Der Landesbeauftragte für den Datenschutz Niedersachsen

Tätigkeitsbericht 2025

Niedersachsen

Der Landesbeauftragte für den Datenschutz Niedersachsen

31. Tätigkeitsbericht 2025

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, 30159 Hannover

Bildnachweis
Daniel George: Seite 8
LfD Niedersachsen: Seiten 38, 43, 85, 94, 108, 113, 114, 117
Adobe Stock: Titelbild (Markus Windeler), Seite 15 (your123), Seite 23 (flashmovie), Seite 35 (your123), Seite 68 (Bongkarn), Seite 79 (your123), Seite 89 (your123), Seite 97 (artjazz), Seite 105 (.shock), Seite 111 (Liudmyla), Seite 113 (Foto auf Flyer: Gorodenkoff)

Das Titelbild zeigt den Wasserturm der ostfriesischen Wattenmeerinsel Langeoog.

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

Vorwort

Das Jahr 2025 hat uns eindrücklich vor Augen geführt, wie eng technische Innovationen, rechtliche und politische Rahmenbedingungen sowie gesellschaftliche Entwicklungen miteinander verflochten sind. Schon im Tätigkeitsbericht 2024 hatten wir zu mehr digitaler Souveränität in der Verwaltung geraten. Und seitdem zeichnet sich immer deutlicher ab, wie dringend wir die Weichen stellen müssen. In der aktuellen geopolitischen Lage ist es wichtiger denn je, in der öffentlichen Verwaltung, aber auch in Schulen, Vereinen und Unternehmen auf vertrauenswürdige, europäische IT-Lösungen zu setzen.

Die weiterhin große Abhängigkeit wesentlicher Teile unserer IT-Infrastruktur von außereuropäischen Anbietern birgt erhebliche Risiken – für die Sicherheit, für die Selbstbestimmung und die Handlungsfähigkeit unseres Landes. Ich möchte daher alle Verantwortlichen in Niedersachsen ermutigen, neue Wege zu gehen, Alternativen zu prüfen und gemeinsam innovative Lösungen zu gestalten. Wir unterstützen sie dabei. Das gilt insbesondere für den Einsatz von Systemen Künstlicher Intelligenz: In diesem immer noch neuen und hochdynamischen Bereich sollten wir nicht leichtfertig auf die Angebote der globalen Technologiekonzerne setzen, sondern die Potenziale europäischer und regionaler Entwicklungen nutzen – und diese damit auch stärken.

Künstliche Intelligenz bewegt uns auch als Datenschutzaufsicht. Mit der KI-Stabsstelle, der aktiven Beteiligung am KI-Reallabor CRAI in Osnabrück und dem erfolgreichen KI-Symposium im Niedersächsischen Landtag im vergangenen Jahr haben wir wichtige Impulse gesetzt (s. Kapitel E.1). Unser Ziel ist es, den digitalen Wandel in Niedersachsen aktiv, verantwortungsvoll und datenschutzgerecht mitzugestalten.

Zurzeit wird im Rahmen eines überfälligen nationalen Umsetzungsgesetzes zur KI-Verordnung intensiv darüber diskutiert, die Aufgabe der Marktaufsicht über KI-Systeme zentral bei der Bundesnetzagentur anzusiedeln. Wir

halten es allerdings für verfassungsrechtlich zwingend und auch deutlich sinnvoller, dass die Marktaufsicht über in der niedersächsischen Verwaltung eingesetzte KI-Systeme auch in Niedersachsen angesiedelt ist (siehe Kapitel E.1.2). Wir stehen mit unserer Expertise dafür bereit, diese Aufgabe zu übernehmen.

Mich und meine Behörde beschäftigt das Thema Künstliche Intelligenz aber auch auf eine ganz praktische Weise. Im Jahr 2025 haben wir in Niedersachsen einen extremen Anstieg bei den Beschwerdeeingängen um 70 Prozent auf 4.022 erlebt (siehe Kapitel C.1). Im Schnitt erreichen uns also täglich elf Schreiben von niedersächsischen Bürgerinnen und Bürgern, die einen möglichen Datenschutzverstoß melden. Das zeigt uns einerseits, wie hoch das Vertrauen und auch die Erwartung der Menschen in unsere Arbeit ist, und wie ernst sie den Schutz ihrer Daten nehmen. Gleichzeitig gehen wir davon aus, dass ein Teil des Anstiegs auch von einem erleichterten Zugang zu unserer Behörde durch KI-Chatbots herrührt. Denn wer im Internet nach Datenschutzverstößen recherchiert, bekommt über die in Suchmaschinen integrierten KI-Systeme außer einem Hinweis über Beschwerdemöglichkeiten häufig gleich auch ein individualisiertes Beispielschreiben mitgeliefert.

Einerseits freut uns dieser erleichterte Zugang der Bürgerinnen und Bürger zu unserer Behörde und damit zur Durchsetzung ihrer Grundrechte natürlich. Andererseits stellt die aktuelle Situation unsere Behörde, die nicht automatisch mit den Beschwerdezahlen mitwächst, vor große Herausforderungen. Denn unser Anspruch bleibt es, nicht nur Beschwerden effizient und möglichst schnell zu bearbeiten, sondern auch weiterhin den niedersächsischen Gesetzgeber zu beraten, Unternehmen und Vereine zu unterstützen und Datenschutzbeauftragte zu schulen.

Mit Blick auf 2026 erwarten uns spannende Diskussionen beim Datenschutz. In Brüssel wird über die Überarbeitung der Datenschutz-Grundverordnung (DSGVO) beraten. Die EU-Kommission überprüft einerseits im sogenannten Digital Fitness Check zentrale Datenschutzregelungen und legt andererseits mit dem digitalen Omnibusgesetz Vorschläge für Änderungen an der DSGVO vor – mit möglicherweise weitreichenden, hoffentlich nicht nur negativen Folgen für das Datenschutzniveau in Europa (siehe Kapitel H). Die Datenschutzkonferenz hat diese Vorschläge kritisiert und im Gegenzug Anpassungen der DSGVO vorgeschlagen, die Hersteller insbe-

sondere von IT-Produkten stärker in die Verantwortung nehmen und kleine sowie mittlere Unternehmen entlasten.

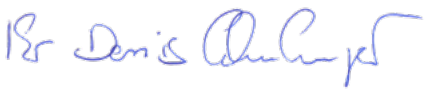
In Deutschland wird weiter über eine Zentralisierung der Datenschutzaufsicht für den nicht-öffentlichen Bereich diskutiert. Wir sind überzeugt, dass der direkte Kontakt zu einer unabhängigen Datenschutzbehörde in Niedersachsen für Bürgerinnen, Bürger und Unternehmen unverzichtbar bleibt.

Und in Niedersachsen stehen wir 2026 mit der Kommunalwahl im September erstmals vor einer Wahl, bei der die EU-Verordnung über die Transparenz und das Targeting politischer Werbung Anwendung findet (siehe Kapitel D). Sie soll die Integrität politischer Willensbildung stärken und Bürgerinnen und Bürger vor Desinformation schützen. Parteien und andere Akteure werden verpflichtet, Transparenz über die Finanzierung und die gezielte Ansprache von Wählergruppen herzustellen. Insbesondere müssen sie sogenanntes Profiling kenntlich machen – wenn ihre Werbung also auf eine einzelne Person anhand von Alter, Vorlieben, Verhalten oder anderen Eigenschaften zugeschnitten ist.

Auch die niedersächsische Landtagswahl 2027 wirft bereits ihre Schatten voraus. Viele Gesetzesvorhaben, die die im Landtag vertretenen Fraktionen noch vor Ende der Legislatur auf den Weg bringen wollen – etwa im Bereich der polizeilichen Ermittlungsbefugnisse, der Gesundheit und der Schulen –, erfordern einen wachsamen Blick auf die Wahrung der Grundrechte. Wir beraten die Ministerien und den Landtag im Hinblick auf die datenschutzrechtlichen Anforderungen solcher Gesetzesvorhaben.

Vor dem Hintergrund all dieser Herausforderungen gilt mein größter Dank allen meinen Kolleginnen und Kollegen, die sich in unserer Behörde jeden Tag mit großem Engagement für den Datenschutz in Niedersachsen einsetzen und deren vielfältige Arbeit Sie in diesem Tätigkeitsbericht niedergeschrieben finden. Bedanken möchte ich mich auch bei unseren Partnerinnen und Partnern in Verwaltung und Politik, aber auch in der Wissenschaft, Wirtschaft und Gesellschaft für die vertrauensvolle Zusammenarbeit.

Ich wünsche Ihnen eine spannende Lektüre und viele interessante Erkenntnisse beim Lesen unseres 31. Tätigkeitsberichts, den wir in diesem Jahr kompakter und kürzer gestaltet haben.



Empfehlungen des Landesbeauftragten für den Datenschutz Niedersachsen

An den Niedersächsischen Landtag

1. Immer deutlicher treten derzeit die Zentralisierungsbestrebungen beim Vollzug der europäischen Digitalgesetzgebung zutage. Es gilt, die bewährte föderale Eigenständigkeit zu verteidigen und zu bewahren. Unsere föderale Ordnung gewährleistet in besonderem Maße die Berücksichtigung und Wertschätzung regionaler Besonderheiten und Schwerpunkte, die Vertrauen schaffen und unser Land erfolgreich machen. So auch beim Datenschutz. Die Datenschutzaufsicht im eigenen Land hat viele Vorteile für Bürgerinnen und Bürger, Unternehmen, Forschungseinrichtungen und Behörden in Niedersachsen. Das gilt auch und gerade für den Umgang mit neuen Techniken wie KI-Systemen und -Modellen. Ich empfehle daher, sich weiterhin und nachdrücklich für eine handlungsfähige Datenschutzbehörde vor Ort in Niedersachsen einzusetzen.
2. Nach wie vor unterliegt die Verarbeitung personenbezogener Daten durch Gerichte in ihrer justiziellen Tätigkeit keiner datenschutzrechtlichen Kontrolle. Diese aufsichtsrechtliche Lücke steht im Gegensatz zu den hohen Anforderungen des europäischen Datenschutzrechts an den Schutz personenbezogener Daten. Dadurch besteht das Risiko, dass die Rechte der betroffenen Personen nicht ausreichend gewahrt werden. Die Einrichtung besonderer Stellen im Justizwesen wäre daher sinnvoll, um eine wirksame und unabhängige datenschutzrechtliche Kontrolle zu gewährleisten.

An die Niedersächsische Landesregierung

3. Die Sicherung der Souveränität Deutschlands ist ein Gebot der Stunde. Dies gilt im Besonderen für die digitale Souveränität. Außer technologischer Expertise und finanziellen Mitteln erfordert es zuallererst den deutlichen Willen zum grundlegenden Umdenken bei der Planung, Konzeption und Beauftragung der Digitalisierung der niedersächsischen

Verwaltung. Das Augenmerk ist dabei auf alle Ebenen zu richten, von der technischen Infrastruktur bis zum Einsatz von Systemen der Künstlichen Intelligenz. Digitale Souveränität herzustellen, gelingt nur „top-down". Ich bitte die Landesregierung daher, konsequent die Weichen für eine digital souveräne Zukunft und eine stabile Handlungsfähigkeit der öffentlichen Hand in Niedersachsen zu stellen.

4. Ich bitte die Landesregierung, sich über eine Bundesratsinitiative oder in anderer geeigneter Weise für eine Änderung im Bundesdatenschutzgesetz einzusetzen. Ziel sollte es sein, den Datenschutzbehörden im gerichtlichen Bußgeldverfahren vergleichbare Rechte wie der Staatsanwaltschaft einzuräumen – entsprechend zur Regelung für Kartellbehörden im Gesetz gegen Wettbewerbsbeschränkungen.[1] Der aktuelle Fall eines nicht durchsetzbaren Bußgelds (siehe Kapitel F) hat deutlich gemacht, dass die alleinige Zuständigkeit der Staatsanwaltschaften zu erheblichen praktischen Problemen führen kann. Datenschutzbehörden verfügen über die notwendige Fach- und Fallkenntnis, sodass sie gerichtliche Bußgeldverfahren effizient und sachgerecht selbst fortführen können. Eine entsprechende Regelung würde die Staatsanwaltschaften entlasten, die Datenschutzbehörden stärken, doppelte Arbeit vermeiden und so die Verfahrensabläufe insgesamt optimieren.

An die niedersächsischen Unternehmen

5. Unternehmen müssen sich aktiv mit den neuen EU-Digitalrechtsakten und deren Ausführungsgesetzen vertraut machen. Insbesondere müssen sie sich mit der KI-Verordnung und mit dem möglichen Einsatz von Systemen Künstlicher Intelligenz in der eigenen Organisation auseinandersetzen. Die Verantwortlichen sollten die einzusetzenden Produkte für die Nutzung sorgfältig auswählen, die Beschäftigten wirkungsvoll schulen und Handlungsanweisungen bereitstellen. Vor der unkontrollierten Nutzung privater KI-Anwendungen im beruflichen Kontext („Schatten-IT") warne ich. Sie birgt unkalkulierbare Risiken für den Daten- und Geheimnisschutz und kann Haftungsrisiken nach sich ziehen.
6. Die zahlreichen Pannenmeldungen, aber auch die Ergebnisse der Prüfungen unseres IT-Labors (siehe Kapitel I) zeigen: In Unternehmen fehlen zu oft das erforderliche Bewusstsein oder die Ressourcen für

1 § 82a Abs. 1 Satz 3 GWB.

wirksame IT-Sicherheitskonzepte. Sie riskieren damit nicht nur Datenschutzverletzungen, wenn sensible Daten ihrer Kunden und Beschäftigten abfließen, sondern auch hohe wirtschaftliche Schäden. Ein gezielter Schutz vor Angriffen von außen – beispielsweise durch ein konsequentes Patch-Management – ist daher dringend angeraten.

