Darüber hinaus ist zu erwarten, dass von Datenübermittlungen in die USA Betroffene erneut gerichtlichen Rechtsschutz suchen werden und auch der neue Datenschutzrahmen EU-USA perspektivisch vom EuGH überprüft werden wird.

Insofern kann aus Sicht der niedersächsischen Datenschutzaufsichtsbehörde noch keine abschließende langfristige „Entwarnung" für Datenübermittlungen in die USA gegeben werden. Nicht zuletzt vor diesem Hintergrund empfehlen wir, bereits eingeleitete oder umgesetzte Strategien zur digitalen Souveränität unbedingt weiterzuverfolgen. Sofern aber die Verarbeitung personenbezogener Daten ausschließlich im Europäischen Wirtschaftsraum erfolgt, haben Verantwortliche und Auftragsverarbeiter hierüber eine effektive Kontrolle und können die Einhaltung des Datenschutzniveaus langfristig und dauerhaft sicherstellen.

1 Abrufbar unter https://dataprivacyframework.gov/list
2 Art. 46 DSGVO.
3 Art. 47 DSGVO.
4 Art. 49 DSGVO.

H Abgeschlossene Bußgeldverfahren

Abgeschlossene Bußgeldverfahren

Im Jahr 2023 hat die niedersächsische Datenschutzaufsicht Geldbußen in Höhe von insgesamt rund 5,3 Millionen Euro verhängt. Die Gesamthöhe ist dabei überwiegend auf drei einzelne Verfahren zurückzuführen. Die Mehrzahl der 2023 verhängten Geldbußen betraf erneut Fälle unzulässiger Videoüberwachung.

Im Jahr 2023 hat unsere Behörde insgesamt 101 neue Fälle unter Gesichtspunkten einer möglichen Geldbuße geprüft. Im gleichen Zeitraum haben wir 51 Erstbescheide in Bußgeldsachen erlassen, die sich zum Teil auf Fälle bezogen, die wir bereits in den Vorjahren eingeleitet hatten. Von diesen Bescheiden sind 33 rechtskräftig geworden, da die Adressaten keinen Einspruch eingelegt oder einen eingelegten Einspruch vor Abgabe an das Gericht vollständig zurückgenommen haben. Die nicht mit Geldbußen abgeschlossenen Verfahren sind entweder noch nicht beendet, waren nicht bußgeldwürdig, wurden eingestellt oder wurden an andere zuständige Stellen abgegeben.

Im Jahr 2023 haben wir 51 Erstbescheide in Bußgeldsachen erlassen.

Mit Erstbescheiden haben wir Geldbußen in Höhe von rund 5,3 Mio. Euro festgesetzt.[1] Die Bescheide erließ unsere Behörde gegenüber Verantwortlichen aus den Bereichen Gastgewerbe, Industrie, Finanzdienstleistungen, Immobilienmakler, Fitnessstudios, Rechtsdienstleiser, sonstige Dienstleister sowie gegen natürliche Personen. Bei Bescheiden gegenüber natürlichen Personen ging es teilweise um Verstöße, die sie als Inhaber eines Unternehmens begangen hatten.

Geahndet wurden Verstöße gegen die Artikel 5, 6, 9, 13, 17, 25, 26, 28, 30, 31, 32, 35, 37 sowie 83 Absatz 5 Buchstabe e der Datenschutz-Grundverordnung (DSGVO) und § 26 des Bundesdatenschutzgesetzes (BDSG). Bei den Verstößen handelte es sich um die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage, um Verstöße gegen die Informations-, Auskunfts- und Löschpflicht, die Pflicht zur Beachtung von Widersprüchen

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).

gegen die Verarbeitung, den Nichtabschluss von Auftragsverarbeitungsverträgen, die Nichtführung beziehungsweise Nichtvorlage von Verzeichnissen der Verarbeitungstätigkeit, um unzureichende technische Maßnahmen, um das Fehlen einer Datenschutzfolgenabschätzung sowie um die Nichtbeachtung behördlicher Anweisungen.

Im Jahr 2023 wurden durch die Gerichte 14 Entscheidungen zu Bußgeldverfahren getroffen. Überwiegend haben die Bußgeldadressaten die Verstöße im Wege gerichtlicher Verständigungen[2] in der Sache eingeräumt und ihre Einsprüche auf die Rechtsfolgenseite, also die Höhe einer Geldbuße, beschränkt. Dadurch 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 2024 erwartet. Im Folgenden geben wir einen Überblick über besondere Fälle.

Profilbildung zu Werbezwecken mit Smart-Data-Verfahren

Einzelne Kreditinstitute bildeten mit vorhandenen personenbezogenen Daten aktiver Kundinnen und Kunden Profile zur werblichen Ansprache. Die Institute werteten Zahlungsdaten wie das im Vorjahr eingegangene Gehalt, Zahlungen per E-Payment und Grundkosten wie Energieversorgung, aus. Außerdem wurden Stammdaten wie Alter, Familienstand, Dauer der Kundenbeziehung sowie Angaben zum Wohnumfeld wie der Anteil der Erwerbstätigen und die Anzahl der PKW-Neuzulassungen im sogenannten Mikromarkt, mit zur Profilbildung ausgewertet.

Ziel der Institute war es, anhand der so gebildeten Profile diejenigen Kundinnen und Kunden zu identifizieren, die für spezifische Produktwerbung besonders zugänglich sein könnten. Solche Auswertungen der vorhandenen Bankdaten wie auch das Hinzuziehen weiterer Daten zu Werbezwecken war von den Kundinnen und Kunden vernünftigerweise nicht zu erwarten. Die Unternehmen konnten sich daher nicht auf berechtigte Interessen der Verantwortlichen[3] als Rechtsgrundlage stützen. In einem Ver-

2 Siehe auch Tätigkeitsbericht 2021 I.4.

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

fahren hat die Datenschutzaufsicht eine Geldbuße in Höhe von 220.000 Euro festgesetzt. Weitere Verfahren zur werblichen Profilbildung sind zum Ende des Berichtszeitraumes noch nicht abgeschlossen. Mehr zu dem Fall lesen Sie in Kapitel G.3.3.

Unzureichende Informationserteilung bei externen Compliance-Maßnahmen

Der LfD hat eine anlasslose Kontrolle eines durch externe Stellen durchgeführten Compliance-Audits bei einem Unternehmen abgeschlossen und bei einem Audit wegen der nach Ansicht des LfD unzureichenden Informationserteilung an die Beschäftigten nach einer von der Behörde angenommenen Zweckänderung eine Geldbuße in Höhe von 4,3 Millionen Euro festgesetzt. Das Unternehmen hat Einspruch gegen den Bußgeldbescheid eingelegt, sodass der Bescheid nicht rechtskräftig wurde. Bis zu einer rechtskräftigen Entscheidung gilt die Unschuldsvermutung. Einzelheiten zu diesem Fall finden Sie in Kapitel G.3.5.

Weitergabe besonderer Kategorien personenbezogener Daten

Eine Person versuchte, spezialisierte Beschäftigte ihres ehemaligen Arbeitgebers durch teilweise aggressive Kontaktaufnahmen abzuwerben. So schrieb sie Beschäftigte wiederkehrend elektronisch an oder hielt sie an ihrer Privatadresse auf, sodass sie verspätet zur Arbeit erschienen. Das ehemalige Unternehmen entschied sich, dem aktuellen Arbeitgeber einen Hinweis zu diesem Verhalten zu geben.

Dieser Hinweis enthielt aber zusätzlich besondere Kategorien von personenbezogenen Daten, da auch über Krankschreibungen und Krankenhausaufenthalte der Person informiert wurde. Eine Ausnahme für die Offenlegung dieser Daten gemäß DSGVO[4] lag nicht vor. Hierfür setzten wir gegen das verhältnismäßig kleine Unternehmen eine Geldbuße in Höhe von 9.600 Euro fest.

4 Art. 9 Abs. 2 DSGVO.

Unzureichende technisch-organisatorische Maßnahmen

Gegenüber einer Kette von Fitnessstudios verhängte unsere Behörde Geldbußen in Höhe von insgesamt 24.000 Euro wegen vier Vorwürfen. Etwa die Hälfte des Betrages entfiel auf verschiedene technisch-organisatorischer Mängel. So erfolgten unverschlüsselte Datensicherungen auf einem USB-Stick am Schlüsselbund des Geschäftsführers und in der Privatwohnung eines Beschäftigten. Weiterhin betrieben Studios lokale Backup-Systeme im selben Raum wie die Systeme für den Produktiveinsatz. Softwareseitig wurde über das erforderliche Maß hinaus mit Administratorrechten gearbeitet, es fehlte an einer Mandantentrennung und an einem Berechtigungskonzept. Ferner fehlte eine Dokumentation der Hard- und Software sowie der technisch-organisatorischen Maßnahmen. Hinzu kam, dass per Fernwartungssoftware jederzeit heimlich auf die PC-Arbeitsplätze der Beschäftigten zugegriffen werden konnte.

Zwei Unternehmen veröffentlichten Fotos jugendlicher Teilnehmerinnen und Teilnehmer von Fernreisen auf ihren Internetseiten und in sozialen Netzwerken.[5] Die vollständige Fotosammlung war auf den Internetseiten frei abrufbar. Im Rahmen unserer Prüfung hat das Unternehmen die wirksamen Einwilligungen in die Veröffentlichung nicht nachgewiesen. Zudem entsprach die uns vorgelegte Einwilligung nicht den gesetzlichen Anforderungen, da sie den Unternehmen erlaubte, die Fotos in beliebigen sozialen Netzwerken zu veröffentlichen. Vor dem Amtsgericht wiesen die Unternehmen für einige – aber nicht alle – abgebildeten Personen Einwilligungen nach, mussten sich für die Zuordnung der Einwilligungen jedoch der Hilfe Dritter bedienen. Im Beschlussverfahren erkannte das Amtsgericht im Benehmen mit der Behörde auf Geldbußen in Höhe von jeweils 3.000 Euro.

Immer wieder treten außerdem Fälle auf, in denen E-Mail-Newsletter unabsichtlich per offenem Verteiler versendet werden.[6] Auf diesem Wege erhalten die Empfänger zahlreiche E-Mail-Adressen anderer Personen, teilweise im Format Vorname.Nachname@Arbeitgeber.de, ohne dass für diese Offenlegung eine Rechtsgrundlage bestünde. Im Berichtsjahr wurde wegen eines offenen E-Mail-Verteilers mit rund 150 Adressaten gegenüber einem Verein eine Geldbuße in Höhe von 3.000 Euro festgesetzt. Statt

5 Vgl. Tätigkeitsbericht 2019 J.10.3 für einen früheren Vorfall.
6 Ausführlich siehe Tätigkeitsbericht 2013/14 ab Seite 74.

der manuellen Versendung per E-Mail ist für die Versendung an zahlreiche Empfänger die Verwendung eines Mailinglistenprogramms als technische Maßnahme zu empfehlen, zumal diese den Empfängerinnen und Empfängern ermöglichen können, sich selbst vom Newsletter abzumelden.

Geldbußen im Zusammenhang mit Covid-19

Eine Ärztin rief bereits vor dem Berichtsjahr zu einer Versammlung auf. Der Aufruf enthielt Kampfbegriffe wie „Pharma-Faschismus" und „Impfdiktatur". Die Ärztin sendete den Aufruf per WhatsApp auch an Patientinnen und Patienten, welche ihr die Kontaktdaten in ihrer beruflichen Eigenschaft anvertraut hatten. Eine Rechtsgrundlage für den Versand des Aufrufs an die Patientinnen und Patienten gab es nicht, zumal darin eine Zweckänderung lag, die mit dem ursprünglichen Zweck nicht mehr vereinbar war. Festgesetzt wurde im Berichtsjahr eine Geldbuße in Höhe von 2.500 Euro. Da Einspruch gegen den Bußgeldbescheid eingelegt wurde, ist die Sache dem Amtsgericht vorgelegt worden, konnte aber noch nicht verhandelt werden, weil die Adressatin der Geldbuße erst zum Ende des Berichtszeitraumes nach Deutschland zurückgekehrt ist. Bis zu einer rechtskräftigen Entscheidung gilt auch hier die Unschuldsvermutung.

Bei verschiedenen polizeilichen Kontrollen wurden noch im Jahr 2023 Corona-Kontaktdaten aufgefunden.

Bei verschiedenen polizeilichen Kontrollen wurden noch im Jahr 2023 Corona-Kontaktdaten aufgefunden. Bis zum 23. Februar 2022 musste unter anderem in der Gastronomie zwecks Kontaktnachverfolgung dokumentiert werden, wer dort zu Gast war. Diese Dokumentationen waren nach drei Wochen zu vernichten, sodass sie jedenfalls nach Datum sortiert werden mussten. Bereits Mitte März 2022 hätten sämtliche Kontaktdatenblätter vernichtet werden müssen. Die Bußgeldverfahren sind noch anhängig.

Verstöße in der Immobilienwirtschaft

Bei der Prüfung im Bereich der Immobilienwirtschaft haben wir verschiedene Verstöße festgestellt.[7] In fünf Fällen setzten wir Geldbußen nach Erörterungsverfahren mit der Verwaltungsbehörde fest:

7 Siehe Beitrag G.3.2.

- 16.600 Euro gegen ein Unternehmen mit einem Umsatz im Bereich von rund 10 Millionen Euro wegen fehlender Vereinbarungen über die gemeinsame Verantwortlichkeit, dem Erheben und Weiterverarbeiten personenbezogener Daten ohne Rechtsgrundlage (6 datenschutzrechtlich Betroffene) und dem nicht rechtzeitigen Löschen personenbezogener Daten (3 Betroffene).
- 7.100 Euro gegen ein Unternehmen mit einem Umsatz unter 2 Millionen Euro wegen der Verarbeitung personenbezogener Daten ohne Rechtsgrundlage (4 datenschutzrechtlich Betroffene) sowie nicht rechtzeitiges Löschen personenbezogener Daten (2 datenschutzrechtlich Betroffene).
- 9.600 Euro gegen ein Unternehmen mit einem Umsatz von rund 7 Millionen Euro wegen des nicht rechtzeitigen Löschens personenbezogener Daten, unzureichendem Zugang zu Pflichtinformationen und eines unvollständigen Verzeichnisses der Verarbeitungstätigkeiten. Mildernd wurde berücksichtigt, dass Datensätze noch während der Vor-Ort-Kontrolle gelöscht wurden.
- 9.800 Euro gegen ein Unternehmen wegen fehlender Vereinbarungen über die gemeinsame Verantwortlichkeit, dem unzureichenden Nachweis von Einwilligungen bei der Vor-Ort-Kontrolle sowie dem nicht rechtzeitigen Löschen personenbezogener Daten (4 datenschutzrechtlich Betroffene).
- 3.000 Euro gegen ein Einzelunternehmen mit einem Umsatz um 400.000 Euro wegen dem nicht rechtzeitigen Löschen personenbezogener Daten (4 datenschutzrechtlich Betroffene).

Heimliches GPS-Tracking

Im Berichtsjahr sind wieder vermehrt Beschwerden zu GPS-Tracking an uns gerichtet worden. Soweit der Anwendungsbereich der DSGVO eröffnet ist, fehlt den Verantwortlichen insbesondere für heimliches GPS-Tracking regelmäßig die Rechtsgrundlage.[8]

In einem Fall argumentierte der Verantwortliche, dass die Nutzung eines GPS-Trackers wegen eines Notstands nicht sanktioniert werden könne. Der Adressat des Bußgeldbescheids hatte den Tracker angebracht, um etwaige

8 Ausführlicher siehe Tätigkeitsbericht 2020 ab Seite 84.

Verstöße gegen gerichtliche Schutzmaßnahmen zum Schutz einer dritten Person (Gewaltschutzanordnungen wie z. B. ein Kontaktverbot) feststellen und nachweisen zu können. Die Position wurde jedoch nicht nur erhoben, wenn sich der Adressat der Anordnung im ihm verbotenen Bereich beweg-

Im Jahr 2023 erhielten wir vermehrt Beschwerden zu GPS-Tracking.

te. Stattdessen wurden sämtliche Positionen seines Fahrzeugs über bis zu 100 Tage mit einer zeitlichen Auflösung von 30 Sekunden erhoben, sodass dessen Lebensgewohnheiten ausgeforscht werden konnten.

Zuständig für die Durchsetzung gerichtlicher Schutzmaßnahmen sind die Polizei beziehungsweise die Justiz.[9] Gleiches gilt für die elektronische Aufenthaltsüberwachung von Personen zum Beispiel mit elektronischer Fußfessel.[10] Die für einen Notstand erforderliche gegenwärtige, nicht anders abwendbare Gefahr war weder für die Behörde noch das Gericht ersichtlich. Vom Amtsgericht wurde unter Berücksichtigung der wirtschaftlichen Verhältnisse im Beschlussverfahren im Benehmen mit der Datenschutzaufsicht eine Geldbuße in Höhe von 900 Euro festgesetzt.

9 § 11 und $ 17a NPOG, § 4 GewSchG.
10 § 68b StGB, § 17c NPOG.

Gegen Ende des Berichtsjahres sind Fälle mit Bluetooth-Tracker eingegangen, deren Bearbeitung noch nicht abgeschlossen werden konnte. Genutzt wurden Apple AirTags. Diese und ähnliche Tracker sind nicht darauf angelegt, ihre Position selbst bestimmen und übertragen zu können. Stattdessen senden sie ihre Kennung mit energiesparenden Funktechniken aus, was eine Laufzeit der etwa münzgroßen Geräte von ungefähr einem Jahr ermöglicht. Die Kennung der Ortungsgeräte wird von Smartphones in der Umgebung aufgenommen, welche den ungefähren Standort an den Hersteller übermitteln, der den Standort wiederum dem Nutzer des Trackers mitteilt. Über den Fortgang der Verfahren berichten wir im Folgebericht.

Videoüberwachung einer Veranstaltungsfläche und deren Umgebung

Bei der Kontrolle einer Veranstaltungsfläche haben wir verschiedene Verstöße festgestellt.[11] In dem geführten Bußgeldverfahren setzten wir gegen den Betreiber Geldbußen in Höhe von insgesamt 475.000 Euro wegen sechs Verstößen fest:

- Überwachung öffentlicher Bereiche außerhalb des eigenen Grundstückes mit 6 Kameras außerhalb von Veranstaltungstagen und 49 Kameras während Veranstaltungstagen sowie unzulässige Speicherdauer und unzulässige Zwecke.
- Unzureichende Erfüllung der Informationspflichten nach Artikel 13 DSGVO.
- Nicht abgeschlossene Vereinbarung über die gemeinsame Verantwortlichkeit.
- Zwei nicht abgeschlossene Verträge über die Auftragsverarbeitung.
- Unzutreffende Angaben gegenüber der Aufsichtsbehörde im Verwaltungsverfahren, unzureichende Verzeichnisse der Verarbeitungstätigkeit und Nichtmeldung des Datenschutzbeauftragten bei der Aufsichtsbehörde.
- Nichtdurchführung einer Datenschutz-Folgenabschätzung.
- Das Unternehmen hat Einspruch gegen den Bußgeldbescheid eingelegt. Bis zu einer rechtskräftigen Entscheidung gilt die Unschuldsvermutung.

11 Siehe Tätigkeitsbericht 2021 J.9.

Sonstige Videoüberwachung und Dashcams

Viele Fälle betrafen auch im Jahr 2023 den Bereich der Videoüberwachung. Dabei lag ein Schwerpunkt auf Verfahren, in denen Arbeitgeber ihre Beschäftigten sowie Kundinnen und Kunden per Video überwachten. Das Vorgehen gegen Videoüberwachung am Arbeitsplatz haben wir bereits in vergangenen Tätigkeitsberichten ausführlich vorgestellt.[12] Einzelne hervorzuhebende Fälle von Geldbußen aus dem vergangenen Jahr:

- 1.900 Euro ergingen im Wege einer Verständigung vor Gericht gegen ein Unternehmen des Gaststättengewerbes mit weniger als 100.000 Euro Jahresumsatz wegen der unzulässigen Überwachung von Beschäftigten sowie Kundinnen und Kunden.
- 3.200 Euro gegen ein Unternehmen mit etwa 500.000 Euro Jahresumsatz wegen der Überwachung von Trainingsflächen in einem Fitnessstudio im Wege einer Erörterung mit der Verwaltungsbehörde. Berücksichtigt wurden verschiedene mildernde Umstände.
- 20.000 Euro gegen ein Unternehmen des Beherbergungs- und Gaststättengewerbes mit einem Jahresumsatz zwischen 2 und 4 Millionen Euro wegen Überwachung von Beschäftigten sowie Kundinnen und Kunden im Wege einer gerichtlichen Verständigung ohne Verhandlung.
- 12.500 Euro gegen ein Unternehmen mit weniger als 1 Million Euro Jahresumsatz wegen Überwachung von Beschäftigten und Nichtbeachtung einer vollziehbaren Anweisung im Wege einer Verständigung vor Gericht in öffentlicher Verhandlung.
- 24.000 Euro gegen ein Industrieunternehmen mit weniger als 10 Millionen Euro Jahresumsatz wegen der Überwachung öffentlichen Verkehrsraums im Wege einer Erörterung mit der Verwaltungsbehörde.

Zahlreiche Bußgeldentscheidungen entfielen zudem erneut auf Dashcams und andere Kamerasysteme, die anlasslos Videosequenzen aufzeichneten und damit von den Verantwortlichen unzulässig eingesetzt wurden. Zu Dashcam-Geldbußen haben wir bereits ausführlich berichtet[13] und einen umfangreichen Fragen-Antworten-Katalog zum Betrieb von Dashcams veröffentlicht.[14] Eine Geldbuße in Höhe von 4.000 Euro setzten wir gegen

12 Siehe Tätigkeitsbericht 2019 J.9.4, Tätigkeitsbericht 2020 I.4 ab Seite 82 und Tätigkeitsbericht 2021 J.9.2.

13 Siehe Tätigkeitsbericht 2019 I.5.

14 https://lfd.niedersachsen.de/193497.html

ein Unternehmen fest, dessen Firmenfahrzeug über integrierte Kameras verfügte, die den fließenden und ruhenden Verkehr aufnahmen. Erneut

Zahlreiche Bußgeldentscheidungen entfielen auf den Betrieb von Dashcams.

zeigte sich im Jahr 2023, dass Dashcam-Aufzeichnungen geeignet sind, das Fehlverhalten der Verwender aufzuzeichnen. Nach Auswertung des Videomaterials hat unsere Behörde mögliche Verkehrsordnungswidrigkeiten sowie -straftaten bei den für die Verfolgung zuständigen Stellen zur Anzeige gebracht.

In einem anderen Fall hatte eine unbekannte Person eine Kamera mit SIM-Karte im Bereich einer Baumreihe befestigt und auf einen Parkplatz gerichtet. Zur Ermittlung des Inhabers der SIM-Karte haben wir die Bestandsdaten beim Netzbetreiber angefragt.[15] Der Netzbetreiber erteilte die Auskunft.[16] Das Verfahren ist noch anhängig.

Livestreaming des öffentlichen Verkehrsraums

Parallel zu ihrer primären Tätigkeit hat eine Fahrschule Fahrstunden live im Internet gestreamt. Dabei waren weite Teile des öffentlichen Verkehrsraumes sichtbar. Nachdem die Fahrschule im Verwaltungsverfahren noch

15 Grundlage der Anfrage: § 100j Absatz 1 Satz 1 Nr. 1 Strafprozessordnung.
16 Grundlage der Auskunft: § 174 Absatz 3 Nr. 1 Telekommunikationsgesetz.

mitteilte, nicht weiter zu streamen[17], hat sie das Streaming einige Monate später wieder aufgenommen. Vorgeworfen haben wir daher zwei Tatzeiträume für die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage sowie die unzureichende Erfüllung von Informationspflichten, den Nichtabschluss eines Vertrages über die Auftragsverarbeitung beziehungsweise einer Vereinbarung über die gemeinsame Verantwortlichkeit mit dem Streamingportal und das fehlende Verzeichnis der Verarbeitungstätigkeiten.

In öffentlicher Verhandlung wurde vom Amtsgericht im Wege einer Verständigung über alle Verstöße eine Geldbuße in Höhe von 17.000 Euro verhängt. Die Höhe der festgesetzten Geldbuße im Verhältnis zum Umsatz des Unternehmens – rund 200.000 Euro – macht deutlich, dass es sich um besonders gewichtige Verstöße handelte.

17 Siehe Tätigkeitsbericht 2022 J.8.3.

I Deutsche Datenschutzkonferenz

I.1 Arbeitskreis Versicherungswirtschaft: Beratung zu Gesundheitsdaten und Verhaltensregeln

Im Arbeitskreis Versicherungswirtschaft der Datenschutzkonferenz beraten wir als Vorsitzende mit den anderen Aufsichtsbehörden datenschutzrechtliche Fragen aus der Versicherungsbranche. Im Berichtsjahr ging es unter anderem darum, ob eine Einwilligung für die Verarbeitung von Gesundheitsdaten durch Krankenversicherungen notwendig ist und ob Versicherungen dem Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) Personen melden dürfen, die besonders häufig Schäden an Autos geltend machen.

Es ist umstritten, auf welcher datenschutzrechtlichen Grundlage Versicherungen Gesundheitsdaten bei einer Leistungsprüfung verarbeiten dürfen.[1] Fraglich ist, ob es für diese Verarbeitungen einer Einwilligung[2] bedarf oder ob sie auf eine Rechtsgrundlage gestützt werden kann, weil die Gesundheitsdaten zur Prüfung eines Anspruchs erforderlich sind.[3] In unserem Tätigkeitsbericht 2022 waren wir der Auffassung, dass eine Einwilligung nicht notwendig sei, hatten aber bereits angemerkt, dass die Beratungen noch nicht abgeschlossen sind.

Vor dem Hintergrund erster Rechtsprechung zu dieser Auslegungsfrage und dem Bedürfnis nach einer bundesweit einheitlichen Handhabung haben wir uns inzwischen der Auffassung angeschlossen, dass es grundsätzlich einer Einwilligung bedarf. Nachdem die Beratungen im Arbeitskreis abgeschlossen sind, liegt die Frage nun der Datenschutzkonferenz (DSK) zur Beschlussfassung vor.

1 Siehe auch Tätigkeitsbericht 2022 E.2.
2 Art. 9 Abs. 2 Buchstabe a DSGVO.
3 Art. 9 Abs. 2 Buchstabe f DSGVO.

Dürfen häufige Schadensmeldungen ans HIS übermittelt werden?

Der Arbeitskreis hat sich mit dem Gesamtverband der deutschen Versicherungswirtschaft und der informa HIS GmbH, die das Hinweis- und Informationssystem der Versicherungswirtschaft (HIS) betreibt, zu einem neuen Meldegrund ausgetauscht. Das HIS dient der Aufdeckung von Versicherungsbetrug und ist bereits seit 2011 in Betrieb. Versicherungsunternehmen können hier auf Grundlage standardisierter Meldegründe Meldungen an das HIS vornehmen und dadurch auch personenbezogene Daten übermitteln, erheben und speichern.

So lässt sich beispielsweise aufklären, wenn jemand versucht, einen Schaden an einem PKW bei verschiedenen Versicherungen mehrfach abzurechnen. Im Jahr 2023 hat die informa HIS GmbH einen neuen Meldegrund eingeführt. Darüber wollen die Versicherungen ermitteln, ob Personen mit weit überdurchschnittlicher Häufigkeit in Schadensfälle mit betrügerischer Absicht involviert sind. Der Arbeitskreis hat den neuen Meldegrund zur Kenntnis genommen und mit der informa HIS GmbH eine Evaluation vereinbart, wenn statistisch belastbare Erkenntnisse zur Nutzung des neuen Meldegrunds vorliegen.

Verhaltensregeln der Versicherungswirtschaft

Der Gesamtverband der Deutschen Versicherungswirtschaft hat bei der zuständigen Aufsichtsbehörde einen Antrag auf Genehmigung von Verhaltensregeln gestellt. Verhaltensregeln sind ein Instrument, um abstrakte Regelungen der DSGVO für definierte Verarbeitungsbereiche zu konkretisieren, wie zum Auskunftsrecht, und so eine einfachere und bessere Anwendung zum Beispiel in bestimmten Branchen zu gewährleisten.[4] Wegen der deutschlandweiten Geltung der Verhaltensregeln findet hierzu eine Diskussion über die einzelnen Bestimmungen und Abstimmung im Arbeitskreis statt. Diese dauert noch an.

4 Art. 40 DSGVO.

I.2 Arbeitskreis Beschäftigtendatenschutz: Bundesweite und niedersächsische Regelungen unzureichend

In der Datenschutzkonferenz hat unsere Behörde den Vorsitz des Arbeitskreises Beschäftigtendatenschutz inne. Die Konferenz fordert wiederholt ein Beschäftigtendatenschutzgesetz – wir sehen uns durch ein aktuelles Urteil des Europäischen Gerichtshofs bestätigt.

Aufgabe des Arbeitskreises (AK) Beschäftigtendatenschutz ist es, einheitliche Positionen aller Aufsichtsbehörden zu datenschutzrechtlichen Fragen im Beschäftigtenkontext zu erarbeiten. Der Arbeitskreis bereitet Entscheidungen der Datenschutzkonferenz (DSK) vor und bespricht aktuelle Themen und Urteile.

So tauschte sich der Arbeitskreis Anfang 2023 zu besonderen Fallkonstellationen im Beschäftigtenkontext aus. Mit unseren Kolleginnen und Kollegen aus anderen Datenschutzbehörden diskutierten wir die Umsetzung der DSGVO in der Praxis, ob zum Beispiel Betriebsvereinbarungen als Erlaubnisnorm zum Tragen kommen und wie diese gemäß den Vorgaben der DSGVO auszugestalten wären.[1] Für uns wurde deutlich, dass Betriebsvereinbarungen nur dann als Rechtsgrundlage zur Verfügung stehen können, wenn sie auch die von der DSGVO geforderten Schutzvorschriften zugunsten der Beschäftigten enthalten.

Außerdem behandelten wir besondere Fälle, die im Zusammenhang mit der Corona-Pandemie stehen. In diesem Zusammenhang vertritt der Arbeitskreis die Ansicht, dass die Verantwortlichen die während der Corona-Pandemie zum Beispiel zur Zutrittskontrolle erhobenen 3G-Daten (geimpft, genesen oder negativ getestet) regelmäßig löschen müssen.