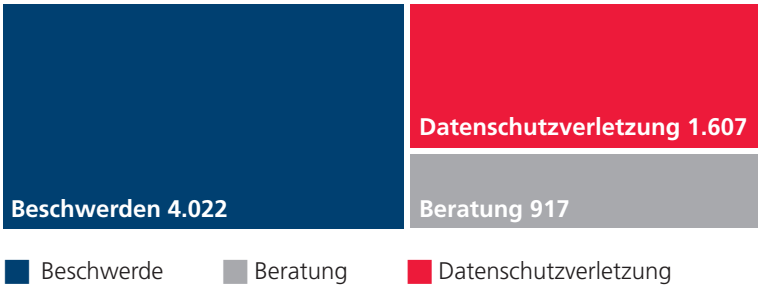
C Zahlen und Fakten

C.1 Blick in die Zahlen: Beschwerden auf Rekordniveau

Das Jahr 2025 stellte die Datenschutzaufsichtsbehörde Niedersachsen vor besondere Herausforderungen bei der Fallbearbeitung. Im Laufe des Berichtsjahrs zeichnete sich eine deutliche Steigerung der Fallzahlen ab, die sich nicht allein durch ein gestiegenes Datenschutzbewusstsein und ein umfassenderes Wissen um die Möglichkeiten individueller Rechtsdurchsetzung erklären lässt. Besonders auffällig war, dass immer häufiger Beschwerden eingingen, bei denen der Einsatz von Künstlicher Intelligenz beim Erstellen der Eingaben naheliegt. Denn inzwischen verweisen in Suchmaschinen integrierte KI-Chatbots bei Fragen rund um den Datenschutz häufig auf die Möglichkeit, eine Beschwerde an die zuständige Datenschutzbehörde zu richten. Oft liefern sie dazu gleich Formulierungsvorschläge für Anschreiben mit. Darauf deuten die Texte einiger Beschwerden hin, die typische Spuren oder Überbleibsel aus der Kommunikation mit KI-Chatbots enthalten.

Aus Sicht des Grundrechtsschutzes der Betroffenen ist diese Entwicklung grundsätzlich positiv zu bewerten, da sie den Zugang zur Aufsichtsbehörde erleichtert und das Bewusstsein für den Datenschutz stärkt. In der Praxis bringt sie jedoch erhebliche Herausforderungen mit sich: Während die Anzahl der Eingaben deutlich steigt, bleiben viele Eingaben unvollständig und erfordern zusätzlichen Bearbeitungsaufwand. Das ist mit den bisherigen Strukturen nur schwer zu bewältigen.

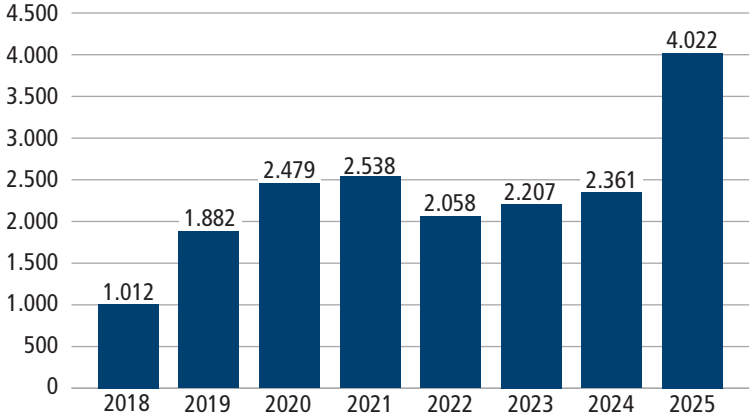
A1 – Beschwerden, Beratungen und Datenschutzverletzungen 2025



Beschwerden: Zuwachsrate von 70,4 Prozent

Im Jahr 2025 gingen in unserer Behörde insgesamt 4.022 Beschwerden ein. Dies entspricht einem Anstieg von 70,4 Prozent gegenüber dem Berichtsjahr 2024, in dem uns 2.361 Beschwerden erreichten. Ein wesentlicher Teil der Beschwerden betraf mit über 750 die Videoüberwachung im privaten Bereich, beispielsweise wenn Privatpersonen Überwachungskameras so ausrichten, dass sie Nachbargrundstücke oder öffentliche Flächen erfassen. Im Bereich der Wirtschaft fällt vor allem ein starker Anstieg von Beschwerden über Inkassounternehmen und Auskunfteien auf. Auch die Zahl der Beschwerden gegenüber der Wohnungswirtschaft und dem Einzelhandel erhöhte sich deutlich. Zudem verzeichneten wir erstmals auch 20 Beschwerden gegenüber Betreibern von KI-Systemen.

A2 – Zahl der Beschwerden 2018 bis 2025



Geringfügig mehr Datenschutzverletzungen

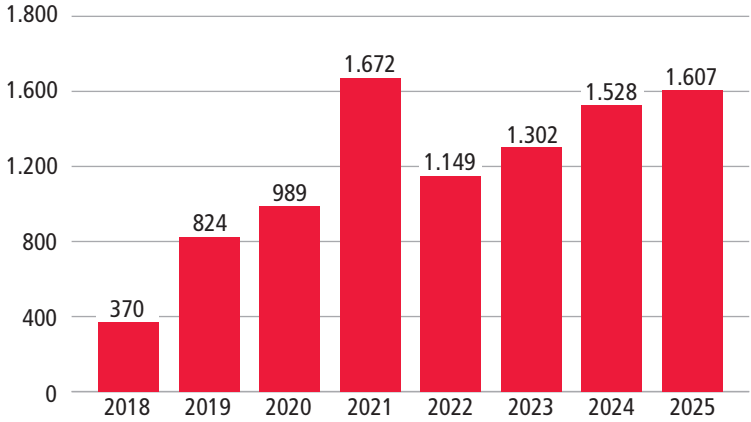
Unabhängig von dem deutlichen Anstieg der Datenschutzbeschwerden blieb die Zahl der uns gemeldeten Datenschutzverletzungen auf einem hohen Niveau: Mit 1.607 gemeldeten Datenschutzverletzungen[1] betrug der Anstieg 2025 rund 5,2 Prozent, verglichen zu den 1.528 Meldungen des Jahres 2024.

1 Nach Art. 33 DSGVO.

Sowohl öffentliche Stellen als auch Unternehmen sind verpflichtet, Datenschutzverletzungen etwa infolge von Cyberangriffen, Diebstahl oder unzureichenden Schutzmaßnahmen innerhalb von 72 Stunden an die zuständige Datenschutzbehörde zu melden, sofern durch die Datenschutzverletzung ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Ein Beispiel einer solchen Verletzung im Gesundheitsbereich und ihre Folgen finden Sie in Kapitel E.4.1.

Den moderaten Anstieg der Meldungen können wir anhand der vorliegenden Fallzahlen keinem bestimmten Bereich oder einer einzelnen Ursache zuordnen. Vielmehr gehen wir davon aus, dass die fortschreitende Digitalisierung in nahezu allen Lebensbereichen sowohl das Risiko von Datenpannen als auch die Anfälligkeit für Cyberangriffe und Datendiebstähle erhöht – und damit auch die Wahrscheinlichkeit, dass entsprechende Vorfälle gemeldet werden.

A3 – Gemeldete Datenschutzverletzungen 2018 bis 2025



Verhängte Geldbußen des Jahres 2025

Im Jahr 2025 haben wir Geldbußen in einer Gesamthöhe von rund 705.000 Euro verhängt. Die festgesetzten Bußgelder richteten sich unter anderem gegen Unternehmen aus den Bereichen Gastgewerbe, Handel, Finanzdienstleistungen, Fitnessstudios, der Bauwirtschaft, Logistik, Produktion sowie gegen natürliche Personen. Bei den Verstößen handelte es

sich um die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage, um die Verletzung von Informationspflichten, die Nichtführung oder die Nichtvorlage von Verzeichnissen der Verarbeitungstätigkeit sowie um die Nichtbeachtung unserer behördlichen Anweisungen. Von den 34 Erstbescheiden in Bußgeldsachen hatten zum Zeitpunkt der Berichtslegung bereits 26 Bescheide Rechtskraft erlangt. Sie wurden also von den Beschiedenen nicht mit den ihnen zustehenden Rechtsmitteln angefochten.

Zuwachs an Aufgaben und Zuständigkeiten

Mit dem Zuwachs an Aufsichtszuständigkeiten ist davon auszugehen, dass die Fallzahlen wohl in den kommenden Jahren kontinuierlich steigen. So kommen beispielsweise durch die übertragenen Aufgaben nach dem Gesundheitsdatennutzungsgesetz (GDNG)[2] und der Verordnung über die Transparenz und das Targeting politischer Werbung (TTPW-VO)[3] weitere datenschutzrelevante Regelungsbereiche hinzu, die wahrscheinlich zu einer Zunahme der Fallzahlen führen werden.

Parallel beobachten wir seit Jahren ein zunehmendes Bewusstsein für den Schutz der Privatsphäre und die informationelle Selbstbestimmung. Bürgerinnen und Bürger sind sich dieser Rechte in einer immer stärker digitalisierten Welt zunehmend bewusst und machen davon Gebrauch. Aus Perspektive des Datenschutzes ist dies ein Erfolg, den wir auch als Anerkennung unserer Arbeit verstehen. Klar ist jedoch auch, dass dynamisch steigende Fallzahlen und erweiterte Zuständigkeiten nur mit einem entsprechenden Zuwachs an Ressourcen und Ausstattung zufriedenstellend bewältigt werden können. Nur so können wir auf der „Digitalisierungsautobahn“ auch weiterhin als Leitplanke und notfalls auch als Airbag einen wirksamen Schutz des Grundrechts auf Datenschutz gewährleisten.

2 Siehe Kapitel E.4.2.
3 Siehe Kapitel D.

C.2 Beteiligung an Gesetzgebungsverfahren

Die Begleitung von Rechtssetzungsvorhaben durch die Landesdatenschutzaufsichtsbehörde ist gleich in mehrfacher Hinsicht zentral. Zum einen ist eine Beteiligung des Landesbeauftragten für den Datenschutz bei Gesetzgebungsvorhaben der Landesregierung Teil des vorgeschriebenen Gesetzgebungsverfahrens, besonders wenn im Gesetzentwurf Datenschutzaspekte berührt sind.[4] Zum anderen kann die im Haus vorhandene Expertise im Gesetzgebungsverfahren effektiv und vorausschauend eingesetzt werden. Denn unter unserer Beratung entstandene Gesetze sind mit der gebotenen Datenschutzsensibilität versehen.

Nicht zuletzt sind klare Gesetzesregelungen, die Tatbestand und Rechtsfolge von Datenverarbeitungsbefugnissen eindeutig festlegen, für die einfache Anwendbarkeit in der täglichen Praxis bedeutsam und tragen so auch zum Grundrechtsschutz bei.

Im Jahr 2025 haben wir die folgenden Rechtssetzungsvorhaben begleitet.

Gesetze des Landes

Niedersächsische Verfassung (Verf NI)
Niedersächsisches Gesetz zur Ausführung des Artikel-10-Gesetzes (Nds. AG G 10)
Niedersächsisches Bildungszeitgesetz (NBildZG)
Niedersächsisches Disziplinargesetz (NDiszG)
Niedersächsisches Gesundheitsfachberufegesetz (NGesFBG)
Niedersächsisches Justizgesetz (NJG)
Niedersächsisches Gesetz zur Ausführung des Achten Buchs des Sozialgesetzbuchs und zur Niedersächsischen Kinder- und Jugendkommission (Nds AG SGB VIII)
Niedersächsisches Kommunalwahlgesetz (NKWG)

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

Niedersächsisches Gesetz zur Ausführung der Förderung durch den Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (Niedersächsisches ELER-Fördergesetz – NEFG)
Niedersächsisches Maßregelvollzugsgesetz (Nds. MVollzG)
Niedersächsisches Polizei- und Ordnungsbehördengesetz (NPOG)[5]
Niedersächsisches Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke (NPsychKG)
Niedersächsisches Gesetz über gemeindliche Schiedsämter (Niedersächsisches Schiedsämtergesetz - NSchÄG)
Niedersächsisches Schulgesetz (NSchG)
Niedersächsisches Gesetz zur obligatorischen außergerichtlichen Streitschlichtung (Niedersächsisches Schlichtungsgesetz – NSchlG)
Niedersächsisches Verfassungsschutzgesetz (NVerfSchG)
Niedersächsisches Gesetz über das amtliche Vermessungswesen (NVermG)

Staatsverträge

Digitale Medien-Staatsvertrag (DMStV – Diskussionsentwurf / Teil 1)[6]
Glücksspielstaatsvertrag 2021
Jugendmedienschutz-Staatsvertrag

5 Siehe ausführlich Kapitel E.7.1.
6 Siehe ausführlich Kapitel E.2.3.

Verordnungen, Richtlinien, Erlasse und sonstige Regelungen des Landes

Verordnung über die Anerkennung von Angeboten zur Unterstützung im Alltag nach dem Elften Buch des Sozialgesetzbuchs (AnerkVO SGB XI)
Niedersächsische Glücksspielverordnung (NGlüSpVO)
Niedersächsische Kommunalwahlordnung (NKWO)
Niedersächsische Laufbahnverordnung (NLVO)
Richtlinie über die Gewährung von Zuwendungen zur Förderung gemeinsamer Modellvorhaben nach § 123 SGB XI (SGB XI §123 GMZuwRdErl, NI)
Verordnung über das Verbot des Führens von Waffen und Messern in Verkehrsmitteln und Einrichtungen des öffentlichen Personenverkehrs

Gesetze des Bundes

Politische-Werbung-Transparenz-Gesetz (PWTG): Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/900 des Europäischen Parlaments und des Rates vom 13. März 2024 über die Transparenz und das Targeting politischer Werbung[7]

Zu einigen dieser Rechtsetzungsvorhaben finden Sie in diesem Tätigkeitsbericht ausführlichere Informationen: Zum NPOG in Kapitel E.7.2, zum DMStV und JMStV in Kapitel E.2.3 und zum PWTG in Kapitel D.