1 Art. 88 Abs. 2 DSGVO.

Forderung nach einem Beschäftigtendatenschutzgesetz

Im März 2023 hat ein Urteil des Europäischen Gerichtshofs (EuGH)[2] aufgezeigt, dass im Zusammenhang mit der Verarbeitung von Beschäftigtendaten zahlreiche deutsche Vorschriften überprüft und womöglich angepasst werden müssen. Dies gilt auch für niedersächsische Regelungen.

Der AK Beschäftigtendatenschutz hat in diesem Zusammenhang für die 105. Datenschutzkonferenz eine Entschließung nebst Hintergrundpapier mit Hinweisen für die Praxis zur weiteren Vorgehensweise vorbereitet, die die DSK im Mai 2023 veröffentlicht hat.[3] Darin weist die DSK den Gesetzgeber auf die große Bedeutung des Urteils auf die Regelungen zum Beschäftigtendatenschutz in Deutschland hin und fordert ihn dazu auf, ein eigenes Beschäftigtendatenschutzgesetz zu schaffen.

Die Forderung ist nicht neu: Bereits im April 2022 hatte die DSK sich in einer Entschließung „Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!"[4] an den Gesetzgeber gewandt.

Ausblick 2024

Nach den Ausführungen des EuGH im oben genannten Urteil liegt der Schluss nahe, dass sowohl die bundesrechtlichen als auch die niedersächsischen Regelungen die vom EuGH aufgestellten Anforderungen nicht erfüllen. Es bleibt abzuwarten, ob und wie der Bundesgesetzgeber in einem Beschäftigtendatenschutzgesetz beziehungsweise der Landesgesetzgeber in landesrechtlichen Regelungen die seitens des EuGH im Urteil dargestellte Rechtsansicht umsetzen.

Nach Aussage der Landesregierung[5] wurde hierzu bereits eine „landesübergreifende Erörterung und Prüfung" eingeleitet. Damit soll festgestellt werden, ob die niedersächsischen Regelungen für die Verarbeitungen personenbezogener Daten von Beschäftigten durch öffentliche Stellen den

2 Siehe Urteil des EuGH vom 30. März 2023 in der Rechtssache C-34/21, Kurzlink: https://t1p.de/eugh-2023

3 Siehe DSK-Entschließung „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!", März 2023, Kurzlink: https://t1p.de/dsk-be-2023 (PDF).

4 Kurzlink: https://t1p.de/dsk-be-2022 (PDF).

5 Siehe Stellungnahme der Niedersächsischen Landesregierung zum 28. Tätigkeitsbericht des LfD Niedersachsen, Abschnitt E3 „Datenschutzkonferenz fordert ein Beschäftigtendatenschutzgesetz", abrufbar unter https://www.stk.niedersachsen.de/227327.html

Vorgaben der DSGVO entsprechen.[6] Das Ergebnis der Prüfung bleibt abzuwarten.

Fazit

Auch wenn wir für die Aufgabe als Vorsitz des AK Beschäftigtendatenschutz etliche Ressourcen zur Verfügung stellen müssen, erweist sich die „Investition" als äußerst sinnvoll. Wir schützen damit die Beschäftigten und geben gleichermaßen Arbeitgebern und Arbeitgeberinnen Rechtssicherheit bei der Verarbeitung der personenbezogenen Daten ihrer Beschäftigten.

6 Art. 88 Abs. 1, 2 DSGVO, Art. 6 Abs. 1 Buchst. c oder e DSGVO in Verbindung mit einer jeweiligen nationalen Rechtsgrundlage.

Chatkontrolle führt zu unverhältnismäßiger Massenüberwachung I.3

Die Europäische Kommission arbeitet an einer Verordnung zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern. Diese soll Anbieter dazu verpflichten, in ihren Online-Diensten die Kommunikation ihrer Nutzer zu durchsuchen. Viele Kritiker sehen in dem als Chatkontrolle bezeichneten Entwurf der Verordnung einen drastischen Eingriff in Grundrechte. Hierzu hat sich die DSK in einer Entschließung deutlich positioniert.

Seit 2014 gilt in Europa eine Übergangsverordnung zur Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, die in der Öffentlichkeit wenig wahrgenommen worden ist. Sie führt bereits seit einigen Jahren dazu, dass Anbieter von E-Mail-, Chat- und Messenger-Diensten freiwillig Techniken einsetzen, um sexuellen Kindesmissbrauch im Internet in ihren Diensten aufzudecken, zu melden und zu entfernen. Dafür analysieren sie die Inhalte der Kommunikation automatisiert nach bestimmten Indikatoren. Von dem hiermit verbundenen Verstoß gegen die europarechtlichen Vorschriften zur Vertraulichkeit der Kommunikation hat die Übergangsverordnung die Anbieter entbunden.

Die nun geplante Verordnung soll deutlich weitergehen. Adressaten sind darin nicht nur Anbieter von sogenannten nummernungebundenen interpersonellen Kommunikationsdiensten, also etwa Messenger- oder Mail-Diensten. Vielmehr sind künftig alle Anbieter von interpersonellen Kommunikationsdiensten, einschlägigen Diensten der Informationsgesellschaft, Hosting-Diensten und Internetzugangsdiensten von der Verordnung betroffen.

Zudem werden diesen ausdrücklich verpflichtende Maßnahmen auferlegt zur Verhinderung des sexuellen Missbrauchs von Kindern im Internet, und zwar durch Bewertung und Minderung von Risiken sowie gegebenenfalls durch gezielte Maßnahmen, um sexuellen Missbrauch von Kindern im Internet aufzudecken, zu melden und Material dazu zu entfernen.

Die Datenschutzkonferenz (DSK) ist in ihrer Entschließung vom 17. Oktober 2023[1] zu dem deutlichen Votum gekommen, dass die geplante Chatkontrolle zu einer unverhältnismäßigen, anlasslosen Massenüberwachung führt. Hauptkritikpunkt ist die Tatsache, dass die Erfüllung der vorgesehenen Pflichten durch die Anbieter für alle Nutzer dieser Dienste unterschiedslos und verdachtsunabhängig zu einer Totalüberwachung vertraulicher Kommunikation führt.

Die DSK betont, dass ohne Zweifel die Notwendigkeit besteht, Kinder im Internet vor sexuellem Missbrauch zu schützen und entsprechende Straftaten aufzudecken. Sie stellt nicht die Ziele der geplanten Verordnung infrage, sondern das vorgesehene Mittel einer staatlich angeordneten Kontrolle und Überwachung von Kommunikation in einem unverhältnismäßigen Ausmaß. Auch wenn dieser Ansatz hoch umstritten ist, sollten die Pflichten der Anbieter sogar dann gelten, wenn die Kommunikation Ende-zu-Ende verschlüsselt ist. Der Anbieter wäre damit verpflichtet gewesen, diese Verschlüsselung aufbrechen zu können, so dass die Vertraulichkeit der Kommunikation nicht mehr gewährleistet gewesen wäre. Im November 2023 teilte das Europäische Parlament mit, dass Aufdeckungsanordnungen bezüglich Ende-zu-Ende-verschlüsselter Kommunikation und Textnachrichten vom Anwendungsbereich ausgenommen wären.

Fazit

Die Entschließung der Datenschutzkonferenz ist ein sehr wichtiges Statement gegen die vorgesehene anlasslose Massenüberwachung durch die Chatkontrolle. Diese greift fundamental in die Grundrechte auf Achtung des Privat- und Familienlebens, der Vertraulichkeit der Kommunikation und zum Schutz personenbezogener Daten ein und stellt eine verfassungswidrige Vorratsdatenverarbeitung dar.

Die Bekämpfung des sexuellen Missbrauchs von Kindern im Internet ist zweifellos ein hehres Ziel und unstreitig ein wichtiges Anliegen. Sie muss durch andere zielgerichtete und effiziente Maßnahmen erreicht werden, ohne dabei pauschal das für eine Demokratie und unseren gesellschaftlichen Zusammenhalt gleichermaßen essentielle Grundrecht auf Vertraulichkeit der Kommunikation auszuhöhlen.

1 Kurzlink: https://t1p.de/dsk-chatkontrolle (PDF).

Einwilligungsdienst statt Cookie-Banner? Quadratur des Kreises gescheitert I.4

Mit einer Verordnung über Dienste zur Einwilligungsverwaltung gemäß § 26 TTDSG will das Bundesministerium für Digitales und Verkehr die unbeliebten Einwilligungsbanner auf Webseiten und in Apps entbehrlich machen. In einer Stellungnahme hat die Datenschutzkonferenz das Ziel der Verordnung zwar grundsätzlich unterstützt, aber mit dem aktuell vorliegenden Verordnungsentwurf als nicht erreichbar bewertet.

Eine der wenigen innovativen Vorschriften, die durch das Telekommunikation-Telemedien-Gesetz (TTDSG) am 1. Dezember 2021 neu eingeführt worden ist, ist die Verordnungsermächtigung zu den anerkannten Diensten zur Einwilligungsverwaltung gemäß § 26 TTDSG. Einwilligungsbanner auf Webseiten und in Apps sind für viele ein leidiges Übel, das jeder schnell überwinden möchte. Mit der Einführung von § 26 TTDSG wurde das Ziel verbunden, Internetnutzer von dieser Last zu befreien.

Ersetzt werden sollen die Banner durch anerkannte Dienste zur Einwilligungsverwaltung.[1] Diese stellen nutzerfreundliche und wettbewerbskonforme Verfahren zur Einwilligung in die Verarbeitung von Verkehrs- und Standortdaten, das Speichern von Informationen auf Endeinrichtungen und den Zugriff auf bereits auf diesen gespeicherten Informationen dar, insbesondere um den Einsatz von Cookies und anderen Trackingtechniken zu ermöglichen.

Nach der ursprünglichen Idee sollten Internetnutzer über die Einwilligungsverwaltungsdienste einmalig festlegen, welche Cookies, Tracking- und sonstigen Drittdienste diese akzeptieren und welche nicht, um anschließend nicht bei jedem Webseitenbesuch erneut danach gefragt werden zu müssen.

In einem zweiten Anlauf veröffentlichte das Bundesministerium für Digitales und Verkehr (BMDV) im Juni 2023 einen überarbeiteten Entwurf für

1 Diese werden auch als Personal Information Management Service (PIMS) bezeichnet.

eine Einwilligungsverwaltungsverordnung (EinwV). Diese soll gemäß § 26 TTDSG den Rechtsrahmen festlegen, der zu einer Anerkennung solcher Dienste führt, damit Internetnutzer diesen vertrauen können. Zugleich sollen Browser die Einstellungen, die die Endnutzer im Zusammenhang mit der Einwilligung nach § 25 vorgenommen haben, auch tatsächlich berücksichtigen.

Unlösbare Probleme

Zum Verordnungsentwurf hatte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ausführlich Stellung genommen.[2] Die DSK betont in dieser Stellungnahme, dass das mit dem Verordnungsentwurf verfolgte Ziel, Einwilligungsbanner auf Webseiten überflüssig zu machen, mit dem Regelungsansatz der Einwilligungsverwaltungsverordnung nicht erreicht werden kann.

Das BMDV steht vor zwei unlösbaren Problemen, die bereits in § 26 TTDSG angelegt sind. Erstens umfasst § 26 TTDSG nur Einwilligungen für den Einsatz von Cookies und Trackingtechniken.[3] Auf den Webseiten werden und müssen aber in aller Regel auch Einwilligungen für die Verarbeitungen personenbezogener Daten gemäß der Datenschutz-Grundverordnung (DSGVO) eingeholt werden[4], die beim Einsatz von Cookies und Trackingtechniken insbesondere für personalisierte Werbung erforderlich sind. Diese lassen sich nicht über die Einwilligungsverwaltungsdienste abdecken, da dem deutschen Gesetzgeber aufgrund des Vorrangs der DSGVO die Regelungskompetenz fehlt.

Zweitens müssen die Einwilligungen den Anforderungen an wirksame Einwilligungen nach DSGVO genügen. Der Entwurf sieht vor, dass der Nutzer im Einwilligungsverwaltungsdienst „generelle Einwilligungen" abgibt.[5] Diese wären als unzulässige Pauschaleinwilligungen zu werten.

Aus dem Entwurf der EinwV geht allerdings die Funktionsweise der Dienste gar nicht genau hervor. Obwohl die Grundfunktion der Dienste die Ertei-

2 DSK, Stellungnahme zum Referentenentwurf des BMDV zur Rechtsverordnung nach § 26 Abs. 2 TTDSG vom 11. Juli 2023, Kurzlink: https://t1p.de/dsk-ttdsg (PDF).
3 Gemäß § 25 TTDSG.
4 Art. 6 Abs. 1 Buchst. a DSGVO.
5 § 3 Abs. 4 EinwV-Entwurf.

lung der Einwilligung und damit deren Wirksamkeit betrifft[6], scheint sich der Einsatz der Dienste tatsächlich darauf zu beschränken, die auf den jeweiligen Webseiten erteilten Einwilligungen zu speichern, zu verwalten und bei Bedarf zu übermitteln. Die Abgabe der Einwilligung erfolgt anscheinend nicht direkt im Einwilligungsverwaltungsdienst, sondern – wie bisher – beim erstmaligen Öffnen der Webseite über die Cookie-Banner.

Anforderungen an die anerkannten Dienste

In der Stellungnahme weist die DSK des Weiteren darauf hin, dass die technische und organisatorische Ausgestaltung der anerkannten Dienste in dem Entwurf der Einwilligungsverwaltungsverordnung weitgehend offengelassen wird. Es wird vor allem keine Aussage getroffenen, ob die Lösungen lokal, also browserbasiert oder zentral, also serverbasiert ausgestaltet werden sollen.

Aus datenschutzrechtlicher Perspektive weisen browserbasierte Lösungen den Vorteil auf, dass zusätzliche Datensammlungen bei einem Dienstleister leichter vermieden werden und daher geringere Anforderungen an die Datensicherheit zu stellen sind. Den Grundsätzen der Datenminimierung und der Datensicherheit würde insofern Rechnung getragen.

Teilweise entsteht der Eindruck, die Einwilligungsverwaltungsdienste sollen weniger dem Nutzer dienen, als vielmehr bei den Unternehmen den Aufwand verringern.

Änderungsvorschläge

Die Stellungnahme enthält nach diesen übergeordneten Kritikpunkten zu zahlreichen Regelungen im Entwurf der EinwV konkrete Änderungsvorschläge. Teilweise entsteht der Eindruck, die Einwilligungsverwaltungsdienste sollen weniger dem Nutzer dienen, als vielmehr bei den Unternehmen den Aufwand verringern, von den Nutzern ihrer Webseiten Einwilligungen zu bekommen. Vielen der Änderungsvorschläge ist daher gemeinsam, dass das Ziel der Entlastung der Webnutzer in den Fokus gerückt wird.

6 Gemäß § 3 Abs. 1 EinwV-Entwurf.

Fazit

Zu dem Entwurf der EinwV haben viele unterschiedliche Interessensvertreter Stellungnahmen abgegeben.[7] Es liegen allerdings keine Informationen darüber vor, ob und wann die Arbeiten an diesem Verordnungsentwurf fortgesetzt werden. Aufgrund der grundlegenden Kritikpunkte der Datenschutzkonferenz halten wir es für so gut wie ausgeschlossen, dass mit der Verordnung die Ziele von § 26 TTDSG erreicht werden können. Dies gilt aufgrund der grundsätzlichen Probleme selbst dann, wenn eine grundlegende Überarbeitung erfolgt.

7 Alle Stellungnahmen können hier eingesehen werden: https://bmdv.bund.de/goto?id=528368

Prüfungsmaßstäbe für Pur-Abo-Modelle auf Webseiten I.5

Die Datenschutzkonferenz hat einheitliche datenschutzrechtliche Prüfungsmaßstäbe für sogenannte Pur-Abo-Modelle festgelegt. Diese Positionierung war erforderlich, weil auf immer mehr Webseiten Besucher zwischen Einwilligung und Abo entscheiden müssen und sich Beschwerden hierzu häufen.

Bei einem Pur-Abo-Modell stehen den Nutzenden einer Website über ein Einwilligungsbanner üblicherweise zwei Möglichkeiten zur Auswahl, um auf die Inhalte zugreifen zu können. Entweder schließen sie ein sogenanntes Pur-Abo ab, oder sie willigen – ohne Pur-Abo – ein, ihre Daten für profilbasierte und individualisierte Werbung freizugeben. Nur bei Wahl eines Pur-Abos sind Tracking-Mechanismen deaktiviert und die Website kann ohne individuelle Profilbildung und personalisierte Werbung genutzt werden.

Die Besucherinnen und Besucher zahlen also nicht für die Artikel, Videos oder Podcasts. Sie verhindern vielmehr damit, dass ihre personenbezogenen Daten durch digitales Marketing monetarisiert werden.

Medien bieten auf ihren Webseiten außer dem Pur-Abonnement häufig ein weiteres Abonnement an, das sie meist als Plus-Abonnement bezeichnen. Bei diesem Abonnement zahlen die Nutzer für Beiträge auf der Webseite, die unabhängig vom Abschluss eines Pur-Abos oder der Abgabe einer Einwilligung für alle kostenpflichtig sind.

Die Aufsichtsbehörden erhalten seit der Einführung der ersten Pur-Abo-Modelle regelmäßig Beschwerden über Websites, die diese Modelle anbieten. Die Datenschutzkonferenz (DSK) hat deshalb in einem Beschluss zur „Bewertung von Pur-Abo-Modellen auf Websites“ die datenschutzrechtlichen Anforderungen an Pur-Abo-Modelle konkretisiert und festgelegt.[1] Der Beschluss kann einerseits in der Praxis als Hilfestellung für die konkrete

1 DSK-Beschluss „Bewertung von Pur-Abo-Modellen auf Websites“, Kurzlink: https://t1p.de/dsk-pur-abos (PDF).

Ausgestaltung eines Pur-Abo-Modells dienen. Anderseits stellt er die einheitlichen Prüfmaßstäbe der Aufsichtsbehörden für die Öffentlichkeit dar.

Pur-Abo statt „Alles Ablehnen"-Schaltfläche

Mit einem Pur-Abo-Modell umgehen Betreiber von Webseiten häufig die Forderung der Aufsichtsbehörden, eine „Alles Ablehnen"-Schaltfläche im Einwilligungsbanner auf der ersten Seitenebene anzubieten. So eine Schaltfläche stellt sicher, dass die Einwilligung über das Banner nicht erzwungen, sondern freiwillig ist.[2] Diesbezüglich stellt die DSK in dem Beschluss fest, dass das Pur-Abo-Modell grundsätzlich geeignet ist, das Defizit einer gleichwertigen Alternative zur „Alles Annehmen"-Schaltfläche" zu beseitigen.

Denn mit dem Pur-Abo gibt es eine Alternative, die Webseite ohne Abgabe der Einwilligung zu nutzen. Von Abonnenten darf der Betreiber allerdings nur ein marktübliches Entgelt für die trackingfreie Alternative verlangen und er muss allen Nutzern einen gleichwertigen Zugang zu derselben Leistung eröffnen. Zudem dürfen bei Abonnenten keine Cookies oder anderen Trackingtechniken eingesetzt oder Drittdienste auf der Webseite eingebunden werden, die einwilligungsbedürftig sind.[3]

Wirksamkeit der Einwilligung von Nicht-Abonnenten

Die DSK betont, dass Einwilligungen von Nutzern der Webseite, die kein Pur-Abo abgeschlossen haben – also Nicht-Abonnenten – nach den Anforderungen der Datenschutz-Grundverordnung (DSGVO) wirksam sein müssen. Es gelten bei einem Banner mit den Alternativen Pur-Abo und Einwilligung dieselben Anforderungen wie für Einwilligungsbanner ohne die Pur-Abo-Alternative.

Von Abonnenten darf der Betreiber nur ein marktübliches Entgelt für die trackingfreie Alternative verlangen.

Besonders hervorzuheben ist in die Anforderung der Granularität der Einwilligung. Häufig soll der Nutzer in unterschiedliche Verarbeitungszwecke einwilligen, wie zum Beispiel zur personalisier-

2 Siehe zu dieser Forderung ausführlich DSK, Orientierungshilfe für Anbieter von Telemedien, Version 1.2, Rn. 47, 132 ff., Kurzlink: https://t1p.de/dsk-telemedien (PDF).

3 Gemäß § 25 TTDSG oder Art. 6 Abs. 1 Buchst. a DSGVO.

ten Werbung mit Profilbildung, Anzeige von externen Inhalten wie Videos oder Verbesserung der Webseite. Weichen die Verarbeitungszwecke wesentlich voneinander ab, ist die Einwilligung nur freiwillig, wenn Nutzer die einzelnen Zwecke selbst und aktiv auswählen können.

Fazit

In der Praxis zeigt sich, dass die Webseitenbetreiber die von der DSK formulierten Anforderungen bei Bannern mit Pur-Abo-Modellen häufig nicht vollständig umsetzen. In den meisten Fällen holen sie von Nicht-Abonnenten keine wirksamen Einwilligungen ein. Dabei geht es nicht um die Frage, ob die Betreiber der Webseite diese kostenlos zur Verfügung stellen müssen. Es steht ihnen frei, die Webseite ausschließlich als kostenpflichtigen digitalen Dienst anzubieten – sich also für die Kenntnisnahme der Inhalte bezahlen zu lassen. Die Werbefinanzierung kann so insbesondere mit inhaltsbasierter Werbung ohne Tracking und Profilbildung der Nutzerinnen und Nutzer datenschutzkonform erfolgen.

Nicht mit dem Datenschutzrecht vereinbar ist es aber, die Webseite durch personalisierte Werbung mit umfassender Profilbildung durch zahlreiche Drittdienste zu finanzieren, ohne für diese Prozesse wirksame Einwilligungen vorliegen zu haben. Der Beschluss der DSK wird hoffentlich dazu führen, dass Anbieter die Bewertungsmaßstäbe beachten, um Durchsetzungsmaßnahmen der Aufsichtsbehörden zu vermeiden.

I.6 Trainingsdaten aus dem Straßenverkehr: So lernt das autonome Fahrzeug

Für das Entwickeln autonomer Fahrzeuge benötigen die Automobilhersteller Unmengen an Trainingsdaten aus dem echten Verkehr. Diese Daten sammeln spezielle Fahrzeuge bei Entwicklungsfahrten ein – ausgestattet mit Kameras, Mikrofonen und allerlei Sensoren. Die datenschutzrechtlichen Rahmenbedingungen hat die Datenschutzkonferenz in einem Positionspapier konkretisiert.

Im Verkehr sind immer mal wieder Fahrzeuge von Unternehmen oder Forschungseinrichtungen zu erblicken, die teils sichtbar mit zusätzlichen technischen Merkmalen wie Videokameras oder Antennen ausgestattet sind. Damit generieren sie möglichst umfassende Datensammlungen zum realen Verkehrsgeschehen, um das autonome Fahren weiterzuentwickeln.

In den Datensammlungen der Videokameras, Mikrofone und sonstigen Sensoren sind zahlreiche personenbezogene Daten vorhanden, beispielsweise Aufnahmen von Passanten, Gespräche zwischen Radfahrern und Standortinformationen zu Fahrzeugen. Die Besonderheit ist, dass die für die Entwicklung der neuen Technik erforderlichen Daten nicht ausschließlich in Laboren oder auf Testgeländen gesammelt werden, sondern im realen Verkehr und somit sehr viele Unbeteiligte von den Datenverarbeitungen betroffen sind.

Die Datenschutzkonferenz (DSK) zeigt in einem Positionspapier auf, unter welchen Bedingungen diese Entwicklungsfahrten datenschutzkonform durchgeführt werden können.[1] In dem Papier haben die Datenschutzbehörden versucht, die Interessen aller Beteiligten in bestmöglichen Einklang zu bringen – die Interessen der Fahrzeughersteller an neuen Produktentwicklungen, das gesamtgesellschaftliche Interesse an der Erhöhung der Verkehrssicherheit und das sowohl gesellschaftliche als auch individuelle Interesse, sich im öffentlichen Raum unbeobachtet bewegen zu können. Das Positionspapier führt dazu Kriterien und Schutzmaßnahmen auf, um

1 DSK, Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten vom 27.9.2023, Kurzlink: t1p.de/dsk-umgebung (PDF).

den Datenschutz Dritter, die in das Blickfeld der Kameras und der Sensorik der Fahrzeuge geraten, bestmöglich zu schützen.

Unter anderem führt es besonders schützenswerte Verkehrsbereiche auf, wie zum Beispiel von der Straße aus einsehbare Räumlichkeiten, Schulhöfe oder Spielplätze, wobei die Eingriffstiefe in die Privatsphäre durch eine Mehrfacherfassung solcher Bereiche deutlich erhöht werden kann.

Schließlich müssen die Daten, die in Entwicklungsfahrten gewonnen und verarbeitet werden, durch technische Sicherungsmaßnahmen bestmöglich geschützt werden. Daher fordert das Positionspapier außer der sorgfältigen Abwägung der berechtigten Interessen der Betreiber und den Grundrechten der Betroffenen eine Datenschutz-Folgenabschätzung, das heißt eine strukturierte Risikoanalyse und Dokumentation der ergriffenen Maßnahmen zur Eindämmung der erkannten Risiken.

Fazit

Das Positionspapier zeigt deutlich, dass das der Datenschutz technischen Entwicklungen nicht ablehnend und behindernd gegenübersteht. In enger Zusammenarbeit mit dem Verband der Automobilindustrie e. V. (VDA) haben die Aufsichtsbehörden datenschutzkonforme Lösungen entwickelt, die die Entwicklung des autonomen Fahrens unterstützen und zugleich den berechtigten Interessen der Verkehrsteilnehmer auf Schutz ihrer Privatsphäre angemessen Rechnung tragen.

I.7 Entschließungen zum Datenschutz in der medizinischen Forschung und bei medizinischen Registern

Die Datenschutzkonferenz hatte im Jahr 2023 einen Themenschwerpunkt im Bereich der medizinischen Forschung. In zwei Entschließungen gibt sie Gesetzgebern des Bundes und der Länder wichtige Hinweise, wie das öffentliche Interesse an einer Nutzung von Gesundheitsdaten in einen sachgerechten Ausgleich mit dem Recht der Betroffenen auf informationelle Selbstbestimmung gebracht werden kann.

Bereits im Vorjahr hatte die Datenschutzkonferenz (DSK) einen Fokus auf den Datenschutz im Forschungsbereich gerichtet und damit der hohen gesellschaftlichen Bedeutung der wissenschaftlichen Forschung mit Gesundheitsdaten Rechnung getragen.[1] Im Jahr 2023 richtete sich der Blickwinkel nunmehr auf die konkrete Gesetzgebung des Bundes und der Länder.

Datenschutz in der Forschung durch einheitliche Maßstäbe stärken

Gegenwärtig besteht bei der Forschung mit Gesundheitsdaten in Bund und Ländern eine heterogene Rechtslage. Die landesrechtlichen Regelungen, die die Datenverarbeitung zu Forschungszwecken durch Krankenhäuser und andere Stellen des öffentlichen Gesundheitsdienstes betreffen, weichen oftmals erheblich voneinander ab. Dies kann sich bei länderübergreifenden Forschungsvorhaben nachteilig auf die Projektdurchführung und den Datenschutz der betroffenen Personen auswirken.

1 Siehe Tätigkeitsbericht 2022, E.4 sowie die DSK-Entschließung „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz" vom 23. März 2022 und die DSK-Entschließung „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung" vom 24. November 2022, abrufbar unter https://www.datenschutzkonferenz-online.de/entschliessungen.html.

Die DSK hat in ihrer Entschließung „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“[2] vom 23. November 2023 Eckpunkte für aufeinander abgestimmte gesetzliche Regelungen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken erstellt.

Dies betrifft außer den konkreten Zulässigkeitsvoraussetzungen insbesondere die Forderung einer gesetzlichen Festlegung geeigneter Garantien und Maßnahmen sowie einer uneingeschränkten Datenschutzaufsicht. Zugleich richtet die DSK in ihrer Entschließung einen Appell an die Gesetzgeber, zeitnah eine Vereinheitlichung der forschungsrelevanten Rechtsgrundlagen vorzunehmen und somit den Datenschutz bei länderübergreifenden Forschungsvorhaben zu stärken.

Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register

Die DSK knüpft mit ihrer Entschließung „Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register“[3] vom 23. November 2023 an das Vorhaben der Bundesregierung zur Schaffung eines Registergesetzes an.[4] In der Entschließung stehen konkrete datenschutzrechtliche Anforderungen, damit der Aufbau und die Nutzung medizinischer Register datenschutzkonform erfolgt.

Neben der Forderung nach einer gesetzlichen Vollregelung der Verarbeitungsvoraussetzungen betrifft dies die gesetzliche Festlegung geeigneter Garantien und Maßnahmen zur Wahrung der Grundrechte der betroffenen Personen. Insbesondere sollen unabhängige Vertrauensstellen eingeführt werden, denen eine zentrale Rolle bei der Anonymisierung und Pseudonymisierung der Gesundheitsdaten vor der Bereitstellung für Forschende und bei der Verwaltung bereichsspezifischer Kennzeichen zukommen soll. Zudem sind verhältnismäßige Regelungen über die Aufbewahrungsdauer und Löschfristen der Registerdaten zu treffen. Bei besonderen Risiken wie zum Beispiel einem Remotezugriff auf Gesundheitsdaten über digitale Portale soll der Gesetzgeber im Rahmen einer gesetzlichen Datenschutz-Folgeabschätzung globale Risiken der Registersysteme ermitteln. Darüber

2 Kurzlink: https://t1p.de/dsk-forschung (PDF).
3 Kurzlink: https://t1p.de/dsk-register (PDF).
4 Vgl. Koalitionsvertrag 2021–2025, Mehr Fortschritt wagen, S. 65, Kurzlink: https://t1p.de/koalition-2021

hinaus sind geeignete technische und organisatorische Maßnahmen zur Risikominimierung als Mindeststandard bereits im Gesetz festzulegen.

Fazit

Die DSK hat mit ihren aktuellen Entschließungen erneut belegt, dass eine im öffentlichen Interesse liegende Nutzung von Gesundheitsdaten unter Wahrung eines hohen Datenschutzniveaus möglich ist, sofern Bund und Länder die erforderlichen rechtlichen Rahmenbedingungen schaffen.