7 Siehe ausführlich Kapitel D.

D Schlaglicht: Transparenz & Targeting bei politischer Werbung

Die Verordnung über die Transparenz und das Targeting politischer Werbung: Schutz demokratischer Systeme durch Transparenz?

Nie zuvor war die Demokratie in Europa so massiv durch digitale Einflussnahme bedroht wie heute. Mit wenigen Klicks können politische Akteure – und ausländische Mächte – gezielt Millionen Bürgerinnen und Bürger mit maßgeschneiderten Botschaften erreichen und so ihre Meinungen und Wahlentscheidungen beeinflussen. Die Enthüllungen um Cambridge Analytica 2016[1] und die Manipulationen bei internationalen Wahlen, etwa bei der Präsidentschaftsstichwahl in Rumänien 2024[2], die sogar zur Aufhebung und Neuwahl geführt haben, zeigen die Gefahren deutlich. Die Berichte des Verfassungsschutzes zu erheblichen ausländischen Cyberangriffen im Vorfeld von Wahlen offenbaren, wie brisant das Thema der Flut der Desinformation auch in sozialen Netzwerken ist: Die digitale Welt ist zum Schauplatz im Kampf um Aufmerksamkeit, Deutungs- und Meinungshoheit geworden. Die Europäische Union reagiert mit der Verordnung (EU) 2024/900 über die Transparenz und das Targeting politischer Werbung (TTPW-VO)[3] – ein juristischer Schutzwall gegen die schleichende Unterwanderung unserer demokratischen Grundordnung.

Die digitale Welt ist zum Schauplatz im Kampf um Aufmerksamkeit und Deutungshoheit geworden.

Die am 13. März 2024 in Kraft getretene TTPW-VO ist seit dem 10. Oktober 2025 in allen Mitgliedstaaten unmittelbar anwendbares Recht. Sie muss nur insoweit mit nationalen Gesetzen umgesetzt werden, als bestimmte in der EU-Verordnung vorgesehene Zuständigkeiten und Befugnisse zugewiesen werden müssen. Die TTPW-VO ergänzt die Datenschutz-Grundverordnung (DSGVO) und den Digital Services Act (DSA).

1 Siehe auch Bundeszentrale für politische Bildung, 2. Mai 2019, https://t1p.de/cambridge-analytica (Kurzlink).
2 Siehe auch Bundeszentrale für politische Bildung, 29. April 2025, https://t1p.de/wahlen-2024 (Kurzlink).
3 https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202400900 (PDF).

Im Jahr 2026 finden viele Wahlen in Deutschland statt, in Niedersachsen im September 2026 die Kommunalwahl. Damit rückt die Verordnung gleichermaßen in den Fokus der Anbieter politischer Wahlwerbung wie auch der Bürgerinnen und Bürger, die Werbung erhalten.

Dieses Schlaglicht gibt einen Überblick über die Zielsetzung der Verordnung und die daraus resultierenden Rechte für die Betroffenen und Pflichten für Internet-Plattformen, Parteien und andere Verantwortliche aus dem Blickwinkel der Landesdatenschutzbehörden. Die Umsetzungsgesetze von Bund und Ländern liegen aktuell noch nicht vor, sodass Strukturen erst im laufenden Prozess entstehen.

Anwendungsbereich und Zielsetzung

Die Regelungen der TTPW-VO gelten umfassend für alle Medienformen, also auch audiovisuelle Medien, Printmedien sowie Online- und Offline-Werbung.[4]

Eine Ausnahme stellt Kapitel III der TTPW-VO dar, das sich explizit auf Wahlwerbung im Internet bezieht und für das die Landesdatenschutzbehörden zuständig sind.[5] Ihnen obliegt insbesondere der Schutz vor der missbräuchlichen Verwendung personenbezogener Daten zur gezielten Wahlwerbung durch sogenanntes Profiling und Targeting im Internet.

Die Vorschriften beziehen sich auf in der Regel bezahlte Werbung politischer Akteure oder andere Kampagnen, deren Ziel es ist, das Ergebnis einer Wahl oder eines Referendums zu beeinflussen. Die Vorgaben gelten für EU-, Bundestags-, Landtags- und Kommunalwahlen sowie Organe und Organwalter[6] in Gebietskörperschaften.

Mit der Verordnung will die EU den Prozess der demokratischen Meinungs- und Willensbildung von Bürgerinnen und Bürgern vor Manipulation schützen. Sie ergänzt die in der Europäischen Grundrechtecharta verankerten Rechte und Freiheiten. Die freie Meinungsbildung des Einzelnen und ein offener Austausch der Positionen im Prozess der politischen Willensbil-

4 Art. 2 Abs. 2 TTPW-VO.
5 Art. 18–20 TTPW-VO.
6 Organwalter sind natürliche Personen, die für ein Organ einer juristischen Person handeln und dessen Aufgaben wahrnehmen.

dung sollen geschützt werden, um freie unbeeinflusste Wahlen sicherzustellen. Dies ist nur möglich, wenn Informationen transparent und ungefiltert sind und nicht manipulativ eingesetzt werden.

Ein weiterer Zweck der TTPW-VO ist die EU-weite Harmonisierung der Regelungen, um den freien Wettbewerb der Werbewirtschaft im Bereich politischer Werbung zu verbessern.

Manipulierendes Profiling und Targeting

Ein zentrales Anliegen der Verordnung ist das Verhindern manipulativer Beeinflussung durch personalisiertes Targeting. Durch die Vielzahl gesammelter Daten kann die digitale Werbewirtschaft umfangreiche Profile erstellen, die Rückschlüsse auf viele Persönlichkeitsmerkmale der Internetnutzenden zulassen. Diese können nicht nur für kommerzielle Werbung genutzt werden, sondern auch für passgenaue politische Ansprache – also Wahlwerbung. Politische Werbung kann dafür zielgerichtet auf einzelne Wählergruppen ausgespielt werden, indem bestimmte Informationen besonders betont werden, sie sprachlich angepasst ist und besonders auf die Interessen und Lebensumstände der Wählergruppe zugeschnitten ist. Aspekte, die der Wählergruppe nicht wichtig sind, oder die sie eher kritisch sieht, werden nicht oder weniger deutlich behandelt. Dieses Targeting genannte Vorgehen ermöglicht eine sehr individuelle werbliche Ansprache der jeweiligen Zielgruppe.

Mit Targeting können Akteure die Meinungsbildung manipulieren und die Wahlentscheidungen maßgeblich beeinflussen. Wenn keine gemeinsame, faktenbasierte und unstrittige Informationsbasis mehr besteht und Meinungsvielfalt nicht mehr wahrgenommen wird, stört das die politische Meinungsbildung erheblich und kann eine Gefährdung für die Demokratie bedeuten. Dies nutzen auch Drittstaaten[7] in großem Maßstab zur Beeinflussung von Wahlen. Eine solche Beeinflussung ist daher eine Gefahr für die öffentliche Sicherheit und Stabilität. Die TTPW-VO regelt deshalb, dass drei Monate vor einer Wahl keine Wahlwerbung aus Drittstaaten an Wahlberechtigte ausgebracht werden darf.

7 Ein Drittstaat im EU-Recht ist ein Staat, der weder Mitglied der Europäischen Union noch des Europäischen Wirtschaftsraums (EWR) ist.

Zum Schutz der Bürger und Bürgerinnen ist es nur erlaubt, personenbezogene Daten für politische Werbung zu nutzen, wenn diese gegenüber dem Verantwortlichen ausdrücklich ihre Einwilligung zur Erhebung der Daten für diesen Zweck erklärt haben. Es wird ausgeschlossen, dass Plattformen bereits vorliegende Profil-Informationen, etwa aus Werbetracking, verwenden dürfen. Es ist verboten, besonders sensible persönliche Daten[8] der Betroffenen zu benutzen, etwa die politische Meinung, Religion, ethnische Herkunft, sexuelle Orientierung oder Gesundheitsdaten. Auch dürfen keine personenbezogenen Daten von Minderjährigen und potenziellen Jungwählern genutzt werden, die das nationale Wahlalter in frühestens einem Jahr erreichen.

Kennzeichnungspflichten

Damit eine manipulationsfreie Meinungsbildung möglich ist, muss Wahlwerbung gekennzeichnet werden. Diese Pflicht trifft die Herausgeber politischer Werbung. Herausgeber im Sinne der Verordnung ist jeder, der politische Werbung veröffentlicht, zustellt oder verbreitet – das gilt auch für Dienstleister.

Die TTPW-VO normiert allgemeine Transparenzvorschriften für politische Werbedienstleistungen[9] und ergänzt diese durch besondere Vorgaben für politische Werbung im Internet.[10] Es sei an dieser Stelle der Vollständigkeit halber erwähnt, dass bei politischen Werbedienstleistungen darüber hinaus gegebenenfalls Vorschriften aus weiteren Gesetzen wie der DSGVO, dem Presserecht, dem DSA und weiteren landesgesetzlichen Bestimmungen beachtet werden müssen.

Jeder politischen Werbung ist eine Transparenzmitteilung anzufügen.

Jeder politischen Werbung ist eine Transparenzmitteilung anzufügen, aus der hervorgeht, dass es sich um eine politische Werbung handelt, wer der Sponsor (Auftraggeber) ist

8 Vgl. Art. 9 DSGVO.

9 Art. 11 und 12 TTPW-VO. Siehe auch Vorgaben in der Durchführungsverordnung (EU) 2025/1410 der Kommission vom 9. Juli 2025 über das Format, das Muster und die technischen Spezifikationen der Kennzeichnungen und Transparenzbekanntmachungen politischer Anzeigen: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202501410.

10 Art. 19 TTPW-VO.

und gegebenenfalls, wer hinter dem Sponsor steht.[11] Das schließt die Adressdaten ein, sowie welche Wahl oder welches Referendum mit der Werbung angesprochen wird. Es ist darüber hinaus die Identität des Sponsors anzugeben und wer die Anzeige bezahlt, also die Herkunft der Geldquelle sowie diverse weitere Informationen, die unter anderem die Dauer, Reichweite und die finanzielle Strahlkraft der Anzeige und der Werbekampagne betreffen.[12] Zudem ist mitzuteilen, falls personenbezogene Daten verwendet wurden und diese Daten einem Targeting oder Anzeigeschaltungsverfahren unterzogen wurden.[13] Alternativ kann ein klarer und leicht zugänglicher Hinweis angebracht werden, wo diese Informationen aufgerufen werden können.

Die Verantwortlichen müssen darüber hinaus die Logik und die wichtigsten Parameter der eingesetzten Verfahren öffentlich machen. Wenn sie Künstliche Intelligenz oder besondere Anzeigenverfahren verwenden, müssen sie auch hierzu genaue Angaben machen.[14] Es sind diverse Informationen offenzulegen über die Zielgruppenbestimmung, die Kategorien verwendeter personenbezogener Daten, die Ziele, Mechanismen und Logik des Targetings, den Verbreitungszeitraum und die Zahl der erreichten Einzelpersonen.

In die Transparenzerklärung sind auch Hinweise zum Beschwerdeverfahren und zu offiziellen Informationsquellen zu Wahlen und Referenden aufzunehmen.

Ausnahmen und Schutz der Meinungsfreiheit

Von der Verordnung ausgenommen sind private, unbezahlte politische Meinungsäußerungen, die nicht kommerziell oder nicht professionell organisiert sind, sowie Mitteilungen von Parteien oder gemeinnützigen Organisationen an ihre Mitglieder. Ebenso ist amtliche Information zur Organisation von Wahlen oder öffentliche Kommunikation von Behörden nicht erfasst, sofern diese nicht auf die Beeinflussung von Wahlergebnissen abzielt. Auch gesetzlich geregelte, unentgeltliche Kandidatenvorstellungen

11 Art. 11 TTPW-VO.
12 Art. 12 TTPW-VO.
13 Einschließlich Informationen aus Art. 19 Abs. 1 c, e TTPW-VO.
14 Art. 19 TTPW-VO.

sind von den Regelungen ausgenommen, um die Meinungsfreiheit, die politische Teilhabe und die Informationsfreiheit nicht unverhältnismäßig einzuschränken.

Nationale Umsetzung und Zuständigkeiten in Deutschland

Die nationale Umsetzung der Verordnung in Deutschland erfolgt auf Bundesebene durch das Politische-Werbung-Transparenz-Gesetz (PWTG), das sich zum Zeitpunkt der Erstellung dieses Berichts noch im Gesetzgebungsprozess befindet.[15] Darin werden die Zuständigkeiten für die verschiedenen Aufgaben geregelt, die der Verordnungsgeber den Mitgliedsstaaten zuschreibt. Bei Redaktionsschluss lag ein Regierungsentwurf vom 17. Dezember 2025 nach Beratung im Bundesrat mit Empfehlungen der Bundesregierung vor.

Im Anschluss an die Verabschiedung des PWTG und in Abhängigkeit von den dort getroffenen Regelungen sind auf Länderebene Gesetzgebungsverfahren durchzuführen und es ist ein Medienstaatsvertrag[16] abzuschließen, um die nicht im PWTG geregelten Zuständigkeiten auf Länderebene[17] und die Anwendung des Ordnungswidrigkeitengesetzes zu regeln. Es können zusätzlich auch Verwaltungsvereinbarungen abgeschlossen werden. Nach dem derzeitigen Entwurfsstand des PWTG wird die Bundesnetzagentur wesentliche Teile der Verordnung beaufsichtigen.[18] Sie wird Kontaktstelle auf EU- Ebene sein und das Online-Verzeichnis der bevollmächtigten Vertreter für Anbieter politischer Werbedienstleister führen.[19]

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wird mit der Überwachung und Durchsetzung von Artikel 20 der

15 Über den aktuellen Stand des Gesetzgebungsverfahrens informiert der Bund auf seiner Webseite: https://t1p.de/pwtg (Kurzlink).

16 Die Landesmedienanstalten sind bereits für Wahlwerbung zuständig, möglicherweise zukünftig auch für Art. 11, 12 TTPW-VO.

17 Regelungen zu Art. 22 Abs. 4 TTPW-VO, Auffangregelung für nicht genannte Aspekte wie Vorschriften (Art. 20, 1-6 TTPW-VO) und nicht genannte Akteure, die nicht Anbieter von Vermittlungsdiensten sind.

18 Art. 7–10, 13–17 und 21 der TTPW-VO für Anbieter von Vermittlungsdiensten.

19 Links zu Websites der Mitgliedstaaten: https://political-advertising.ec.europa.eu/screen/public/representative/list

Verordnung betraut, der das Übermitteln von Informationen zur Wahlwerbung an Interessenten regelt – soweit das Bundesdatenschutzgesetz eine Zuständigkeit für die Durchsetzung der Datenschutzgrundverordnung bestimmt. Die Zuständigkeit bezieht sich damit primär auf öffentliche Stellen des Bundes.

Landesdatenschutzbehörden überwachen Targeting und Transparenz

Keiner nationalen Umsetzungsgesetze bedarf es für die Aufsicht über die Überwachung von Targeting[20] und der Transparenz hinsichtlich des Targetings.[21] Hier sind die Datenschutzaufsichten der Länder, also in Niedersachsen unsere Behörde, aus der EU-Verordnung unmittelbar zuständig.

Bei Landesdatenschutzbehörden können sich Betroffene beschweren, wenn sie den Verdacht haben, dass sie über das Internet politische Werbung erhalten, für deren Ausspielung unerlaubtes Targeting eingesetzt wurde. Die Nutzung personenbezogener Daten bei politischer Werbung ist bei Targeting- und Online-Anzeigen nur erlaubt, wenn der Verantwortliche die Daten von der betroffenen Person erhoben hat und die betroffene Person ausdrücklich ihre Einwilligung zur gesonderten Verarbeitung der personenbezogenen Daten für die Zwecke der politischen Werbung gegeben hat. Die Ablehnung einer Zustimmung gilt auch für die Zukunft und es darf nicht immer wieder erneut nach einer Einwilligung gefragt werden. Betroffene können sich auch beschweren, wenn Profiling vorliegt und dafür besonders sensible personenbezogene Daten[22] verwendet wurden. Darüber hinaus ist eine Beschwerde bei den Landesdatenschutzbehörden möglich, wenn Plattformbetreiber die erforderlichen Transparenzerklärungen beim Ausspielen politischer Werbung[23] nicht oder nicht vollständig beigefügt haben.

Die Landesdatenschutzbehörde prüft solche Beschwerden und kann bei Verstößen Anordnungen zur Unterlassung, Löschung oder Änderung der

20 Gemäß Art. 18 TTPW-VO.
21 Gemäß Art. 19 TTPW-VO.
22 Vgl. Art. 9 DSGVO.
23 Nur gemäß Art. 19 TTPW-VO, nicht für Transparenzvorschriften nach Art. 11 und 12 TTPW-VO.

Datenverarbeitung treffen. Dabei können auch Bußgelder verhängt werden.

Vor einer Beschwerde sollten Betroffene aber zunächst die in den Werbeanzeigen verpflichtend bereitzustellenden Widerrufsmöglichkeiten oder das verpflichtend vorgesehene Beschwerdeformular der Herausgeber der zu beanstandenden Werbung verwenden. Führt dies nicht zum Erfolg oder ist dies erst gar nicht bereitgestellt, so kann Beschwerde bei der zuständigen Datenschutzbehörde erhoben werden.

Aktuell bestehen allerdings noch Einschränkungen für die Durchsetzung der Verordnung durch die Datenschutzbehörden. Bis sie auch die vollumfänglichen Befugnisse nach dem Ordnungswidrigkeitenrecht erhalten haben, werden die Datenschutzbehörden die Einhaltung der Verordnung nur eingeschränkt durchsetzen können.

Ausblick

Bei profilgestütztem Targeting zur Online-Werbung ist die Werbewirtschaft weit entwickelt und hochspezialisiert. Anzeigen im Internet können vollautomatisiert in Sekundenbruchteilen nach personalisierten Kriterien, Persönlichkeitsprofilen und Umgebungs-Checks passgenau ausgespielt werden. Die Initiative des EU-Verordnungsgebers, den Bereich der politischen Werbung stärker zu regulieren, begrüßen wir ausdrücklich. Die TTPW-VO setzt hier neue Maßstäbe für Transparenz und Datenschutz bei politischer Werbung und reagiert auf Gefahren für die politische Meinungsbildung durch Manipulation.

Dabei soll ausdrücklich dem Argument entgegengetreten werden, dass damit die politische Werbung für Parteien, Verbände oder zivilgesellschaftliche Organisationen erschwert und politische Meinungsäußerung unterdrückt werden soll. Private, unbezahlte politische Meinungsäußerung Einzelner unterfällt nicht der TTPW-VO. Auch im kommerziellen Bereich wird Meinung nicht unterdrückt, sondern soll offen als solche ausgewiesen werden. In Abgrenzung zu den ansonsten üblichen Formen des sogenannten Microtargetings darf politische Werbung jedoch nur noch mit Einwilligung sowie unter Nutzung von Profildaten ausgespielt werden, die direkt bei der betroffenen Person erhoben wurden. Höchstpersönliche sensible

Daten wie Religion, Herkunft oder politische Meinung dürfen grundsätzlich nicht verwendet werden.

Große Dienstleister in der Werbewirtschaft wie Meta und Alphabet mit ihren Plattformen wie Instagram, Facebook oder YouTube haben unter Hinweis auf die Vorschriften zu Transparenz und zu Targeting der TTPW-VO politische Werbung zunächst untersagt, weil deren Prozesse und Techniken nach eigener Aussage die nunmehr gebotene Transparenz nicht ermöglichen und sie das Risiko der Verletzung der neuen Regeln nicht ausschließen können.

Damit müssen sich nicht nur die Account-Betreiber darauf einstellen, Reichweite für ihre politischen Inhalte auch ohne Online-Werbebudgets zu generieren. Letztlich muss sich auch die Werbewirtschaft umstellen und das Geschäft so umstrukturieren, dass neue Werbeplätze geschaffen werden, die ein unzulässiges Targeting ausschließen. Es bleibt abzuwarten, ob und wie sich der Markt neu und datenschutzfreundlicher entwickelt.

Die Wirksamkeit der EU-Verordnung für den Schutz der demokratischen Prozesse in der digitalen Welt hängt maßgeblich von der Umsetzung auf nationaler Ebene ab. Angesichts der komplexen Rechtslage, in der neben der TTPW-VO auch andere Regelwerke wie die DSGVO, der DSA und diverse Mediengesetze parallel gelten, ist eine klare und verbindliche Koordinierung der Zuständigkeiten zwischen den beteiligten Behörden unerlässlich.

Hausaufgaben für die Gesetzgeber

Die wichtigste Forderung an die Gesetzgeber ist eine klare gesetzliche Regelung zur Zuständigkeitsabgrenzung. Es bedarf der zügigen Verabschiedung von Bundes- und Landesgesetzen sowie von Staatsverträgen, die die Aufgabenverteilung und die Zusammenarbeit zwischen den Landesdatenschutzbehörden, Landesmedienanstalten, der Bundesnetzagentur und der Bundesdatenschutzbeauftragten verbindlich regeln. Nur so können Strukturen etabliert werden, die eine effektive und reibungslose Zusammenarbeit in Deutschland und europaweit gewährleisten. Und dann ist auch eine

Die wichtigste Forderung an die Gesetzgeber ist eine klare gesetzliche Regelung zur Zuständigkeitsabgrenzung.

schnelle Reaktion auf Verstöße möglich, die den rechtswidrigen Einfluss auf Wahlen erfolgreich begrenzt.

Die zuständigen Behörden müssen zeitnah mit den notwendigen Befugnissen ausgestattet werden, insbesondere im Bereich des Ordnungswidrigkeitenrechts, um Verstöße gegen die TTPW-VO konsequent ahnden zu können. Voraussichtlich wird dies für die Landesdatenschutzbehörden oder Landesmedienanstalten nicht einheitlich durch das PWTG geregelt werden, sodass die Landesgesetzgeber hier einzeln gefordert sein werden. Durch die zeitlichen Unterschiede ist für eine Übergangszeit mit einem bundesweiten Flickenteppich zu rechnen.

Schließlich sind die in der TTPW-VO formulierten Definitionen und die Transparenzpflichten zu konkretisieren. Die noch offenen Leitlinien, insbesondere zum Targeting bei Online-Werbung[24] müssen zeitnah vom Europäischen Datenschutzausschuss vorgelegt werden, um die praktische Anwendung zu erleichtern und Orientierung für alle Beteiligten zu schaffen. Ohne diese Maßnahmen droht die Gefahr, dass die hohen Anforderungen der TTPW-VO zunächst nur auf dem Papier bestehen bleiben und die demokratische Integrität bei bevorstehenden Wahlen wie den Kommunalwahlen in Niedersachsen 2026 nicht ausreichend geschützt wird. Der Gesetzgeber ist daher gefordert, die rechtlichen und organisatorischen Rahmenbedingungen schnell und umfassend zu schaffen, um die Verordnung wirksam und bürgernah umzusetzen.

24 Art. 18, 19 TTPW-VO.

E Aktuelle Themen

E.1 Künstliche Intelligenz

E.1.1 Symposium zur Künstlichen Intelligenz des LfD Niedersachsen

Im November 2025 hatten wir zu einem Symposium zur rechtssicheren Nutzung von Künstlicher Intelligenz in das Forum des Niedersächsischen Landtags eingeladen. Schirmherrin war die Landtagspräsidentin Hanna Naber. Knapp 150 Teilnehmerinnen und Teilnehmer haben sich auf dem Symposium über Wege zur rechtssicheren und vertrauensvollen KI in Niedersachsen informiert. Dabei tauschten sie sich über rechtliche, praktische, aber auch ethische Fragen beim Einsatz von Künstlicher Intelligenz aus.

Ergebnisse der Expertengespräche zur Künstlichen Intelligenz

Das KI-Symposium diente als Rahmen für die Präsentation der Ergebnisse unserer KI-Expertengespräche, über die wir im Tätigkeitsbericht 2024 berichtet haben, an eine weite Fachöffentlichkeit.[1] Den ausführlichen Ergebnisbericht zu den KI-Expertengesprächen hat unsere Behörde zuvor im Juni 2025 veröffentlicht[2] und an den Landtag übermittelt[3], da aus den Erkenntnissen die folgenden zentralen Empfehlungen an den Landesgesetzgeber und an die Landesregierung abgeleitet werden konnten.

Zentrale Empfehlungen des Berichts an den Landesgesetzgeber:

- Rechtsgrundlagen schaffen für das Training von KI-Modellen mit personenbezogenen Daten durch öffentliche Stellen
- Klare gesetzliche Regelungen zum Einsatz Künstlicher Intelligenz in der Landesverwaltung

Zentrale Empfehlungen des Berichts an die Landesregierung:

- Unterstützung beim datenschutzkonformen Einsatz von KI, etwa durch Standards, Schulungen und Folgeabschätzungen
- Förderung und Forschung zu vertrauenswürdiger, erklärbarer KI
- Ausbau von Unterstützungsangeboten für KMU, z. B. durch einen niedersächsischen KI-Gipfel

1 Abschlussbericht abrufbar unter https://lfd.niedersachsen.de/242757.html
2 Siehe Tätigkeitsbericht 2024, Kapitel E.
3 Vgl. Pressemitteilung vom 18. Juni 2025, https://lfd.niedersachsen.de/242633.html

Rahmenbedingungen zum Einsatz von KI gefordert

An dem KI-Symposium nahmen Interessierte aus Kommunen, der Landesverwaltung, Unternehmen, Universitäten und anderen Einrichtungen teil. Das Vortragsprogramm haben Expertinnen und Experten aus Verwaltung, Wirtschaft und Forschung gestaltet. Im Eröffnungsvortrag stellte die Leiterin der KI-Stabsstelle des LfD Niedersachsen, Dr. Silke Jandt, die Ergebnisse der KI-Expertengespräche des LfD Niedersachsen vor und skizzierte Lösungswege für datenschutzrechtliche Herausforderungen beim Training und Output von KI-Systemen. Gesine Irskens, Referatsteilleiterin im Justizministerium Niedersachsen, gab einen Einblick in den Einsatz von Künstlicher Intelligenz im Justizwesen, etwa zur in Niedersachsen genutzten Anwendung MAKI (Massenverfahrensassistenz mit KI), die Gerichte bei Massenverfahren unterstützt.