Digitale Souveränität: Ein lohnenswertes datenschutzpolitisches Ziel I.8

Zu Recht hat die Strategie der digitalen Souveränität in die politische Agenda im Bund und auch in Niedersachsen Einzug gehalten. Ein Positionspapier der Datenschutzkonferenz formuliert die wesentlichen Kriterien für digital souveräne IT-Lösungen und hilft bei Produktentscheidungen und in Beschaffungsprozessen.

Die Datenschutzaufsicht in Niedersachsen hat sich bereits früh damit befasst, wie man datenschutzfreundliche IT-Architekturen mit typischen Merkmalen digitaler Souveränität fördert. Bereits im Jahr 2020 hat dann die Datenschutzkonferenz (DSK) eine Entschließung zu dem Thema veröffentlicht.[1] Diese hat die Anforderungen und Kriterien für digital souveräne IT-Lösungen weitgehend abstrakt entlang der Kernforderungen nach Transparenz, Wechselmöglichkeiten, Gestaltungsmöglichkeiten und des angemessenen Einflusses auf die Anbieter ausgerichtet. Um diesen allgemeinen Appell zu vertiefen und praxisnah auszugestalten, hat die DSK 2021 eine Task Force „Digitale Souveränität" unter der Federführung des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI) eingerichtet, in der auch unsere Behörde aktiv mitgewirkt hat.

Im Jahr 2023 hat die DSK ein Positionspapier zu den Kriterien für souveräne Clouds erarbeitet und veröffentlicht.[2] Mit diesem Positionspapier liegt nunmehr ein praxisnaher Katalog konkreter Prüfpunkte zur Beurteilung einer IT-Lösung oder Cloud-Dienstleistung vor.

Die Kriterien werden in Muss- und Soll-Kriterien abgestuft und umfassen unter anderem so zentrale Aspekte wie eine herstellerunabhängige Modularität, offene Standards und Schnittstellen sowie insbesondere die Frage des Standortes eines Cloud-Dienstleisters.

1 DSK-Entschließung „Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen", September 2020, Kurzlink: https://t1p.de/dsk-souv (PDF).

2 DSK-Entschließung „Kriterien für Souveräne Clouds", Mai 2023, abrufbar unter https://lfd.niedersachsen.de/229590.html

Wir befinden uns in einer Situation, in der der Markt von einigen wenigen großen Cloud-Anbietern wie Google, IBM, Amazon und Microsoft – sogenannten Hyperscalern – beherrscht wird und damit die eigene digitale Souveränität nicht gewährleistet werden kann.

Das kann insbesondere im öffentlichen Bereich fatal sein: Menschen müssen darauf vertrauen können, dass ihre personenbezogenen Daten beim Staat sicher sind und in Übereinstimmung mit den Anforderungen des Datenschutzrechts verarbeitet werden. Das muss der Staat garantieren – und diese Garantie kann nur dann wirksam und glaubwürdig abgegeben werden, wenn die staatliche Stelle selbst die Souveränität über die von ihr verarbeiteten Daten innehat.

Fazit

Die digitale Souveränität bietet einen strategischen Mehrwert, um nachhaltig die IT-Lösungen für die öffentliche Verwaltung datenschutzkonform betreiben zu können und damit Rechtsstaatlichkeit auch in der digitalen Welt zu sichern.

Wir haben die Kriterien für souveräne Clouds dem niedersächsischen IT-Planungsrat zur Kenntnis gegeben. Es bleibt zu hoffen, dass der IT-Planungsrat in seiner beratenden Rolle für die Landesregierung die Bedeutung der digitalen Souveränität als staatliches Ziel noch deutlicher in den Fokus rückt.

OZG 2.0: Update für das Onlinezugangsgesetz I.9

Das Änderungsgesetz zum Onlinezugangsgesetz tritt voraussichtlich im Lauf des Jahres 2024 in Kraft. Es soll unter anderem für Onlinedienste der Verwaltung die nötigen Rechtsgrundlagen bei der länderübergreifenden Verarbeitung personenbezogener Daten schaffen. Die niedersächsische Datenschutzbehörde berät verschiedene Verantwortliche zur Rechtslage nach Inkrafttreten des Änderungsgesetzes.

Neben der Beratung rund um das Änderungsgesetz zum Onlinezugangsgesetz in unserem direkten Zuständigkeitsbereich ist unsere Behörde Mitglied der Kontaktgruppe der Datenschutzkonferenz „OZG 2.0", die in der Vergangenheit das Bundesministerium des Inneren und für Heimat im Rahmen des Gesetzgebungsverfahrens beraten hat und auch im Jahr 2023 mehrere Stellungnahmen zu den jeweils aktuellen Gesetzesentwürfen verfasst hat.

Der zum Zeitpunkt des Redaktionsschlusses aktuelle Gesetzesentwurf datiert vom 23. Februar 2024.[1] Er umfasst in Artikel 1 die geplanten Änderungen des Onlinezugangsgesetzes (OZG-E) und in Artikel 2 die geplanten Änderungen des E-Government-Gesetzes (EGovG-E).[2]

Datenschutzrechtliche Änderungen

Das Änderungsgesetz beschäftigt sich in mehreren Bereichen mit dem Datenschutz bei behördlichen Online-Dienstleistungen. Eine Herausforderung ist beispielsweise der „Einer für alle"-Ansatz (EfA), wonach jeweils eine Stelle einen Dienst entwickeln und danach länderübergreifend anderen Stellen zur Verfügung stellen soll.[3] Mit dem OZG-Änderungsgesetz wird die einen EfA-Online-Dienst betreibende Behörde Verantwortlicher

1 BT-Drs. 20/10417: https://dserver.bundestag.de/btd/20/104/2010417.pdf (PDF).
2 Die Artikel 3 bis 9 des OZG-Änderungsgesetzes behandeln die geplanten Änderungen weiterer Gesetze, auf die hier jedoch nicht näher eingegangen wird.
3 Siehe hierzu Kapitel I.10.

für die Verarbeitung personenbezogener Daten[4] im Rahmen des Onlinedienstes.[5] Diese Behörde erhält auch eine spezielle Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen des Onlinedienstes.[6] Außerdem kommt eine weitere Rechtsgrundlage für die Zwischenspeicherung der Vorgänge[7] im Onlinedienst hinzu. Die reguläre Speicherdauer beträgt 30 Tage nach der letzten Bearbeitung[8], wobei der Ausnahmetatbestand, der eine längere Speicherdauer zulässt, derzeit aus unserer Sicht leider zu viel Raum für Interpretation lässt.

Dezentrale Bürgerkonten wie das Servicekonto Niedersachsen[9] werden nach Ablauf einer Übergangszeit von drei Jahren[10] durch ein zentrales Bürgerkonto, die Bund-ID, abgelöst.[11] Datenschutzrechtlich verantwortlich für die Verarbeitung personenbezogener Daten im Bürgerkonto ist die für das Konto zuständige Stelle.[12] Welche das sein wird, wird durch eine Rechtsverordnung bestimmt.[13]

Eine komplexe Rechtslage

Bei einem weitgehend digitalisierten Verwaltungsvorgang (Reifegrad 4 nach dem Modell des IT-Planungsrats[14]), geschieht nicht nur die Abwicklung des Antrages auf elektronischem Weg, sondern auch der Abruf der erforderlichen Nachweise (Once-Only-Nachweisabruf[15]). Dabei ist festzustellen, dass sich die hierfür erforderlichen Rechtsgrundlagen der Verarbeitung nicht nur im OZG-E, sondern auch in weiteren Gesetzen und Gesetzesentwürfen finden.

Während das OZG-E die Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten in einem elektronischen Antragsformular beschreibt,

4 Gemäß Art. 4 Abs. 7 DSGVO.
5 § 8a Abs. 4 OZG-E.
6 § 8a Abs. 1 OZG-E.
7 § 8a Abs. 2 OZG-E.
8 § 8a Abs. 3 OZG-E.
9 Erreichbar unter https://servicekonto.niedersachsen.de/Start/
10 § 13 Abs. 1 OZG-E
11 § 3 Abs. 1 OZG-E.
12 § 8 Abs. 6 OZG-E.
13 § 3 Abs. 1 Satz 3 OZG-E.
14 OZG-Reifegradmodell, Kurzlink: https://t1p.de/planungsrat (PDF).
15 Siehe hierzu den Tätigkeitsbericht 2021, G.8.

regelt das EGovG-E den Nachweisabruf. Als weiteres Puzzle-Teil behandelt das am 31. August 2023 in Kraft getretene ID-Nummerngesetz[16] den hierzu zuvor erforderlichen Abruf der zentralen ID-Nummer beim Bundesverwaltungsamt (BVA). Weiterer Regelungsbedarf dürfte sich ferner auf der Länderebene ergeben.

Die Bund-ID soll dezentrale Bürgerkonten in Zukunft ablösen.

Fazit

Was künftig aus Sicht des Bürgers mit ein paar Klicks funktionieren soll, ist im föderalen Kontext rechtlich gar nicht so einfach abzubilden. Wir erwarten dennoch eine zügige Umsetzung des lange überfälligen Gesetzgebungsvorhabens, um die erforderlichen Regelungen wirksam werden zu lassen und die Bürgerinnen und Bürger sowohl von Behördengängen zu entlasten als auch die notwendige Transparenz und Datenschutzkonformität des behördlichen Handelns herzustellen.

16 Siehe auch das Kapitel I.10.

I.10 Registermodernisierung: „Once Only“ rückt immer näher

Im Jahr 2023 haben wir unser Engagement im Projekt „Gesamtsteuerung Registermodernisierung“ im Auftrag der Datenschutzkonferenz fortgesetzt und unsere beratende Funktion in diversen Projektgremien wahrgenommen.

Bei den Projekten zur Umsetzung des Onlinezugangsgesetzes (OZG) gestalten die zuständigen Behörden und IT-Dienstleister den für die Bürgerinnen und Bürger sichtbaren Teil von digitalen Verwaltungsportalen, das Front-End. Im Unterschied dazu befasst sich die Registermodernisierung mit dem Back-End, den dahinter liegenden Registern, in denen der Staat Daten wie zum Beispiel Geburtsurkunden oder Adressnachweise speichert. In diese Register und die dort stattfindende Verarbeitung haben die Bürgerinnen und Bürger in der Regel keinen Einblick. Umso wichtiger ist es, die Transparenz über die Verarbeitung personenbezogener Daten auch „im Hintergrund“ herzustellen.

Erprobungsprojekte im Rahmen der Registermodernisierung

Die Datenschutzkonferenz (DSK) hat der niedersächsischen Datenschutzaufsicht das Mandat erteilt, sie im Projekt „Gesamtsteuerung Registermodernisierung“ zu vertreten.[1] Im Rahmen dieses Projekts haben wir uns 2023 unter anderem mit diversen Erprobungsprojekten beschäftigt.

Mit diesen Projekten wollen die Projektbeteiligten testen, wie bestimmte Komponenten und Funktionen des künftigen NOOTS (National Once Only Technical Systems) miteinander interagieren. Über das NOOTS soll der sichere Austausch von Nachweisen, die für ein Verwaltungsverfahren erforderlich sind (z. B. Geburtsurkunden) erfolgen. Denn die Registermodernisierung führt das Once-Only-Prinzip ein: Die Bürgerin oder der Bürger soll beim Kontakt mit den Ämtern und Behörden ihre oder seine Nachweise nicht jedes Mal neu vorlegen müssen. Wiederholt haben wir in diesem Zusammenhang darauf aufmerksam gemacht, dass es auch für die Pilotie-

1 Siehe hierzu auch Tätigkeitsbericht 2022, Kapitel E.7 und Tätigkeitsbericht 2021, Kapitel G.8.

rung oder Erprobung unter Verarbeitung personenbezogener Daten einer Rechtsgrundlage für die Verarbeitung bedarf.

Die Projektgremien haben uns zu diversen datenschutzrechtlichen Aspekten in Zusammenhang mit dem NOOTS konsultiert. Dabei legten wir drei wesentliche Leitplanken zugrunde:

- Transparenz: Bürgerinnen und Bürger müssen jederzeit über die Verarbeitung ihrer Daten durch Behörden informiert sein;
- Willenselement: Bürgerinnen und Bürger haben die Wahl, die für das Verwaltungsverfahren erforderlichen Nachweise selbst an die jeweilige Stelle zu schicken oder sie bei einer anderen Stelle abrufen zu lassen; für Letzteres müssen sie ihren Wunsch bekunden (z. B. durch das Anklicken eines entsprechenden Buttons);
- Faktische Verarbeitungshemmnisse: Stellen, die keine Berechtigung zum Datenzugriff haben, dürfen auch tatsächlich keinen Zugriff erhalten; dies ist durch Implementierung technischer Vorkehrungen sicherzustellen.

Startschuss für zentrale Identifikationsnummer

Am 31. August 2023 ist das Identifikationsnummerngesetz (IDNrG)[2] in Kraft getreten.[3] Spätestens dieser Zeitpunkt war als Startschuss für die registerführenden Stellen zur Vorbereitung der Ersteinspeicherung der zentralen Identifikationsnummer in die Register zu sehen. Die Verwendung der Identifikationsnummer durch die Behörden erfordert unter anderem ein funktionierendes Datenschutzcockpit.

So sind die registerführenden Stellen nun in der Pflicht, natürlichen Personen die Übermittlung ihrer Daten unter Verwendung der Identifikationsnummer digital über eine zentrale Stelle (Datenschutzcockpit) transparent zu machen.[4]

Das betrifft nach Ansicht der Aufsichtsbehörden auch die Ersteinspeicherung der Identifikationsnummer in die Register. Allerdings ist beispielsweise die Rechtsverordnung, die den Betreiber des Datenschutzcockpits fest-

2 IDNrG vom 28. März 2021 (BGBl. I S. 591; 2023 I Nr. 230), das durch Art. 15 des Gesetzes vom 28. Juni 2021 (BGBl. I S. 2250; 2023 I Nr. 230) geändert worden ist.
3 BGBl. Teil I, 2023, Nr. 230, Kurzlink: https://t1p.de/registermodernisierung (PDF).
4 § 2 Nr. 3 IDNrG.

legt[5], zum Zeitpunkt des Redaktionsschlusses noch nicht in Kraft getreten. Daher ist bei der Vorbereitung und der Koordination der Ersteinspeicherung – auch bereits ohne diese Rechtsverordnung – darauf zu achten, dass vor der Verarbeitung der Identifikationsnummer auch die formalen Anforderungen erfüllt sind.

Ende 2023 hat das Niedersächsische Ministerium für Inneres und Sport ein Registermodernisierungsprojekt auf Landesebene ins Leben gerufen. Auch hier stehen wir bei Bedarf beratend zur Verfügung.

Fazit

Die Registermodernisierung wird immer konkreter, der Once-Only-Nachweisabruf rückt immer näher. Wir werden im Rahmen der Umsetzung der Registermodernisierung weiterhin beratend und begleitend tätig sein.

5 § 10 Abs. 5 S. 1 OZG, Onlinezugangsgesetz vom 14. August 2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 16 des Gesetzes vom 28. Juni 2021 (BGBl. I S. 2250; 2023 I Nr. 230) geändert worden ist.

Weitere Verfahrensregeln zur DSGVO geplant I.11

Im Juli 2023 legte die Europäische Kommission einen Vorschlag für eine Verordnung vor, um die Zusammenarbeit der europäischen Datenschutzaufsichtsbehörden zu verbessern und bestimmte Aspekte des Verfahrens zu harmonisieren. Unsere Behörde hat sich 2023 intensiv mit diesem Verordnungsentwurf befasst und eine Arbeitsgruppe der Datenschutzkonferenz geleitet, die eine Stellungnahme dazu erarbeitet hat.