Weitere Vorträge von Professor Dr. Ricardo Usbeck (Leuphana Universität Lüneburg), Franziska Weindauer (Geschäftsführerin TÜV AI.LAB), Professor Dr. Dieter Kugelmann (Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Rheinland-Pfalz) und Jutta Löwe (Head of Regions Compliance bei der Continental Reifen Deutschland GmbH) setzten sich mit rechtlichen und technischen Fragen rund um den Einsatz Künstlicher Intelligenz in Wirtschaft und Verwaltung auseinander, aber auch mit der praktischen Umsetzung. Die Frage der Notwendigkeit spezifischer Rechtsgrundlagen zog sich wie ein roter Faden durch die Vorträge der Veranstaltung, was den Bedarf an einem klaren Rechtsrahmen für den Einsatz von Künstlicher Intelligenz deutlich machte.

Die Notwendigkeit spezifischer Rechtsgrundlagen zog sich wie ein roter Faden durch die Veranstaltung.

In einem abschließenden Panel diskutierte Denis Lehmkemper gemeinsam mit Jutta Löwe, Continental Reifen Deutschland GmbH, und Dr. Horst Baier, CIO der niedersächsischen Landesregierung, über den erfolgreichen Einsatz von KI in Niedersachsens Wirtschaft und Verwaltung. Herr Dr. Baier betonte die großen Chancen von KI etwa beim Beschleunigen von Verwaltungsprozessen oder in der IT-Sicherheit. Er bestärkte die Teilnehmenden, das Thema mutig anzugehen und sich nicht von der raschen Entwicklung überholen zu lassen. Bei aller Popularität von allgemeinen Chatbots riet Jutta Löwe dazu, auf der Grundlage einer Bedarfserhebung zu klären, für welche Prozesse der Einsatz von Chatbots oder spezifischen KI-Systemen

Etwa 150 Teilnehmerinnen und Teilnehmer informierten sich auf dem KI-Symposium des LfD Niedersachsen zu rechtssicheren und vertrauensvollen KI-Systemen.

tatsächlich sinnvoll ist. Denis Lehmkemper bekräftigte diesen Appell: „Ich mache mir Sorgen, dass wir KI an vielen Stellen als Pflaster auf Probleme kleben, die wir eigentlich grundsätzlicher lösen müssten, wenn beispielsweise Prozesse viel zu kompliziert geworden sind."

Insgesamt ziehen wir ein durchweg positives Fazit aus den KI-Expertengesprächen und dem KI-Symposium. Beide Aktivitäten haben deutlich gezeigt, dass ein interdisziplinärer Austausch zwischen Wirtschaft, Verwaltung und Forschung notwendig ist und ein allseitiges großes Interesse daran besteht.

E.1.2 Umsetzung der KI-Verordnung in Deutschland

Die im Juni 2024 in Europa beschlossene Verordnung über Künstliche Intelligenz (KI-VO) erfordert ergänzend ein nationales Umsetzungsgesetz. In diesem waren bis zum 2. August 2025 insbesondere die in der KI-VO vorgesehenen zuständigen Behörden in den Mitgliedstaaten zu benennen.[4]

4 Zum Inkrafttreten und zum Geltungsbeginn s. Art. 113 KI-VO.

In Deutschland ist bis Ende 2025 kein entsprechendes Gesetz beschlossen worden, es wurde aber im September ein erster Entwurf der Bundesregierung für ein neues KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG) vorgelegt.[5] Wir haben gegenüber dem Niedersächsischen Innenministerium eine kritische Stellungnahme zum Entwurf des Durchführungsgesetzes zur KI-Verordnung der Bundesregierung abgegeben.

Zuständige Behörden für die Überwachung der KI-VO

Nach der KI-VO sollen die Mitgliedstaaten mindestens eine notifizierende Behörde oder eine Marktüberwachungsbehörde benennen. Die größere praktische Bedeutung liegt bei der Aufgabe der Marktüberwachung. Der Entwurf der Bundesregierung schlägt in dieser Rolle bis auf wenige Ausnahmen die Bundesnetzagentur (BNetzA) als zentrale zuständige Behörde für die Überwachung der Anforderungen der KI-VO vor. Die Datenschutzaufsichtsbehörden sollen demnach weder für öffentliche noch für nichtöffentliche Stellen als Marktüberwachungsbehörde eingesetzt werden. Sofern beim Einsatz von KI-Systemen personenbezogene Daten verarbeitet werden, soll nach diesem Entwurf zukünftig die Aufsicht darüber durch zwei unterschiedliche Behörden erfolgen.

Verstoß gegen europarechtliche Vorgaben

Die von der Bundesregierung vorgesehene Übertragung der Marktüberwachung für Hochrisiko-KI-Systeme im Kontext von Strafverfolgung, Wahlen, Grenzkontrollen und Justizverwaltung an eine bei der BNetzA eingerichtete unabhängige KI-Marktüberwachungskammer verstößt gegen die in der KI-VO enthaltenen europarechtlichen Vorgaben.[6] Europarechtlich vorgesehen ist, dass diese Zuständigkeiten ausschließlich den Datenschutzaufsichtsbehörden nach der Datenschutz-Grundverordnung (DSGVO) sowie jeder anderen gemäß derselben Bedingungen festgelegten, unabhängigen Behörde[7] übertragen werden dürfen.

5 Referentenentwurf Gesetz zur Durchführung der KI-Verordnung vom 11.9.2025, https://t1p.de/bmds-kivo (Kurzlink).

6 Gemäß Art. 74 Abs. 8 KI-VO.

7 Etwa die in Art. 41 bis 44 JI-Richtlinie der EU festgelegten Aufsichtsbehörden, die unter anderem den Datenschutz im Bereich der Straftaten und Strafvollstreckung regelt.

Durch die Einrichtung einer unabhängigen KI-Marktüberwachungskammer bei der BNetzA können diese Anforderungen nicht erfüllt werden. Dieser fehlt es an der notwendigen Haushaltsautonomie, da ihre Finanzierung aus dem allgemeinen Haushalt der BNetzA stammt. Ebenso fehlt es an der notwendigen Unabhängigkeit, denn der Präsident der BNetzA kann auf Antrag des Bundesministeriums für Wirtschaft und Energie entlassen werden.

Verstoß gegen die Kompetenzordnung des Grundgesetzes

Die unabhängige KI-Marktüberwachungskammer bei der BNetzA soll auch die Aufsicht über den Einsatz von KI-Systemen durch Behörden der Länder und Kommunen erhalten. Das ist mit den verfassungsrechtlichen Vorgaben nicht vereinbar.

Die Ausführung von Bundesgesetzen ist gemäß dem Grundgesetz grundsätzlich Sache der Länder.[8] Das gilt auch für die Ausführung von europäischen Rechtsnormen. Vorliegend kann sich der Bundesgesetzgeber zudem nicht auf die im Grundgesetz verankerte Möglichkeit stützen, eigene Behörden zu errichten.[9] Das wäre nur dann zulässig, wenn dem Bund für diese Angelegenheiten die Gesetzgebungskompetenz zustehen würde.[10] Dies ist bezüglich der Marktaufsicht über Behörden jedoch nicht der Fall. Praktische Relevanz dürften vor allem Fallgestaltungen erlangen, in denen Schulbehörden oder Polizeibehörden der Länder KI-Systeme als Anbieter für eigene Zwecke entwickeln oder als KI-Betreiber anwenden und an keinem Marktgeschehen teilnehmen. Diese Fallgestaltungen unterliegen vollständig dem Schul- beziehungsweise Polizeirecht der Länder. Eine Gesetzgebungskompetenz des Bundes besteht hierfür nicht. Die BNetzA müsste bei der Aufsicht über Schul- oder Polizeibehörden der Länder folglich landesrechtliche Regelungen berücksichtigen. Das ist mit der Kompetenzordnung des Grundgesetzes nicht vereinbar.

8 Art. 83 GG.
9 Art. 87 Abs. 3 S. 1 GG.
10 Art. 87 Abs. 3 S. 1 GG.

Begrenzung der Möglichkeiten zur Einrichtung von KI-Reallaboren

Die KI-VO sieht die Möglichkeit zur Einrichtung von KI-Reallaboren vor.[11] In diesen können für Forschungszwecke personenbezogene Daten unter vereinfachten Bedingungen verarbeitet werden. Im Gesetzentwurf der Bundesregierung ist die Einrichtung mindestens eines „zentralen" KI-Reallabors durch die BNetzA vorgesehen.[12] Der Gesetzentwurf lässt die Einrichtung und den Betrieb von KI-Reallaboren durch andere Behörden im Prinzip zwar unberührt.[13] Allerdings müssen diese anderen Behörden durch Bundes- oder Landesrecht zu Marktüberwachungsbehörden bestimmt worden sein.

Durch die Zentralisierung der Marktüberwachungsaufgaben bei der BNetzA werden deshalb KI-Reallabore ausschließlich bei der BNetzA errichtet werden können. Daraus resultieren für die Praxis gravierende Probleme, die sich negativ auf die Möglichkeiten zur Verarbeitung von personenbezogenen Daten für die Zwecke der Erforschung und Entwicklung von KI-Systemen auswirken werden.

Gesetzgebungsverfahren noch nicht abgeschlossen

Kurz vor Redaktionsschluss dieses Tätigkeitsberichts hat die Bundesregierung am 6. Februar 2026 auf diese Kritik reagiert und einen neuen, zweiten Gesetzesentwurf veröffentlicht.[14] Sofern öffentliche Stellen der Länder KI-Systeme in Verkehr bringen, in Betrieb nehmen oder verwenden, sollen nun die zuständigen Marktüberwachungsbehörden durch die Länder auf Landesebene bestimmt werden. Für die Wirtschaft ist wie im ersten Entwurf die BNetzA vorgesehen.

11 Art. 57 ff. KI-VO.
12 § 13 Abs. 1 S. 1 KI-MIG-E.
13 § 13 Abs. 1 S. 2 KI-MIG-E.
14 https://t1p.de/bmds-kivo (Kurzlink).

E.1.3 Einsatz von LLMoin und MS-Copilot durch öffentliche Stellen

In der niedersächsischen Landesverwaltung haben im Jahr 2025 Pilotversuche zur Einführung eines KI-basierten Verwaltungsassistenten stattgefunden. Verschiedene Behörden erprobten über mehrere Monate den Einsatz der KI-Systeme LLMoin und MS-Copilot Chat. Wir haben das Niedersächsische Innenministerium bei diesem Prozess beraten.

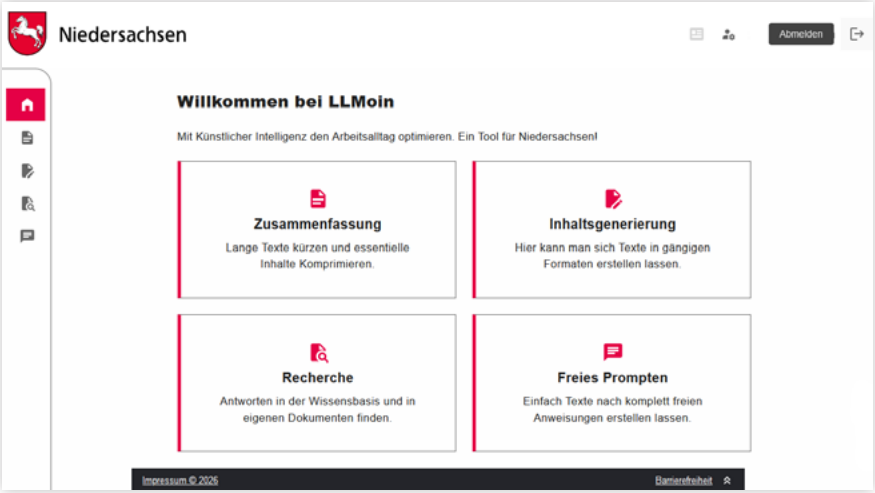
LLMoin ist ein LLM[15]-gestützter Chatbot, den das Amt für IT und Digitalisierung (ITD) der Senatskanzlei Hamburg entwickelt und der IT-Dienstleister Dataport technisch umgesetzt hat. Das KI-System nutzt das KI-Modell GPT-4o. LLMoin kann aber auch mit anderen Large-Language-Modellen (LLM) betrieben werden. LLMoin beinhaltet die Grundfunktionen „Zusammenfassungen", „Inhaltsgenerierung", „Recherche" und „Freies Prompten". Außer bei der Aufgabe „Freies Prompten" müssen Nutzende eigene Dateien hochladen. Im Gegensatz zu MS-Copilot Chat ist jedoch keine Websuche eingebunden.

MS-Copilot Chat ist ein KI-System, das ebenfalls auf dem KI-Modell GPT-4o basiert. Das KI-System Copilot Chat läuft im Browser und ermöglicht durch freies Prompten Texte zu erstellen, Recherchen durchzuführen, sich Fragen beantworten zu lassen und Bilder zu generieren.

Datenschutzrechtliche Herausforderungen

Im niedersächsischen Recht gibt es bislang keine Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten in LLMoin oder MS-Copilot Chat. Grundsätzlich kann auf die fachspezifischen Datenschutzvorschriften zurückgegriffen werden, wenn LLMoin oder MS-Copilot Chat in einem konkreten Verwaltungsverfahren zum Einsatz kommen und dabei personenbezogene Daten verarbeitet werden. Der Rückgriff auf die fachspezifischen datenschutzrechtlichen Rechtsgrundlagen ist allerdings nicht möglich, wenn aus dem Einsatz des KI-Systems zusätzliche datenschutzrechtliche Risiken resultieren, die nur durch ergänzende Anforderungen in der Rechtsgrundlage eingehegt werden können.

15 LLM ist die Abkürzung für Large Language Model, dem generativen KI-Modell hinter KI-basierten Chatbots.



Startseite des KI-Systems LLMoin

Das ist beispielsweise dann der Fall, wenn ein hohes Risiko dafür besteht, dass von LLMoin oder MS-Copilot Chat gegebene unrichtige oder durch Bias verzerrte Antworten in Verwaltungsverfahren verwendet werden. Dem Grundsatz der Richtigkeit personenbezogener Daten kann in diesen Fällen nicht durch einen allenfalls zu einem späteren Zeitpunkt greifenden Berichtigungsanspruch Betroffener angemessen Rechnung getragen werden. Daher kann die Verarbeitung personenbezogener Daten nur unter der Voraussetzung rechtmäßig sein, dass durch zusätzliche technische und organisatorische Maßnahmen die Richtigkeit von personenbezogenen Output-Daten gewährleistet wird. Falls keine spezifischen Datenschutzvorschriften im Fachrecht existieren, kann nicht pauschal auf allgemeine datenschutzrechtliche Rechtsgrundlagen[16] zurückgegriffen werden. Dies ist allenfalls dann möglich, wenn durch die Datenverarbeitung nur in geringem Umfang in Grundrechte der Betroffenen eingegriffen wird.

Wir haben dem Landesgesetzgeber empfohlen, im niedersächsischen Landesrecht eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten beim Einsatz von KI-Chatbots durch öffentliche Stellen zu erlassen.

16 Beispielsweise § 3 NDSG.

Um eine rechtssichere Verwendung von LLMoin und MS-Copilot Chat zu gewährleisten, ist der korrekte Umgang mit sogenannten Halluzinationen des KI-Systems von zentraler Bedeutung. Halluzinationen sind dadurch gekennzeichnet, dass ein KI-System zwar überzeugend klingende, aber faktisch falsche Tatsachen als Ergebnis ausgibt. Um den Grundsatz der Datenrichtigkeit soweit wie möglich zu gewährleisten, müssen Verantwortliche wirksame technische und organisatorische Maßnahmen implementieren. Beispielsweise sollte erwogen werden, die sogenannte Temperatur des KI-Modells[17] auf einen möglichst niedrigen Wert einzustellen. Damit wird das KI-System insgesamt etwas weniger kreativ, aber präziser agieren. Die Verantwortlichen müssen zudem prüfen, welche weiteren Systemparameter vorhanden sind, um die datenschutzrechtlichen Anforderungen gewährleisten zu können.

Im Hinblick auf die Gewährung und Einhaltung der Betroffenenrechte bringt der Einsatz von LLMoin und MS-Copilot Chat große Herausforderungen mit sich. Nach datenschutzrechtlichen Maßstäben ist es aktuell sehr zweifelhaft, ob im KI-Modell personenbezogene Daten berichtigt oder gelöscht werden können. Es ist nur bis zu einem gewissen Grad möglich, Output-Daten zu filtern, sodass sie nicht in die damit umgesetzten Verwaltungstätigkeiten einfließen. Vor dem Einsatz von LLMoin oder MS-Copilot Chat im Regelbetrieb sollten wirksame Prozesse etabliert werden, um auf die Geltendmachung von Betroffenenrechten unter Beachtung dieser Prämissen sachgerecht reagieren zu können.

Vor einer Einführung im Regelbetrieb muss eine umfassende Schulung des Personals erfolgen.

Vor einer flächendeckenden Einführung von LLMoin oder MS-Copilot Chat im Regelbetrieb muss eine umfassende und bedarfsgerechte Schulung des Personals, das das KI-System nutzen soll, erfolgen. Zentrale Aspekte sollten dabei sein, dass alle Nutzerinnen und Nutzer über ein Grundlagenverständnis zur Abgrenzung eines KI-Systems zu einer reinen Wissensdatenbank, zu Halluzinationen in KI-Systemen und zu Bias-Effekten verfügen.

17 Die Temperatur ist ein Parameter bei Sprachmodellen. Dieser steuert, wie deterministisch oder zufällig die generierten Antworten sind. Eine niedrige Temperatur führt zu vorhersehbareren und einheitlicheren Ausgaben, eine höhere Temperatur zu kreativeren – dabei steigt aber auch das Risiko für ungenaue oder falsche Antworten.

Ebenfalls sollte eine solche Schulung dazu befähigen, effektiv zu prompten und Ergebnisse der KI-Systeme kritisch zu evaluieren. Darüber hinaus sollte jede Organisationseinheit bedarfsorientiert geschult werden, um speziellen Anforderungen gerecht zu werden, die sich aus den jeweiligen Fachgebieten ergeben können – beispielsweise der Umgang mit besonderen Kategorien personenbezogener Daten oder rechtliche Besonderheiten durch spezifische Rechtsgrundlagen.

Ausblick

Zukünftig wird die Landesverwaltung KI-Chatbots wie LLMoin oder MS-Copilot Chat einsetzen – auch unter Nutzung personenbezogener Daten. Bisher sind die Rahmenbedingungen für einen datenschutzkonformen Einsatz noch nicht gegeben, die datenschutzrechtlichen Anforderungen scheinen den Verantwortlichen aber sehr wohl bewusst zu sein und es werden erste richtige Weichenstellungen vorgenommen.

Mehr zum Thema Künstliche Intelligenz finden Sie unter https://lfd.niedersachsen.de/ki auf unserer Webseite.

E.2 Digitale Medien

E.2.1 Zu viele Daten bei Foren-Registrierungen gesammelt

Welche Auswirkungen der Grundsatz der Datenminimierung konkret für betroffene Personen hat und wie er hilft, Risiken für diese zu vermeiden, hat ein Verfahren aus dem Jahr 2025 deutlich gemacht. Es richtet sich gegen einen Verantwortlichen, der ein Diskussionsforum im Internet betreibt. Bei der erforderlichen Registrierung wurden deutlich mehr Angaben eingefordert, als es datenschutzrechtlich zulässig ist.

Üblicherweise wird bei der Registrierung in einem Forum verlangt, einen Benutzernamen, eine E-Mail-Adresse und ein Passwort anzugeben. Die E-Mail-Adresse dient in der Regel dem Zurücksetzen des Passworts. Im hiesigen Fall waren darüber hinaus auch Anrede, Vorname, Nachname, Anschrift und Telefonnummer anzugeben.

Was bedeutet das für die Nutzerinnen und Nutzer des Forums? Anschrift und Telefonnummer sind Daten, die beispielsweise für Werbung, aber auch für Phishing und Betrugsversuche genutzt werden können. Außerdem sind sie geeignet, die Identifizierbarkeit einer Person zu erleichtern. Demgegenüber ist das Auftreten unter einem frei gewählten Benutzernamen mit einer gesondert eingerichteten, willkürlichen E-Mail-Adresse quasi anonym möglich. Der Grundsatz der Datenminimierung sorgt also dafür, Risiken für die betroffenen Personen zu verringern. Daten, die nicht vorhanden sind, können weder durch den Verantwortlichen noch durch mögliche Angreifer missbraucht werden. Während bei der Erhebung von E-Mail-Adresse, Benutzernamen und Passwort bei der Registrierung durch Forenbetreiber keine Bedenken bestehen, bedarf es für die Erhebung weiterer Daten einer tragenden Begründung im Einzelfall.

Unwirksame Einwilligung

Im vorliegenden Fall lautete die Begründung, dies geschehe auf der Grundlage einer Einwilligung – doch weil diese Daten als Pflichtfeld abgefragt wurden, waren die Eingaben nicht freiwillig und die Einwilligung damit un-

wirksam.[1] Der Betreiber berief sich sodann auf weitere Rechtsgrundlagen – im Kern war das Argument stets, er müsse unter Umständen mit einzelnen Forennutzenden Kontakt aufnehmen, wenn ein von diesem Nutzenden erstellter Beitrag durch eine andere Person als rechtswidrig gemeldet würde. Dann müsse und wolle er als Betreiber des Forums den Sachverhalt aufklären, um entscheiden zu können, ob der Beitrag zu löschen sei. Dies gebiete die so genannte Störerhaftung.

Dem waren mehrere Argumente entgegenzuhalten: Die Störerhaftung stellt keine rechtliche Verpflichtung dar, bestimmte Daten zu erheben, sondern sieht vielmehr vor, vorhandene Daten zu nutzen. Die Aufklärung des Sachverhalts kann zwar grundsätzlich ein berechtigtes Interesse darstellen, allerdings gab der Betreiber in seinen eigenen Regelwerken an, Beiträge nach einer Meldung auch ohne Aufklärungsbemühungen zu löschen, sodass dieses Interesse bei diesem Betreiber offenbar nur vorgeschoben war.

Unabhängig davon war die Erhebung gleich mehrerer Kontaktmöglichkeiten nicht erforderlich und verstieß damit gegen den Grundsatz der Datenminimierung. Die Kontaktaufnahme zur Aufklärung des Sachverhalts ist über die – ohnehin erhobene – E-Mail-Adresse möglich. Zwar mag eine telefonische Rücksprache besser geeignet sein, den Sachverhalt aufzuklären. Diese könnte aber auch im Einzelfall per E-Mail abgefragt werden. Eine vorsorgliche Speicherung insbesondere der Anschriften aller Forennutzenden ist nicht datenschutzkonform. Sollte sich eine Nutzerin oder ein Nutzer nicht zurückmelden, müsste auf der Grundlage der bekannten Informationen entschieden werden.

Nachdem der Verantwortliche sein Vorgehen wiederkehrend verteidigt hatte, fassten wir unsere Argumente unter Hinweis auf bereits ergangene Gerichtsentscheidungen zusammen und kündigten an, im nächsten Schritt von unseren Abhilfebefugnissen Gebrauch machen zu wollen. Daraufhin passte der Verantwortliche das Registrierungsformular an und löschte auch die unrechtmäßig erhobenen Daten.

1 Art. 7 Abs. 4 DSGVO.

E.2.2 Verwaltungsgericht bestätigt: „Alles ablehnen"-Option im Cookie-Banner ein Muss

Auf nahezu jeder Webseite werden Nutzerinnen und Nutzer mit einem Einwilligungsbanner – oder auch Cookie-Banner – konfrontiert. Der Blick wird oftmals auf eine Schaltfläche mit der Bezeichnung „Alle akzeptieren" gelenkt. Mangels offensichtlicher Alternative klicken viele auf diese Schaltfläche, damit solche Einwilligungsbanner schnellstmöglich verschwinden und der Inhalt der Webseite gelesen werden kann. Mit dem „Alle akzeptieren"-Klick wird allerdings die Erlaubnis erteilt, dass unter Umständen sehr viele Cookies und andere Trackingtechniken eingesetzt werden, um detaillierte Nutzungsprofile zu generieren. So ist es den Werbetreibenden möglich abzuschätzen, ob der Besuchende beispielsweise die Absicht hat, eine Reise zu buchen oder bereit ist, eine Spiele-App zu installieren. In der Folge kann in Echtzeit personalisierte Werbung auf der Webseite ausgespielt werden.

Wir setzen uns seit vielen Jahren gegen manipulativ gestaltete Einwilligungsbanner ein und für wirksame – insbesondere informierte und freiwillige – Einwilligungen. Die Mehrheit der Betreiber reagiert auf unsere Hinweise und passt die Einwilligungsbanner deutlich erkennbar an. Wir erreichen in vielen Fällen zudem, dass die Anzahl der eingesetzten Trackingtechniken deutlich reduziert wird.

Im Berichtszeitraum hat das Verwaltungsgericht Hannover mit Urteil vom 19. März 2025 die Rechtsauffassung der Datenschutzaufsichtsbehörde Niedersachsen bestätigt und die Rechte von Internetnutzerinnen und -nutzern in Sachen Datenschutz gestärkt.[2] Das Gericht urteilte, dass sich die Anforderungen für eine wirksame Einwilligung unmittelbar aus der DSGVO ergeben. Konkret wurden die folgenden Anforderungen bestätigt.

Informiertheit der Einwilligung

Die Anzahl der beteiligten Drittdienstleister ist auf erster Ebene zu nennen. Außerdem muss der Hinweis auf das Widerrufsrecht und der Hinweis auf Verarbeitungen in Drittstaaten unmittelbar sichtbar sein.

Ziel dieser Vorgabe ist es, der Nutzerin oder dem Nutzer das Ausmaß einer erteilten Einwilligung vor Augen zu führen.

2 Aktenzeichen: 10 A 5385/22.

Freiwilligkeit der Einwilligung

Das Einwilligungsbanner darf nicht so gestaltet sein, dass es die Nutzerin oder den Nutzer gezielt zu einer Einwilligung hinlenkt und von einer Ablehnung abhält. Daher ist darauf zu achten, dass das Ablehnen nicht mit einem erheblichen Mehraufwand verbunden ist. Die Möglichkeit, ablehnen zu können, muss erkennbar sein, und klickbare Felder müssen eindeutig beschriftet sein. Nach dem Ablehnen darf die Nutzerin beziehungsweise der Nutzer nicht bei jedem folgenden Webseitenbesuch erneut zur Abgabe der Einwilligung aufgefordert werden.