Die europäischen Datenschutzaufsichtsbehörden arbeiten bei grenzüberschreitenden Datenverarbeitungen im Kooperationsverfahren[1] zusammen.[2] Dabei übernimmt die Aufsichtsbehörde, in deren Zuständigkeitsbereich sich die Hauptniederlassung oder einzige Niederlassung des Verantwortlichen oder des Auftragsverarbeiters befindet, die Rolle der federführenden Aufsichtsbehörde und arbeitet mit den betroffenen Aufsichtsbehörden zusammen.

Die federführende Aufsichtsbehörde wendet bei der Fallbearbeitung ihr jeweiliges nationales (Verwaltungs-)Verfahrensrecht an. Nachdem insbesondere die lange Dauer der Verfahren grenzüberschreitender Datenverarbeitungen in der Kritik stand, hat der Europäische Datenschutzausschuss (EDSA)[3] eine Liste von Verfahrensregeln aufgestellt, die europaweit harmonisiert werden sollten, um die Zusammenarbeit der Aufsichtsbehörden zu verbessern. Die Europäische Kommission hat in ihrem Vorschlag wesentliche vom EDSA in dieser „Wunschliste" formulierten Anregungen aufgegriffen.

Zwei neue Verfahrensschritte im Kooperationsverfahren

Um die Zusammenarbeit der Aufsichtsbehörden im Kooperationsverfahren zu verbessern, sind im Vorschlag zwei neue Verfahrensschritte vorgesehen.

1 Gemäß Art. 60 DSGVO.
2 Zur Zusammenarbeit der europäischen Aufsichtsbehörden siehe Tätigkeitsbericht 2019, C.1.
3 Zur Arbeit des EDSA und dessen Aufgaben siehe Tätigkeitsbericht 2019, C.2.

Zunächst soll die federführende Aufsichtsbehörde verpflichtet werden, den betroffenen Aufsichtsbehörden eine „Zusammenfassung der wichtigsten Aspekte" der Untersuchung zur Verfügung zu stellen. In diesem Dokument soll die Behörde insbesondere die wichtigsten maßgeblichen Fakten, eine vorläufige Ermittlung des Umfangs der Untersuchung und eine erste Feststellung möglicher Korrekturmaßnahmen zusammenfassen.

Falls die federführende Aufsichtsbehörde beabsichtigt, im weiteren Kooperationsverfahren einen Verstoß gegen die DSGVO festzustellen, soll sie verpflichtet werden, „vorläufige Feststellungen" vorzulegen. Diese sollen insbesondere „umfassende und hinreichend klar dargelegte Anschuldigungen" sowie die Abhilfemaßnahmen beinhalten, welche die federführende Aufsichtsbehörde zu ergreifen beabsichtigt.

DSK-Stellungnahme zum Verordnungsentwurf

Der Landesbeauftragte für den Datenschutz Niedersachsen leitete ab Mitte Juli 2023 eine Arbeitsgruppe der Datenschutzkonferenz (DSK), die eine Stellungnahme zu dem Verordnungsentwurf erarbeitet hat.[4] Die DSK begrüßt in ihrer Stellungnahme grundsätzlich, dass die Europäische Kommission wesentliche Anregungen der „Wunschliste" aufgegriffen hat.

Der Entwurf greift tief in bewährte und positive Aspekte der Zusammenarbeit der europäischen Aufsichtsbehörden ein.

Zugleich weist die DSK darauf hin, dass der Verordnungsentwurf deutlich darüber hinaus geht und tief in bewährte und positive Aspekte der Zusammenarbeit der europäischen Aufsichtsbehörden eingreift. Insbesondere problematisiert die DSK, dass mit den vorgesehenen neuen Regelungen die Rechte der europäischen Aufsichtsbehörden einseitig zugunsten der federführenden Aufsichtsbehörde verschoben werden würden. Zudem sollte aus Sicht der DSK in der Verfahrensverordnung die Zielsetzung des Kooperationsverfahrens, die in der Konsensfindung zwischen den Aufsichtsbehörden besteht, an erster Stelle stehen.

4 Abrufbar unter https://datenschutzkonferenz-online.de/stellungnahmen.html

Stellungnahme des EDSA und des Europäischen Datenschutzbeauftragten

Darüber hinaus arbeitete unsere Behörde auf europäischer Ebene an der Entwicklung einer gemeinsamen Stellungnahme des EDSA und des Europäischen Datenschutzbeauftragten zum Verordnungsentwurf mit.[5] Darin wird ebenfalls begrüßt, dass der Vorschlag die wirksame Durchsetzung der Datenschutzvorschriften fördern soll und viele der Vorschläge in der EDSA-„Wunschliste" umsetzt.

Allerdings weist die Stellungnahme darauf hin, dass der Vorschlag eine unangemessene Einschränkung der Bestimmung des Begriffs „maßgeblicher und begründeter Einspruch" enthält. Es sollte für die betroffenen Aufsichtsbehörden weiterhin möglich sein, maßgebliche und begründete Einsprüche gegen den Umfang der Untersuchung einzulegen. Zudem weisen die Autoren der Stellungnahme darauf hin, dass zur Gewährleistung einer raschen und effizienten Durchsetzung eine strengere Regelung gewisser Verfahrensschritte, einschließlich Fristen, erforderlich wäre.

Gesetzgebungsverfahren läuft noch

Seit Herbst 2023 wird der Vorschlag im Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlamentes und in einer Arbeitsgruppe des Europäischen Rates intensiv beraten. Das Gesetzgebungsverfahren wird allerdings voraussichtlich erst nach den Europawahlen 2024 abgeschlossen werden können.

5 EDSA-EDSB, Gemeinsame Stellungnahme 01/2023, Kurzlink: https://t1p.de/edsa-edsb

J Europäischer Datenschutzausschuss

J.1 Berechnung von Bußgeldern – Leitlinien des Europäischen Datenschutzausschusses

Am 24. Mai 2023 hat der Europäische Datenschutzausschuss die Leitlinien 04/2022 über die Berechnung von Geldbußen nach der Datenschutz-Grundverordnung angenommen. Anhand der Leitlinien berechnen die Aufsichtsbehörden Geldbußen wegen Datenschutzverstößen im gesamten Europäischen Wirtschaftsraum einheitlich.

Die Leitlinien ersetzen verschiedene frühere nationale Bußgeldkonzepte, einschließlich des Konzepts der deutschen Datenschutzkonferenz (DSK). Anwendungsbereich und grundlegende Berechnungsmethode der Leitlinien 04/2022 haben sich im Vergleich zum Entwurf aus dem Jahr 2022 nicht geändert.[1]

Nach der Annahme der finalen Fassung (aktuell Version 2.1) durch den Europäischen Datenschutzausschuss (EDSA) werden Geldbußen von den Aufsichtsbehörden grundsätzlich nach den Leitlinien zugemessen.

Berechnungsmethode

Das Standardmodell für die Berechnung sieht weiterhin fünf Schritte vor:

1. Klärung von Konkurrenzen
2. Ermittlung eines Ausgangsbetrags
3. Berücksichtigung weiterer erschwerender oder mildernder Umstände
4. Prüfung des ermittelten Betrages am gesetzlichen Höchstbetrag
5. Prüfung auf Wirksamkeit, Verhältnismäßigkeit und Abschreckungseffekt der Geldbuße

In diesem Beitrag werden insbesondere die Änderungen zur Konsultationsfassung behandelt. Ausführungen zu den einzelnen Schritten können dem vorangegangenen Tätigkeitsbericht[1] entnommen werden.

1 Siehe Tätigkeitsbericht 2022, C.2, S. 17 ff.

Neue Rechenfaktoren und Tabellen für Ausgangsbeträge

Während die Konsultationsfassung der Leitlinien noch starre Rechenfaktoren für jede Größenklasse vorsah, enthält die finale Fassung unterschiedlich breite Spannen, um sowohl den individuellen Gegebenheiten der Unternehmen als auch den konkreten Verstößen im Einzelfall möglichst umfassend Rechnung tragen zu können. Die Untergrenzen der Korridore fallen meist niedriger und die Obergrenzen höher aus als in der Konsultationsfassung. Je umsatzschwächer ein Unternehmen ist, desto niedriger soll dabei der Rechenfaktor und desto stärker die Reduzierung des individuellen Bußgeldkorridors sein.

Bei Verstößen im niedrigeren Bußgeldrahmen[2] ergibt sich folgende Tabelle:

Umsatz im Vorjahr	Rechenfaktor	Verstoß „niedrig“	Verstoß „mittel“	Verstoß „hoch“
Bis 2 Mio. €	0,2 % bis 0,4 %	Über 0 bis 4.000 €	2.000 bis 8.000 €	4.000 bis 40.000 €
Über 2 Mio. bis 10 Mio. €	0,3 % bis 2,0 %	Über 0 bis 20.000 €	3.000 bis 40.000 €	6.000 bis 200.000 €
Über 10 Mio. bis 50 Mio. €	1,5 % bis 10 %	Über 0 bis 100.000 €	15.000 bis 200.000 €	30.000 bis 1.000.000 €
Über 50 Mio. bis 100 Mio. €	8,0 % bis 20 %	Über 0 bis 200.000 €	80.000 bis 400.000 €	160.000 bis 2.000.000 €
Über 100 Mio. bis 250 Mio. €	15 % bis 50 %	Über 0 bis 500.000 €	150.000 bis 1.000.000 €	300.000 bis 5.000.000 €
Über 250 Mio. bis 500 Mio. €	40 % bis 100 %	Über 0 bis 1.000.000 €	400.000 bis 2.000.000 €	800.000 bis 10.000.000 €
Über 500 Mio. €	–	Über 0 bis 0,2 % des Umsatzes	0,2 % bis 0,4 % des Umsatzes	0,4 % bis 2,0 % des Umsatzes

2 Art. 83 Abs. 4 DSGVO.

Bei Verstößen im höheren Bußgeldrahmen[3] ergibt sich folgende Tabelle:

Umsatz im Vorjahr	Rechen-faktor	Verstoß „niedrig“	Verstoß „mittel“	Verstoß „hoch“
Bis 2 Mio. €	0,2 % bis 0,4 %	Über 0 bis 8.000 €	4.000 bis 16.000 €	8.000 bis 80.000 €
Über 2 Mio. bis 10 Mio. €	0,3 % bis 2,0 %	Über 0 bis 40.000 €	6.000 bis 80.000 €	12.000 bis 400.000 €
Über 10 Mio. bis 50 Mio. €	1,5 % bis 10 %	Über 0 bis 200.000 €	30.000 bis 400.000 €	60.000 bis 2.000.000 €
Über 50 Mio. bis 100 Mio. €	8,0 bis 20 %	Über 0 bis 400.000 €	160.000 bis 800.000 €	320.000 bis 4.000.000 €
Über 100 Mio. bis 250 Mio. €	15 % bis 50 %	Über 0 bis 1.000.000 €	300.000 bis 2.000.000 €	600.000 bis 10.000.000 €
Über 250 Mio. bis 500 Mio. €	40 % bis 100 %	Über 0 bis 2.000.000 €	800.000 bis 4.000.000 €	1.600.000 bis 20.000.000 €
Über 500 Mio. €	–	Über 0 bis 0,4 % des Umsatzes	0,4 % bis 0,8 % des Umsatzes	0,8 % bis 4,0 % des Umsatzes

Die vorstehenden Tabellen sind komprimierte Fassungen der Tabellen im Annex der Leitlinien[4], ergänzt um die ungeschriebene Größenklasse 7 mit einem Umsatz von über 500 Millionen Euro.

In der finalen Fassung überlappen sich die Größenklassen horizontal – also zwischen den Schweregraden – teilweise erheblich. Vertikale Überlappungen – also Überschneidungen der Umsatzspannen der Größenklassen – sind hingegen nicht vorgesehen. Es ist Aufgabe der Behörden, insbesondere für Unternehmen an den unteren und oberen Rändern der Umsatzspannen im Einzelfall angemessene Rechenfaktoren anzuwenden.

3 Art. 83 Abs. 5 und 6 DSGVO.

4 EDSA-Leitlinien 04/2022, Version 2.1, Annex (ab S. 44, englische Fassung; ab S. 47, deutsche Fassung), Kurzlink: https://t1p.de/eu-bussgeld

Die neuen Rechenfaktoren begünstigen, dass die ermittelten Bußgeldhöhen den Ansprüchen der DSGVO genügen[5], also wirksam, verhältnismäßig und abschreckend sind.

Einordnung und Flexibilität

Die finalen Leitlinien weisen durch die Überlappungen der Bußgeldkorridore gegenüber der Konsultationsfassung eine deutlich gesteigerte Flexibilität für die Aufsichtsbehörden auf. Der EDSA ist sich allerdings bewusst, dass selbst diese zusätzliche Flexibilität im Einzelfall nicht ausreichen könnte. In die finale Fassung wurden daher zwei weitere Instrumente übernommen.

Die Leitlinien stellen in Randnummer 47 klar, dass ein Ausgangsbetrag die Behörden nicht daran hindern soll, die Geldbuße herabzusetzen oder zu erhöhen, wenn die Umstände es erfordern. Dies kann insbesondere sinnvoll sein, wenn der eröffnete Korridor nicht ausreichend erscheint.

In den Randnummern 18 bis 20 räumen die Leitlinien die Möglichkeit ein, Geldbußen mit Pauschalbeträgen („fixed amounts") festzusetzen. Zwar suggeriert der Terminus, dass es sich um einen statischen Bußgeldkatalog handeln könnte. Um mit dem hergebrachten europäischen und nationalen Recht kompatibel zu sein, kann es sich indes nur um Sockel-Beträge handeln, welche die Basis für die weitere Zumessung darstellen würden. Ausgangspunkt für die Berechnung wäre dann nicht notwendigerweise der Umsatz eines Unternehmens, sondern ein für den bestimmten Verstoß im Vorhinein festgelegter Sockel-Betrag. Die Festlegung solcher Sockel-Beträge entbindet nicht davon, Artikel 83 der DSGVO vollumfänglich anzuwenden und die im Einzelfall maßgeblichen Zumessungskriterien zu beachten. So kann auch nachgelagert noch eine Umsatzkomponente berücksichtigt werden.

5 Art. 83, Abs. 1 DSGVO.

J.2 Verhaltensbezogene Werbung bei Meta – Dringlichkeitsverfahren durchgeführt

Auch im Jahr 2023 befasste sich der Europäische Datenschutzausschuss mit der Zulässigkeit der Verarbeitung personenbezogener Daten zum Zweck der verhaltensbezogenen Werbung. Er führte zu diesem Thema gegenüber Meta ein Dringlichkeitsverfahren durch, an dem der Landesbeauftragte für den Datenschutz Niedersachsen im Rahmen der Ländervertretung in der Enforcement Subgroup des EDSA mitarbeitete.

Meta verarbeitet beim Betrieb seiner Plattformen Facebook und Instagram eine Vielzahl personenbezogener Daten zum Zweck der verhaltensbezogenen Werbung. Dabei erstellt Meta detaillierte Profile seiner Nutzer, um für seine Werbekunden möglichst passgenaue Anzeigen schalten zu können. Mit dieser Art von Werbung lassen sich höhere Umsätze als mit klassischer ungezielter oder kontextbasierter Werbung erwirtschaften.