Unmissverständlich abgegebene Willensbekundung

Klicks auf das Einwilligungsbanner müssen das Ergebnis herbeiführen, das ein durchschnittlicher Nutzer erwartet. Bei einem Button „Akzeptieren & schließen x" in der oberen rechten Ecke erwartet ein durchschnittlicher Nutzer bei einem Klick auf das „x", dass sich das Einwilligungsbanner ohne Einwilligung schließt – tatsächlich wollte der Verantwortliche im entschiedenen Fall hierin eine Einwilligung sehen.

Die Störerhaftung stellt keine rechtliche Verpflichtung dar, bestimmte Daten zu erheben.

Im zweiten Teil seiner Entscheidung äußert sich das Verwaltungsgericht zum Einsatz des Google Tag Managers. Dieser Dienst dient der Einbindung von Code-Fragmenten und erleichtert so die Einbindung anderer Dienste. Das Verwaltungsgericht bestätigte, dass der Google Tag Manager nur eingebunden werden darf, wenn die Nutzerin oder der Nutzer dazu eingewilligt hat. Das folgt einerseits daraus, dass die Klägerin keine anderweitige Rechtsgrundlage für die Verarbeitung anführen konnte, andererseits aus Paragraf 25 Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), der die Endeinrichtung von Endnutzern schützt.[3]

In der Zusammenschau lässt sich feststellen, dass sehr viele Webseitenbetreiber die rechtlichen Voraussetzungen für die Einbindung von Drittdiensten, insbesondere für das Ausspielen personalisierter Werbung, nicht einhalten. Oft werden keine – oder keine wirksamen – Einwilligungen eingeholt. Würden die gesetzlichen Anforderungen eingehalten, wären Cookie-Banner auf Webseiten ein deutlich geringeres Ärgernis. Das Urteil des

3 Mehr zu diesem Paragrafen im Tätigkeitsbericht 2024, G.3.1.

Verwaltungsgerichts Hannover sendet ein deutliches Signal an Webseitenanbieter und trägt so dazu bei, vermehrt datenschutzkonforme Einwilligungslösungen umzusetzen.

E.2.3 Altersverifikation und Content-Analyse per KI: Änderungen im Jugendmedienschutz

Im Berichtszeitraum haben wir zu zwei datenschutzrechtlich relevanten Änderungsvorhaben in Bezug auf den Medienstaatsvertrag Stellung genommen – zum 6. Medienänderungsstaatsvertrag (6. MÄStV) und zum Diskussionsentwurf für Teil 1 des Digitale-Medien-Staatsvertrags (DMStV).[4] Der 6. MÄStV ist bereits am 1. Dezember 2025 in Kraft getreten und aktualisiert den Medienstaatsvertrag (MStV) sowie den Jugendmedienschutz-Staatsvertrag (JMStV). Beide Änderungsvorhaben zielen auf die Verbesserung des Jugendschutzes im Online-Bereich mittels technischer Maßnahmen, bei denen der Datenschutz relevant wird.

Neuer Betriebssystemansatz des 6. MÄStV

Kern der datenschutzrechtlich relevanten Änderungen des JMStV ist die Einführung eines neuen Betriebssystemansatzes. Durch die Einführung der Paragrafen 12 und 12a im JMStV werden Anbieter von Betriebssystemen und von bestimmten Apps verpflichtet, anerkannte Jugendschutzprogramme oder andere geeignete technische Maßnahmen zur Verfügung zu stellen, damit Altersvorgaben von Webseiten und Apps berücksichtigt werden. Jugendschutzprogramme sind in diesem Zusammenhang Softwarelösungen, die Alterskennzeichnungen von veröffentlichten Inhalten auslesen und Angebote erkennen, die nicht für Kinder und Jugendliche geeignet sind.

Solche Jugendschutzprogramme müssen seit 2022 von allen Anbietern eingesetzt werden, die „gewerbsmäßig oder in großem Umfang" Inhalte über Webseiten verbreiten oder zugänglich machen – also zum Beispiel von den Betreibern von sozialen Netzwerken oder Videoplattformen.

Die automatisierte Berücksichtigung von Alterskennzeichnungen im Netz trägt wesentlich dazu bei, dass jugendgefährdende Inhalte Kindern und

4 Abrufbar unter: https://t1p.de/dmstv (Kurzlink, PDF).

Jugendlichen nicht angezeigt werden. Sie ist damit eine tragende Säule im Jugendmedienschutz. Es ist sehr wichtig, dass dieses Schutzkonzept durch die Einführung von Paragraf 12 und 12a im JMStV auf Anbieter von Betriebssystemen und von bestimmten Apps ausgeweitet worden ist, die längst eine primäre Quelle des Medienkonsums von Kindern und Jugendlichen sind.

Aus datenschutzrechtlicher Sicht bedenklich ist allerdings, dass die mit der Alterskennzeichnung in einem engen Zusammenhang stehenden Systeme zur Altersverifikation im Jugendmedienschutz nicht nach datenschutzrechtlichen Kriterien bewertet werden. Die Datenschutzaufsichtsbehörden erachten zahlreiche Altersverifikationssysteme als nicht datenschutzkonform. In vielen Fällen wird der Grundsatz der Datenminimierung nicht ausreichend berücksichtigt. Bei der Altersverifikation werden oft deutlich mehr personenbezogene Daten verarbeitet, als für den eigentlichen Zweck erforderlich ist. Wird beispielsweise der Personalausweis für die Altersverifikation genutzt, werden einige auf dem Ausweis vorhandene Informationen wie Anschrift, Größe, Augenfarbe und Ausweisnummer nicht benötigt. Dennoch wird oft ein – ungeschwärztes – Foto vom Ausweis erbeten.

Die Datenschutzkonformität ist keine Anforderung bei der Bewertung der Altersverifikationssysteme durch die Kommission für Jugendmedienschutz (KJM). Ein positives Prüfergebnis erweckt allerdings bei den Anbietern den Eindruck, dass das Altersverifikationssystem allen rechtlichen Anforderungen entspricht. In der Stellungnahme wurde daher angeregt, die Erfüllung der datenschutzrechtlichen Anforderungen als Bewertungskriterium für Altersverifikationssysteme im JMStV aufzunehmen.

Digitale-Medien-Staatsvertrag

Die Rundfunkkommission hat am 22. Oktober 2025 Eckpunkte für eine zweiteilige Reform des Medienstaatsvertrages (MStV) beschlossen. Zum ersten Teil, dem DMStV, hat sie im Berichtsjahr eine öffentliche Anhörung durchgeführt. Die niedersächsische Datenschutzaufsicht und weitere Landesdatenschutzbehörden haben sowohl dem Rundfunkrat als auch ihren jeweiligen Staatskanzleien eine abgestimmte Stellungnahme zum DMStV übermittelt.

Der datenschutzrechtliche Fokus liegt auf einer geplanten Vorschrift, durch die der Einsatz eines Analysetools für die Webrecherche rechtlich legitimiert werden soll. Entsprechend der Gesetzesbegründung soll mit einem neuen Paragraf 109a im MStV eine Rechtsgrundlage für den Einsatz des KI-basierten Recherchetools KIVI geschaffen werden. Dieses wird allerdings bereits seit 2022 deutschlandweit von allen Landesmedienanstalten eingesetzt. Das KI-Tool KIVI durchsucht Angebote im Internet, einschließlich sozialer Netzwerke, auf rechtswidrige – medienrechtlich (und strafrechtlich) unzulässige – Inhalte. KIVI verarbeitet in sehr großem Umfang personenbezogene Daten und besondere Kategorien personenbezogener Daten. In unserer Stellungnahme gegenüber der Niedersächsischen Staatskanzlei haben wir verfassungs- und datenschutzrechtliche Bedenken geäußert.

Der LfD Niedersachsen hat nur begrenzte Kenntnisse über die Funktionsweise des KIVI-Tools und dies nicht datenschutzrechtlich umfassend geprüft. Es besteht aber der Eindruck, dass mit dem Einsatz des KIVI-Tools eine nicht verfassungskonforme Durchsuchung des Internets vorgenommen wird. Es wird anlasslos nach rechtswidrigen Inhalten auf nahezu allen sozialen Netzwerken recherchiert. Die Landesmedienanstalten scheinen dabei darüber hinauszugehen, was eigentliche Aufgabe oder Zielsetzung des Jugendmedienschutz-Staatsvertrags ist, da die Recherche auch Straftaten erfasst, für deren Aufdeckung originär die Strafverfolgungsbehörden zuständig sind.

Zwar ist es richtig und wichtig, dass Straftaten im Netz verhindert, aufgedeckt und verfolgt werden. Auch den Einsatz von datenschutzkonform ausgestalteten technischen Mitteln unterstützen wir. Die Medienanstalten beaufsichtigen Diensteanbieter und nicht die Einzelpersonen, die die Dienste nutzen.[5] Insbesondere bei den bei jugendlichen populären Plattformen im Internet (etwa Instagram, YouTube, TikTok oder Snapchat) werden die Inhalte nicht vom Anbieter bereitgestellt, sondern von den Nutzern der Plattformen. Diese erfüllen gegebenenfalls die im JMStV aufgeführten Straftatbestände.[6] Ob es sich bei der anlasslosen Recherche strafrechtlich relevanter Veröffentlichungen von Inhalten im Web um eine originäre Aufgabe der Medienanstalten handelt, erfordert eine tiefergehende Diskussion.

5 Gemäß § 20 JMStV.
6 Vgl. § 4 JMStV.

Darüber hinaus waren die im MÄStV vorgesehenen Voraussetzungen[7] für den Einsatz des KIVI-Tools bisher nicht ausreichend, um den Anforderungen der Datenschutz-Grundverordnung zu entsprechen.

Die Stellungnahme hat einen intensiven Austausch zwischen den Landesmedienanstalten, den zuständigen Staatskanzleien und dem Rundfunkrat ausgelöst. Unsere Bedenken werden sehr ernst genommen und es sind bereits Anpassungen erfolgt.

Mindestalter für Social Media – Sinnvolle Maßnahme zur Stärkung des Datenschutzes für Minderjährige? E.2.4

Die Verantwortung von Plattformbetreibern im Kinder- und Jugendschutz steht weltweit im Fokus intensiver Debatten. In Australien greift seit Dezember 2025 ein gesetzliches Verbot, das Kindern und Jugendlichen unter 16 Jahren die Nutzung von Social-Media-Plattformen über eigene Accounts untersagt. Das bereits ein Jahr zuvor erlassene Gesetz hat in Europa und in Deutschland die Diskussion um ein vergleichbares Verbot ausgelöst.[8] Bislang verfolgt die EU einen anderen Weg über einen weniger restriktiven Ansatz. Wir haben vor diesem Hintergrund die aktuelle Rechtslage in Deutschland und Europa überprüft und in einem juristischen Fachartikel als Beitrag für die politische Diskussion veröffentlicht.[9] Diese Diskussion ist zwar vorrangig dem Jugendschutzrecht zuzuordnen. Die Datenschutzaufsichtsbehörden erhalten allerdings einerseits regelmäßig Beschwerden hinsichtlich der Löschung von personenbezogenen Daten Minderjähriger aus Social-Media-Kanälen. Andererseits fordert auch das Datenschutzrecht eine Altersverifikation, die bisher technisch nicht wirkungsvoll umgesetzt wird.

In Europa und in Deutschland ist der Schutz Minderjähriger verfassungsrechtlich verankert und verpflichtet den Gesetzgeber, Kinder und Jugendliche vor vielfältigen Gefahren im Internet zu schützen. Die EU-Kommission kategorisiert diese Risiken in Inhalts-, Kontakt-, Verhaltens- und Verbrau-

7 Vgl. § 109 MStV.

8 Siehe auch „CDU-Vorstoß für Social-Media-Verbot unter 16 Jahren", heise online, https://heise.de/-11167139.

9 Dr. habil. Silke Jandt, Zeitschrift für Rechtspolitik 2025, 69.

cherrisiken. Dahinter verbergen sich zum Beispiel gewaltverherrlichende und pornografische Videos, Cyber-Grooming, Cybermobbing und Hate Speech sowie Influencer-Marketing. Die europäische Rechtslage wird maßgeblich durch den Digital Services Act (DSA), die Audiovisuelle-Mediendienste-Richtlinie (AVMD-RL), die Datenschutz-Grundverordnung (DSGVO) und die Richtlinie über unlautere Geschäftspraktiken (UGP-RL) geprägt. Der DSA verpflichtet insbesondere sehr große Online-Plattformen (VLOPs) mit EU-weit über 45 Millionen Nutzenden zu strukturellen Jugendschutzmaßnahmen, die ein hohes Maß an Privatsphäre und Sicherheit gewährleisten sollen. Dabei besteht keine proaktive Kontrollpflicht für nutzergenerierte Inhalte, sondern eine Haftung erst bei Kenntnis rechtswidriger Inhalte. Ein zentrales Verbot betrifft das Profiling und die darauf basierende Online-Werbung gegenüber Minderjährigen. Die EU-Kommission überwacht die Einhaltung dieser Vorschriften und hat bereits Verfahren gegen TikTok und Meta eingeleitet, um insbesondere Suchtpotenziale und Altersverifikationsmethoden zu prüfen. Ergänzend regelt die AVMD-RL[10] die Verantwortung von Video-Sharing-Plattformen für den Schutz Minderjähriger vor schädlichen Inhalten.