Bereits Ende 2022 hatte der Europäische Datenschutzausschuss (EDSA) in zwei Streitbeilegungsverfahren klargestellt, dass Datenverarbeitungen zum Zwecke der verhaltensbezogenen Werbung nicht erforderlich sind, um gemäß Artikel 6 Absatz 1 Buchstabe b der DSGVO vertragliche Verpflichtungen gegenüber den Nutzern zu erfüllen. Die irische Datenschutzaufsichtsbehörde (DPC) hatte daraufhin Meta unter anderem angewiesen, die betreffenden Datenverarbeitungen nicht mehr auf die Rechtsgrundlage der Vertragserfüllung zu stützen und mit den Anforderungen der Datenschutz-Grundverordnung (DSGVO) in Einklang zu bringen. Zudem wurden Geldbußen in dreistelliger Millionenhöhe gegen Meta verhängt.[1]

Berechtigte Interessen keine anwendbare Rechtsgrundlage

Meta hatte zunächst beabsichtigt, diese Datenverarbeitungen zum Zwecke der verhaltensbezogenen Werbung fortan auf die Wahrung berechtigter Interessen zu stützen, also auf Artikel 6 Absatz 1 Buchstabe f der DSGVO. Der Europäische Gerichtshof entschied allerdings mit Urteil vom

1 Siehe Tätigkeitsbericht 2022, C.4.

4. Juli 2023, dass solche Datenverarbeitungen nur dann als zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich angesehen werden können, wenn diese Verarbeitung innerhalb der Grenzen dessen erfolgt, was zur Verwirklichung dieses berechtigten Interesses absolut notwendig ist.[2] Darauf kündigte Meta an, auf eine Einwilligungslösung umzuschwenken. Die von der DPC gesetzte Frist, die Datenverarbeitungen in Einklang mit den Anforderungen der DSGVO zu bringen, ließ Meta jedoch verstreichen.

Dringlichkeitsverfahren aus Norwegen

Vor diesem Hintergrund hat die norwegische Datenschutzbehörde am 14. Juli 2023 gegenüber Meta in einem Dringlichkeitsverfahren gemäß DSGVO[3] ein auf drei Monate befristetes Verbot der Verarbeitung personenbezogener Daten Betroffener zum Zwecke der verhaltensbezogenen Werbung, die sich auf die Erfüllung vertraglicher Verpflichtungen oder die Wahrung berechtigter Interessen[4] stützt, ausgesprochen. Die Reichweite dieses Verbots war auf Norwegen beschränkt.

Nachdem die norwegische Aufsichtsbehörde im Anschluss beantragt hatte, dass dringend endgültige Maßnahmen gemäß DSGVO[5] erlassen werden müssen, führte der EDSA ein Dringlichkeitsverfahren durch, an dem unsere Behörde intensiv mitarbeitete, und erließ am 10. November 2023 einen verbindlichen Beschluss.

In diesem Beschluss kam der EDSA zu dem Ergebnis, dass Meta weiterhin gegen die DSGVO verstieß, weil das Unternehmen die Verarbeitung personenbezogener Daten immer noch auf Artikel 6 Absatz 1 Buchstaben b und f der DSGVO stützte.[6] Der EDSA verpflichtete die DPC daher, Meta die darauf begründete Verarbeitung personenbezogener Daten zum Zwecke der verhaltensbezogenen Werbung ohne zeitliche Befristung im gesamten Europäischen Wirtschaftsraum zu verbieten.

2 EuGH, Urteil vom 4. Juli 2023 – Rs. C-252/21, ECLI:EU:C:2023:537.
3 Gemäß Art. 66 Abs. 1 DSGVO.
4 Gemäß Art. 6 Abs. 1 Buchst. b oder f DSGVO.
5 Art. 66 Abs. 2 DSGVO.
6 Kurzlink: https://t1p.de/edsa-meta2

Als Antwort führt Meta ein Bezahlmodell ein

Noch bevor die DPC diesen Beschluss des EDSA umsetzte, begann Meta damit, das sogenannte „Pay or Okay"-Modell einzuführen. Bei diesem Modell sollen sich die Nutzenden von Facebook und Instagram entscheiden, ob sie zwischen rund 10 und 13 Euro pro Monat für die Nutzung der Dienste ohne verhaltensbezogene Werbung zahlen oder stattdessen in die Nutzung ihrer personenbezogenen Daten zum Zwecke der verhaltensbezogenen Werbung einwilligen.[7]

Eine Nichtregierungsorganisation machte geltend, dieses Geschäftsmodell sei rechtswidrig, weil es eine Art Datenschutzgebühr einführe. Zudem sei die Höhe der von Meta verlangten Abo-Gebühr unangemessen. Die europäischen Datenschutzbehörden prüfen aktuell die Rechtmäßigkeit von „Pay or Okay"-Modellen, eine Entscheidung stand zum Redaktionsschluss dieses Tätigkeitsberichts noch aus.[8]

7 Gemäß Art. 6 Abs. 1 Buchst. a DSGVO.

8 Vgl. zu Abo-Modellen von Zeitungsverlagen und sonstigen Medien Kapitel I.5.

Hohe Bußgelder für TikTok und Meta nach Streitbeilegungsverfahren vor dem EDSA J.3

Der Landesbeauftragte für den Datenschutz Niedersachsen hat im Jahr 2023 an zwei Streitbeilegungsverfahren des Europäischen Datenschutzausschusses mitgearbeitet – an einem zu Meta und einem zu TikTok. Diese Verfahren sind erforderlich, wenn sich bei grenzüberschreitenden Datenverarbeitungen die federführende Aufsichtsbehörde und die betroffenen Aufsichtsbehörden im Kooperationsverfahren nicht auf das Ergebnis der Untersuchung einigen können.

In den Streitbeilegungsverfahren zu Meta und TikTok arbeitete die niedersächsische Datenschutzbehörde im Rahmen der Ländervertretung in der sogenannten Enforcement Subgroup des Europäischen Datenschutzausschusses (EDSA) mit. Da beide Unternehmen ihre Hauptniederlassung in Europa in Irland haben, ist die irische Aufsichtsbehörde (DPC) für sie zuständig.

Facebook: Datentransfer in die USA

Das erste Streitbeilegungsverfahren betraf einen Beschlussentwurf der DPC vom 6. Juli 2022 in Sachen Meta Platforms Ireland Limited. In diesem Beschlussentwurf hatte die DPC in Folge des Schrems-II-Urteils des Europäischen Gerichtshofs (EuGH)[1] festgestellt, dass die beim Betrieb des Facebook-Netzwerks stattfindenden Datenexporte in die USA auf der Grundlage von Standarddatenschutzklauseln gegen die Datenschutz-Grundverordnung (DSGVO) verstoßen[2] haben. Denn in den USA bestand zu diesem Zeitpunkt kein Datenschutzniveau, das dem in der Europäischen Union gleichwertig war. Daher verpflichtete die DPC Meta, nach einer Umsetzungsfrist von drei Monaten Datenexporte in die USA auszusetzen. Ein Bußgeld verhängte die irische Behörde jedoch nicht. Ebenso wenig ver-

1 Siehe Tätigkeitsbericht 2020, D.1.
2 Art. 46 Abs. 1 DSGVO.

pflichtete sie Meta, bereits in die USA exportierte personenbezogene Daten zu löschen.

Nachdem mehrere betroffene europäische Aufsichtsbehörden mittels maßgeblicher und begründeter Einsprüche unter anderem die Verhängung eines angemessenen Bußgeldes gefordert hatten, führte der EDSA im Frühjahr 2023 ein Streitbeilegungsverfahren gemäß Artikel 65 Absatz 1 Buchstabe a der DSGVO durch.

Als Ergebnis dieses Verfahrens legte der EDSA fest, dass ein Bußgeld erforderlich sei und der Ausgangspunkt für die Bußgeldberechnung zwischen 20 Prozent und 100 Prozent des gesetzlichen Höchstbetrags liegen sollte.[3] Daraufhin verhängte die DPC das höchste bisher unter der DSGVO ausgesprochene Bußgeld in Höhe von 1,2 Milliarden Euro gegen Meta. Zudem verpflichtete der EDSA die DPC, Meta anzuweisen, innerhalb einer Frist von sechs Monaten die unrechtmäßige Verarbeitung der unter Verstoß gegen die DSGVO in die USA exportierten personenbezogenen Daten europäischer Nutzerinnen und Nutzer einzustellen.

Die DPC verhängte mit 1,2 Milliarden Euro gegen Meta das höchste bisher unter der DSGVO ausgesprochene Bußgeld.

Meta hat gegen den verbindlichen Beschluss des EDSA Nichtigkeitsklage vor dem Gericht der Europäischen Union (EuG) eingereicht. Inzwischen ist der neue Angemessenheitsbeschluss der EU-Kommission nach dem Datenschutzrahmen EU-USA[4] in Kraft getreten. Dadurch ist Meta wieder berechtigt, personenbezogene Daten an zertifizierte Unternehmen und Organisationen in den USA übermitteln, ohne geeignete Garantien und zusätzliche Maßnahmen ergreifen oder sich auf spezielle Ausnahmetatbestände stützen zu müssen.

TikTok: Einsatz manipulativer Designs von Bedienoberflächen

Ausgangspunkt eines Verfahrens gegen die Videoplattform TikTok war eine Untersuchung der Rechtmäßigkeit der Verarbeitung personenbezoge-

3 Binding Decision 1/2023 on the dispute submitted by the Irish SA on data transfers by Meta Platforms Ireland Limited for its Facebook service (Art. 65 GDPR), Kurzlink: https://t1p.de/edsa-meta (PDF).

4 Siehe hierzu Kapitel G.10.

Aus Sicht des Europäischen Datenschutzausschusses hat TikTok manipulative Designs eingesetzt, damit sich Minderjährige für ein öffentliches Konto entscheiden (Symbolbild).

ner Daten von minderjährigen TikTok-Nutzenden durch die DPC. Die DPC stellte in ihrem Beschlussentwurf unter anderem fest, dass TikTok gegen die Grundsätze des Datenschutzes durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, der Datenminimierung und der Transparenz verstoßen hatte.

Nachdem betroffene Aufsichtsbehörden maßgebliche und begründete Einsprüche gegen diesen Beschlussentwurf der DPC eingelegt hatten, stellte der EDSA zusätzlich einen Verstoß gegen Artikel 5 Absatz 1 Buchstabe a DSGVO fest, weil TikTok so genannte Dark Patterns (manipulative Designs von Bedienoberflächen) eingesetzt hatte, um Minderjährige dazu zu bewegen, sich für ein öffentliches Konto zu entscheiden. Das hatte zur Folge, dass diese Konten für jedermann zugänglich waren. Folglich wies der EDSA die DPC an, in ihrer endgültigen Entscheidung diesen zusätzlichen Verstoß festzustellen und TikTok anzuweisen, diese Dark Patterns abzustellen.

Im Streitbeilegungsverfahren prüfte der EDSA zudem, ob die von TikTok zwischen dem 31. Juli und dem 31. Dezember 2020 durchgeführten Maßnahmen zur Altersüberprüfung der Nutzerinnen und Nutzer den Anforderungen der DSGVO[5] entsprachen. Der EDSA kam zu dem Ergebnis, dass er nicht über ausreichende Informationen verfügt, um diese Fragestellungen abschließend beurteilen zu können. Zugleich hatte der EDSA allerdings ernsthafte Zweifel an der Wirksamkeit der von TikTok durchgeführten Altersüberprüfung und forderte deshalb die DPC auf, dies in ihrer endgültigen Entscheidung zu berücksichtigen.

Gegen TikTok verhängte die DPC ein Bußgeld in Höhe von insgesamt 345 Millionen Euro.

In ihrem endgültigen Beschluss stellte die DPC wie vom EDSA vorgegeben den zusätzlichen Verstoß gegen Artikel 5 Absatz 1 Buchstabe a der DSGVO[6] fest und verhängte unter anderem ein Bußgeld in Höhe von insgesamt 345 Millionen Euro gegen TikTok.

5 Art. 25 Abs. 1 DSGVO.

6 Verarbeitung personenbezogener Daten „auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise", Art. 5 Abs. 1 Buchst. a DSGVO.

K Öffentlichkeitsarbeit

K.1 Informationsmaterial: Von Schule bis Verein

Es ist bisweilen gar nicht so einfach, im Datenschutz den Durchblick zu bekommen – oder zu behalten. Deshalb veröffentlichen wir regelmäßig FAQs, Infoblätter und Handreichungen zu aktuellen Datenschutzfragen auf unserer Homepage. Diese richten sich an Bürgerinnen und Bürger, Unternehmen, Behörden und Vereine.

Auf unserer Webseite lfd.niedersachsen.de finden Sie im Bereich Infothek nützliche Checklisten, Merkblätter und über 20 FAQs zu wichtigen Aspekten des Datenschutzes und seinen Anwendungsfeldern. In diesem Jahr sind unter anderem eine Handreichung für Vereine und ein Merkblatt für den Newsletterversand hinzugekommen.

Handreichung zum Datenschutz im Verein

https://lfd.niedersachsen.de/56043.html

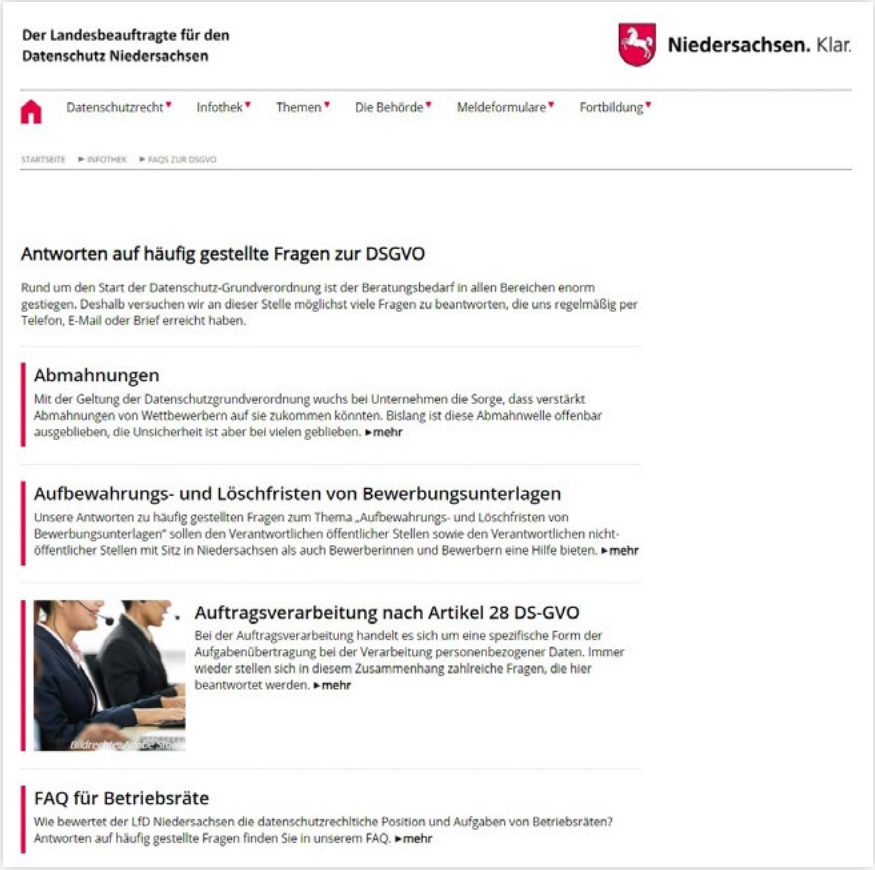
Insbesondere in ehrenamtlich geführten Vereinen fehlt es häufig an Zeit und Ressourcen, sich intensiver mit dem Datenschutz zu beschäftigen. Doch gerade Vereine müssen im Alltag viele personenbezogene Daten verarbeiten, darunter häufig auch besondere Kategorien wie Gesundheitsdaten oder Daten von Kindern und Jugendlichen. Auf 56 Seiten gehen wir in unserer Handreichung „Datenschutz im Verein" unter anderem auf Veröffentlichung von Fotos, den Einsatz von Social Media und die korrekte Meldung von Datenschutzverletzungen ein.

Mehr zum Datenschutz im Verein lesen Sie außerdem in diesem Tätigkeitsbericht in Kapitel G.9.

Merkblatt zum Versand von Newslettern

https://lfd.niedersachsen.de/228657.html

Uns erreichen regelmäßig Hinweise von Betroffenen, die sich über unerwünschte oder stark personalisierte Newsletter beschweren. Die wichtigsten Regeln zum korrekten Aufsetzen, Konfigurieren und Versenden von



Über 20 Datenschutz-FAQs von „Abmahnungen" bis „Website-Betreiber" finden Sie auf unserer Homepage.

Newslettern haben wir niedrigschwellig zusammengefasst und dazu ein kurzes Infoblatt erstellt.

Orientierungshilfe zu Videoüberwachung an Schulen

https://lfd.niedersachsen.de/download/201751/

Eine Videoüberwachung stellt einen besonders tiefen Eingriff in die Rechte der beobachteten und aufgezeichneten Personen dar. Das bedingt für den

Einsatz in Schulen besonders hohe Anforderungen. Unsere Orientierungshilfe zum Thema haben wir aktualisiert und bieten darin nützliche Hinweise, in welchen Fällen eine solche Überwachung an öffentlichen Schulen zulässig ist.

Mehr zur Videoüberwachung an Schulen lesen Sie außerdem in diesem Tätigkeitsbericht in Kapitel G.1.

Veröffentlichungen der Datenschutzkonferenz

Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) bietet auf Ihrer Homepage ebenfalls zahlreiche Tipps und Hinweise an. Unter anderem sind 2023 neu hinzugekommen:

- Anwendungshinweise zur Übermittlung personenbezogener Daten aus Europa an die USA[1]
- Hinweise zu Überwachungsaufgaben von Überwachungsstellen für Verhaltensregeln nach Artikel 40 DSGVO[2]
- Eine Bewertung von Pur-Abo-Modellen auf Websites[3]

Sollten Sie zu einem bestimmten datenschutzrechtlichen Thema bei uns oder auf der Seite der DSK kein Material finden, schreiben Sie uns gerne über poststelle@lfd.niedersachsen.de an.

1 DSK: Anwendungshinweise zur Übermittlung personenbezogener Daten aus Europa an die USA; Kurzlink: https://t1p.de/dsk-eu-usa (PDF).
2 DSK: Hinweise zu Überwachungsaufgaben von Überwachungsstellen für Verhaltensregeln nach Artikel 40 DSGVO; Kurzlink: https://t1p.de/dsk-ueberwachung (PDF).
3 DSK: Eine Bewertung von Pur-Abo-Modellen auf Websites; Kurzlink: https://t1p.de/dsk-pur-abos (PDF).

Vorträge, Veranstaltungen und Workshops K.2

Im Jahr 2023 hat unsere Behörde den Bürgerinnen und Bürgern auf zahlreichen Veranstaltungen den Datenschutz nähergebracht – und sich im Rahmen verschiedener Foren mit anderen Expertinnen und Experten ausgetauscht. Besonders häufig ging es dabei um Entwicklung und Nutzung von Künstlicher Intelligenz und die Bußgeldpraxis in der Datenschutzaufsicht.

Das Thema Künstliche Intelligenz (KI) hat viele Datenschutzveranstaltungen im Jahr 2023 geprägt. Spätestens seit dem Erfolg von ChatGPT und den konkreten Verhandlungen zu einer europäischen KI-Verordnung stellen sich die Menschen auch in Niedersachsen die Frage, ob und wie KI-Systeme mit dem Datenschutz vereinbar sind. Die Expertinnen und Experten unserer Behörde haben in Vorträgen und Workshops darauf hingewiesen, dass schon beim Trainieren von KI-Systemen der Datenschutz ins Spiel kommt – und dass die rasanten Entwicklungen nicht nur datenschutzrechtliche, sondern auch ethische Fragen aufwerfen.[1]

Eine hohe Aufmerksamkeit erfährt unsere Arbeit auch immer dann, wenn wir Geldbußen anordnen. Kein Wunder also, dass Unternehmen und die Öffentlichkeit gerne im Detail erfahren wollen, wie die festgelegten Beträge in der Praxis zustande kommen und bei welchen Verstößen wir aktiv werden.[2] Weil zudem im Jahr 2023 der Europäische Datenschutzausschuss die Berechnung von Bußgeldern vereinheitlicht hat[3], haben wir über dieses Thema besonders häufig referiert.

Bei den bisher höchsten Datenschutz-Bußgeldern in Deutschland ging es um die Überwachung von Mitarbeitenden in Unternehmen – eines davon hatte die Datenschutzaufsicht Niedersachsen angeordnet. Den Beschäftigtendatenschutz begleiten wir besonders intensiv – und das nicht nur, weil wir den entsprechenden Arbeitskreis in der deutschen Datenschutzkonferenz (DSK) leiten.[4] In unseren Vorträgen sind wir vor allem auf die neu-

1 Mehr zu KI und Datenschutz in den Kapiteln E und G.2.1.
2 Mehr zu den Bußgeldverfahren der Datenschutzaufsicht Niedersachsen in Kapitel H.
3 Mehr zu den Bußgeldrichtlinien des Europäischen Datenschutzausschusses in Kapitel J.1.
4 Mehr zu den Aktivitäten des Arbeitskreises Beschäftigtendatenschutz in Kapitel I.2.

en Herausforderungen in der Digitalisierung eingegangen: den Umgang mit digitalen Bewerbungsmappen, die Leistungskontrolle am PC und die Datenschutzanforderungen im spätestens seit der Corona-Pandemie etablierten Homeoffice. Seit Längerem fordern wir gemeinsam mit der DSK ein nationales Gesetz zum Beschäftigtendatenschutz.

Nicht nur mit Vorträgen und Workshops für den Datenschutz unterwegs: Der Landesbeauftragte Denis Lehmkemper (links) im Gespräch mit Felix Roscher und Svenja Höxbroe vom Podcast „Fortbildung macht Schule".

Viele Vortragsanfragen erhielten wir im Jahr 2023 zum vernetzten Fahrzeug. Automobile sind zunehmend vollgepackt mit Sensoren, Kameras und Mobilfunktechnik. Die gesammelten und an den Hersteller übertragenen Daten sind nicht nur notwendig für das autonome Fahren, sondern auch hilfreich, um in Echtzeit Verkehrsdaten auszuwerten, freie Parkplätze zu finden und Blechschäden beim Einparken und im stockenden Verkehr zu vermeiden. Die umfassende Datenverarbeitung schafft aber auch Begehrlichkeiten und macht detaillierte Bewegungsprofile der Fahrzeughaltenden möglich. Wenn Fahrzeughersteller bei ihren Innovationen Datenschutz aber von Anfang an mitdenken und beachten, gelingt die Transformation zum vernetzten Fahren, ohne die Rechte der Bürgerinnen und Bürger zu beeinträchtigen.

Datenschutzinstitut Niedersachsen schult Beschäftigte öffentlicher Stellen K.3

Das Datenschutzinstitut Niedersachsen ist der zentrale Schulungsträger in Sachen Datenschutz für öffentliche Stellen in Niedersachsen. 2023 haben wir mit einem vielfältigen Veranstaltungsprogramm mehr als 200 Beschäftigte öffentlicher Stellen in Niedersachsen geschult. Besonders im Fokus: Die behördlichen Datenschutzbeauftragten, die als Multiplikatoren in ihren Dienststellen auftreten.

Das Datenschutzinstitut Niedersachsen (DsIN) leistet seit seiner Gründung im Jahr 2016 mit seinen Schulungen einen wichtigen Beitrag für Datenschutz und Datensicherheit in Niedersachsen. Angesiedelt ist das DsIN beim Landesbeauftragten für den Datenschutz Niedersachsen (LfD).

Primär schulen und informieren die Expertinnen und Experten des DsIN Beschäftigte öffentlicher Stellen in Niedersachsen zu Datenschutzfragen, aber auch zu Aspekten der IT-Sicherheit. So zählen seit Inkrafttreten der Datenschutz-Grundverordnung auch technisch-organisatorische Maßnahmen des Datenschutzes zur gesetzlichen Verpflichtung der Verantwortlichen. Darüber hinaus fördern unsere Kurse die Wahrnehmung der Datenschutzaufsicht und macht ihr Wirken transparent.

Themen der DsIN-Veranstaltungen

Die DsIN-Veranstaltungen geben einen Überblick über die rechtlichen Grundlagen des Datenschutzes für öffentliche Stellen und technisch-organisatorische Maßnahmen in Theorie und Praxis. Darüber hinaus bieten wir Schulungen für verschiedene Zielgruppen des öffentlichen Dienstes zu spezialisierteren Aspekten des Datenschutzes[1] an.

So widmet sich eine DsIN-Schulung explizit dem Thema „Datenschutz in Schulen“. Hier klären unsere Dozentinnen und Dozenten sowohl über Belange des Datenschutzes für Kinder- und Jugendliche auf, als auch beim

1 Siehe DsIN-Veranstaltungsprogramm: https://lfd.niedersachsen.de/228474.html

Einsatz digitaler Plattformen im Unterricht und in der Organisation schulischer Prozesse. Gerade im Kontext von Schulen sehen sich die behördlichen Datenschutzbeauftragten oftmals mit einer Vielzahl von Fragen zur Verarbeitung und Veröffentlichung von personenbezogenen Daten konfrontiert.

Unsere Fortbildung zum Beschäftigtendatenschutz richtet sich vor allem an Mitglieder von Personalvertretungen. Anhand praxisorientierter Beispiele erfahren die Teilnehmerinnen und Teilnehmer, welche Konsequenzen datenschutzrechtliche Regelungen für Personalvertretungen haben und welche konkreten Maßnahmen Personalvertretungen zur Umsetzung datenschutzrechtlicher Vorgaben treffen müssen.

Ein spezielles Angebot gibt es außerdem zum Sozialdatenschutz, da in der Grundsicherung für Arbeitssuchende, in der Sozialhilfe und im Bereich der Kinder- und Jugendhilfe eine Vielzahl sensibler Daten verarbeitet werden. Die Veranstaltung richtet sich zum Beispiel an Mitarbeiterinnen und Mitarbeiter aus den Sozialverwaltungen oder den Jobcentern in Niedersachsen.

LfD-Infoveranstaltungen für den nicht-öffentlichen Bereich

Im nicht-öffentlichen Bereich bietet unsere Behörde kostenlose Infoveranstaltungen an.[2] Im Jahr 2023 haben wir uns in diesem Bereich vor allem auf Mitglieder von Vereinen konzentriert, die ehrenamtlich für den Datenschutz in einem Verein zuständig sind oder Mitgliederdaten verarbeiten. Praxisnah besprechen unsere Expertinnen und Experten bekannte und typische Beispiele aus dem Vereinsleben und nehmen sich ausführlich Zeit für die Fragen der Teilnehmerinnen und Teilnehmer.

Fazit

Mit einer Mischung aus Präsenzveranstaltungen und Online-Seminaren möchten wir im Flächenland Niedersachsen allen eine Teilnahme ermöglichen, die an datenschutzrechtlichen Themen interessiert sind. Wir hoffen, mit unseren Schulungen das Bewusstsein für Datenschutzthemen zu schärfen und Fachwissen zu verbreiten, um den Datenschutz zu fördern und ein möglichst hohes Datenschutzniveau zu gewährleisten.

2 Siehe unsere Website zu LfD-Infoveranstaltungen: https://lfd.niedersachsen.de/228579.html

Abkürzungsverzeichnis

Abs.	Absatz
AK	Arbeitskreis
Art.	Artikel
AVV	Auftragsverarbeitungsvertrag
Az.	Aktenzeichen
BDSG	Bundesdatenschutzgesetz
BGB	Bürgerliches Gesetzbuch
BKA	Bundeskriminalamt
BMDV	Das Bundesministerium für Digitales und Verkehr
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
Buchst.	Buchstabe/Unterpunkt
BVA	Bundesverwaltungsamt
DPA	Data Processing Agreement
DPC	Leiter/in der irischen Datenschutzbehörde
Drs.	Drucksache
DSB	Datenschutzbeauftragte/r
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DsIN	Datenschutzinstitut Niedersachsen
DSK	Datenschutzkonferenz
eAU	Elektronische Arbeitsunfähigkeitsmeldung
EfA-Prinzip	„Einer für Alle"-Prinzip
EDSA	Europäischer Datenschutzausschuss
EGovG-E	E-Government-Gesetz-Entwurf
EinwV	Einwilligungsverwaltungsverordnung
EuG	Gericht der Europäischen Union
EuGH	Europäischer Gerichtshof
GG	Grundgesetz
GPDP	Italienische Datenschutzaufsicht
HVB	Hauptverwaltungsbeamte
JuMiKo	Konferenz der Justizministerinnen und Justizminister
KI	Künstliche Intelligenz

KiKoN	KI-Kompetenzzentrum Niedersachsen
KIM	Kommunikation im Medizinwesen
KMU	Kleine und mittlere Unternehmen
LaSo	Landesamt für Soziales, Jugend und Familie
LfD	Landesbeauftragter für den Datenschutz
LG	Landgericht
LKA	Landeskriminalamt
MI	Niedersächsisches Ministerium für Inneres und Sport
MJ	Niedersächsisches Justizministerium
NDSG	Niedersächsisches Datenschutzgesetz
NKomVG	Niedersächsisches Kommunalverfassungsgesetz
NMeldVO	Niedersächsische Meldedatenverordnung
NPOG	Niedersächsisches Polizei- und Ordnungsbehördengesetz
NSchG	Niedersächsisches Schulgesetz
OLG	Oberlandesgericht
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz
OZG-E	Onlinezugangsgesetz-Entwurf
RdErl.	Runderlass
RLSB	Regionale Landesämter für Schule und Bildung
Rn.	Randnummer
SGB	Sozialgesetzbuch
SpDi	Sozialpsychiatrischer Dienst
StA	Staatsanwaltschaft
StBerG	Steuerberatungsgesetz
StPO	Strafprozessordnung
TI	Telematik-Infrastruktur
TKÜ	Telekommunikationsüberwachung
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
TOM	Technische und organisatorische Maßnahme
UAbs.	Unterabsatz
VDA	Verband der Automobilindustrie e. V.
VG	Verwaltungsgericht
VO	Verordnung