In Deutschland ergänzen nationale Gesetze wie das Jugendschutzgesetz, der Medienstaatsvertrag und der Jugendmedienschutz-Staatsvertrag die europäischen Vorgaben, greifen jedoch bei ausländischen Plattformen oft nicht effektiv. Die Schutzvorschriften adressieren primär Content-Provider, nicht aber die Betreiber sozialer Netzwerke, die vor allem durch ihr Geschäftsmodell – kostenlose Nutzung gegen personalisierte Werbung – selbst Risiken wie Sucht und Verbrauchertäuschung erzeugen.

Ab 16 in Australien – Stufenmodell in der EU

Das australische Verbot verfolgt einen restriktiven Ansatz mit einer starren Altersgrenze von 16 Jahren und verlangt angemessene, aber datenschutzkonforme Altersverifikationen, deren praktische Umsetzung jedoch eine besondere Herausforderung darstellt. In Europa und Deutschland wird hingegen bisher ein differenzierter Ansatz verfolgt, der altersgestufte Schutzmaßnahmen vorsieht und auf eine zuverlässige Altersverifikation mittels amtlicher Dokumente setzt, wie sie etwa die Kommission für Jugendme-

10 Die AVMD-Richtlinie soll unter anderem bei audiovisuellen Mediendiensten zu einem angemessenen Niveau des Verbraucher- und Kinderschutzes beitragen.

dienschutz (KJM) unterstützt. Die Wirksamkeit des europäischen Modells hängt wesentlich von der konsequenten Rechtsdurchsetzung gegenüber internationalen Plattformen ab, was durch die Zuweisung von Aufsichtsbefugnissen an die EU-Kommission im DSA verbessert werden soll.

Die EU hat sich mittlerweile ebenfalls für eine Altersgrenze für Social Media ausgesprochen.[11] Die Details sind dabei noch offen. Positiv hervorzuheben ist, dass die EU bereits an den technischen Voraussetzungen für eine mögliche Altersbeschränkung arbeitet und eine Verifizierungs-App zum Jugendschutz entwickelt. Diese soll ein verlässliches Altersnachweissystem bieten für Inhalte, die nicht für Kinder und Jugendliche geeignet sind, um zu verhindern, dass mögliche Altersgrenzen einfach umgangen werden können.

Wichtiger wäre es allerdings, auch an einer zuverlässigen Altersverifikation zu arbeiten, damit ein Nutzungsverbot nicht einfach umgegangen werden kann. Dies stellt zurzeit eines der größten Probleme in Australien dar. Ein Verbot weist sicher Vor- und Nachteile auf. Ebenso wie beim bisherigen europäischen Weg wird sich die Wirksamkeit der Maßnahmen vor allem darin zeigen, wie effektiv sie durchgesetzt werden. Dies erfordert eine effiziente Zusammenarbeit aller zuständigen Behörden.

Wichtiger wäre es allerdings, auch an einer zuverlässigen Altersverifikation zu arbeiten.

Mehr zum Thema Digitale Medien finden Sie unter https://lfd.niedersachsen.de/digitale-medien auf unserer Webseite.

11 Siehe auch „EU-Staaten wollen Altersgrenze für Social Media", tagesschau.de, https://www.tagesschau.de/ausland/europa/eu-fuer-mindestalter-in-sozialen-netzen-100.html

E.3 Wirtschaft

E.3.1 CEF 2025: Koordinierte Prüfung der EU-Datenschutzaufsichten zum Recht auf Löschung

Der LfD Niedersachsen hat sich im Frühjahr 2025 an der koordinierten Prüfung des Europäischen Datenschutzausschusses (EDSA) im Rahmen des Coordinated Enforcement Frameworks (CEF) zum Recht auf Löschung beteiligt. Hierbei schrieb die Behörde zehn Unternehmen aus unterschiedlichen Branchen und zehn Behörden in Niedersachsen an mit der Aufforderung, einen Fragebogen zum Umgang mit dem Recht auf Löschung[1] auszufüllen. Damit sollte geprüft werden, ob und inwieweit die Angeschriebenen fest implementierte Prozesse zum Recht auf Löschung vorweisen können, welche Erfahrungen die Verantwortlichen in der Praxis beim Bearbeiten solcher Anträge machen und welchen Schwierigkeiten sie dabei möglicherweise begegnen.

Auf der Grundlage des vom EDSA erarbeiteten Fragebogens hatten wir um Auskunft zu den jeweiligen Prozessen gebeten. Neben statistischen Werten wie der Anzahl der Anfragen, der Unternehmensgröße und dem Wirtschaftssektor wurden auch Fragen zu Kommunikationsprozessen und Löschverhalten gestellt.

Die Zahl der Löschanträge war weitaus geringer, als wir vermutet hatten.

Bei den angefragten Unternehmen und Verwaltungen aus Niedersachsen war die Zahl der Löschanträge weitaus geringer, als wir vermutet hatten. Den geprüften Unternehmen und Verwaltungen war grundsätzlich bekannt, welche Anforderungen sich aus Artikel 17 der DSGVO an den Umgang mit Löschanträgen ergeben. Bei der Prüfung stellten wir erfreulicherweise keine Mängel hinsichtlich des Umgangs mit Löschanträgen fest.

Im Hinblick auf die ebenfalls abgefragten Prozesse bei der Bearbeitung von Löschanträgen haben die geprüften Unternehmen und Verwaltungen die Regelungen der DSGVO eingehalten. Den Befragten waren ausweislich ihrer Antworten die Ziele und Anforderungen des Rechts auf Löschung bewusst.

1 Art. 17 DSGVO.

Neben Niedersachsen hatten sich auch noch andere Aufsichtsbehörden der Länder sowie die Bundesbeauftragte für den Datenschutz (BfDI) und Datenschutzbehörden aus anderen europäischen Ländern an der Prüfung beteiligt.

Im Ergebnis stellten auch die übrigen beteiligten deutschen Aufsichtsbehörden nur wenige bis gar keine Verstöße gegen die DSGVO fest. Bemerkenswert war, dass die von anderen deutschen Aufsichtsbehörden festgestellten Defizite überwiegend im öffentlichen Bereich auftraten.

Für Niedersachsen lässt sich mithin ein positives Fazit der CEF-Prüfung 2025 ziehen und festhalten, dass die untersuchten Regelungen in den geprüften Unternehmen und Verwaltungen bekannt sind, und soweit ersichtlich, korrekt angewendet werden. Es war daher nicht notwendig, weitergehende Prüfungen oder Abhilfemaßnahmen zu ergreifen. Nur in einigen wenigen Fällen war es erforderlich, dass die niedersächsische Datenschutzaufsicht die Befragten mit praktischen Hinweisen zum Umgang mit Löschanträgen unterstützt.

Smart-Data-Verfahren von Kreditinstituten mit neuer Einwilligung E.3.2

Seit einigen Jahren beobachten und beanstanden wir sogenannte Smart-Data-Verfahren bei niedersächsischen Kreditinstituten der genossenschaftlichen Finanzgruppe, in dessen Zusammenhang unsere Behörde verschiedene Maßnahmen ergriffen und auch Bußgelder verhängt hat. Mit Smart-Data-Verfahren generieren Kreditinstitute aus vorhandenen Daten ihrer Kundinnen und Kunden Score-Werte, mit denen sie prognostizieren, ob eine Kundin oder ein Kunde mit hoher Wahrscheinlichkeit ein bestimmtes Finanzprodukt abschließen wird, wenn er oder sie werblich darauf angesprochen wird. Unter anderem analysieren die Kreditinstitute dafür auch Zahlungsverkehrsdaten.

Die aufsichtsbehördlichen Maßnahmen bezogen sich im Kern darauf, dass die Kreditinstitute als Rechtsgrundlage die Interessenabwägung zugunsten ihres berechtigten Interesses anführten.[2] Unsere rechtliche Prüfung kam zu

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

dem Ergebnis, dass solche Verfahren zu eingriffsintensiv sind, um sie auf diese Rechtsgrundlage zu stützen.

Eine Arbeitsgruppe niedersächsischer Genossenschaftsbanken hat uns zum Ende des Berichtszeitraums den Entwurfstext einer neuen Einwilligung in die Verarbeitung personenbezogener Daten für diese Zwecke vorgestellt. Diese Einwilligung stellt nunmehr den Kundinnen und Kunden in einfacher und prägnanter Weise die Zwecke der Verarbeitung sowie die damit einhergehenden Verarbeitungsvorgänge dar. Kundinnen und Kunden haben zudem die Möglichkeit, eine Seite mit tiefergehenden Informationen aufzurufen.

Zudem setzen die Institute keine der bei Cookie-Einwilligungs-Bannern leider verbreiteten sogenannten Dark Patterns ein. Das bedeutet insbesondere, dass Schaltflächen nicht so gestaltet sind, dass Kundinnen und Kunden zu einer bestimmten Entscheidung gedrängt werden (z. B. durch grüne Hervorhebung, größere Schrift oder Bildumbrüche, die Scrollen erforderlich machen).

So wird sichergestellt, dass die betroffenen Kundinnen und Kunden frei entscheiden können, ob die Institute die entsprechenden Analysen durchführen sollen oder nicht. Damit entsprechen die Institute den datenschutzrechtlichen Anforderungen und die Kundinnen und Kunden behalten die Kontrolle über ihre personenbezogenen Daten. Die Kreditinstitute beabsichtigen, die geänderte Einwilligung Anfang 2026 ihren Kundinnen und Kunden zur Entscheidung vorzulegen.

E.3.3 Veraltete Exchange-Server: Auch 2025 noch Lücken in Niedersachsen

Wie bereits in den Vorjahren haben wir uns an niedersächsische Unternehmen gewandt, die Microsoft Exchange-Server mit kritischen Sicherheitslücken betreiben. Unser IT-Labor hatte im Jahr 2025 insgesamt 20 solcher Unternehmen identifiziert, die anschließend eine behördliche Aufforderung von uns erhielten, die Sicherheitslücken zu schließen.

Bei der Verarbeitung personenbezogener Daten müssen die Verantwortlichen, hier die Unternehmen, die Sicherheit der Verarbeitung gewährleisten. Zu den grundlegenden IT-Sicherheitsmaßnahmen gehört ein Patch- und

Änderungsmanagement.[3] Softwareanbieter stellen fortlaufend Updates bereit, die offenbar gewordene Sicherheitslücken schließen. Werden diese Updates nicht oder erst nach geraumer Zeit installiert, wird es Cyberkriminellen leicht gemacht, über kritische Sicherheitslücken Schadsoftware zu installieren und im schlimmsten Fall Unternehmensnetzwerke teilweise oder vollständig zu übernehmen. In den vergangenen Jahren hat sich zunehmend gezeigt, dass solche Angriffe automatisiert erfolgen und daher immer mehr Unternehmen jeder Größe betreffen. Die Folgen können für die betroffenen Unternehmen existenzbedrohend sein, aber auch die personenbezogenen Daten von Kundinnen und Kunden sowie Mitarbeiterinnen und Mitarbeitern sind erheblich gefährdet.

Das IT-Labor des LfD Niedersachsen nutzte Internet-Wide-Scanning-Datenbanken, um veraltete Exchange-Server zu identifizieren und dort bekannte Sicherheitslücken zu verifizieren. Nachdem wir Prüfverfahren eröffnet hatten, forderten wir die Unternehmen zur Schließung der Lücken auf. Wir kündigten zudem an, von unseren aufsichtsrechtlichen Befugnissen Gebrauch zu machen und die Schließung der Sicherheitslücken anzuordnen,[4] falls dies nicht innerhalb der gesetzten Frist erfolgt. Die Unternehmen zeigten sich jedoch kooperativ und meldeten zeitnah die Umsetzung der Maßnahmen. Alle Verfahren konnten deshalb mit Verwarnungen abgeschlossen werden.[5] Nebeneffekt unserer behördlichen IT-Sicherheitsüberprüfung: Die betreffenden Unternehmen werden vor potenziell existenzgefährdenden Hackerangriffen geschützt.

Nebeneffekt: Die Unternehmen werden vor potenziell existenzgefährdenden Hackerangriffen geschützt.

Mehr zum Thema Wirtschaft finden Sie unter https://lfd.niedersachsen.de/wirtschaft auf unserer Webseite.

3 Das Bundesamt für Sicherheit in der Informationstechnik stellt auf seiner Webseite einen entsprechenden IT-Grundschutz-Baustein bereit, siehe Kurzlink: https://t1p.de/bsi-patch (PDF).
4 Auf Grundlage von Art. 58 Abs. 2 Buchst. d DSGVO.
5 Art. 58 Abs. 2 Buchst. a DSGVO.

E.4 Gesundheit

E.4.1 Cyberangriff auf die Ameos-Gruppe: Auch niedersächsische Kliniken betroffen

Im Juli 2025 kam es zu einem Cyberangriff auf die IT-Infrastruktur der Ameos-Gruppe, die als Gesundheitsdienstleister bundesweit über 50 Kliniken betreibt. Bei dem Angriff hatten Unbefugte Zugriff auf personenbezogene Daten. Auch niedersächsische Standorte waren von dem Angriff betroffen. Aufgrund des bundesweiten Ausmaßes haben sich die zuständigen Datenschutzaufsichtsbehörden – unter anderem der LfD Niedersachsen – in einer Arbeitsgruppe zusammengefunden, um eine gemeinsame Aufklärung voranzutreiben.

Nach aktuellem Untersuchungsstand konnte an den niedersächsischen Standorten anders als bei einigen anderen Kliniken kein Abfluss personenbezogener Daten von Patientinnen und Patienten an Dritte festgestellt werden. Lediglich waren die betroffenen digitalen Daten für etwa 24 Stunden nicht abrufbar, da die IT-Systeme nach der Feststellung des Cyberangriffs im Rahmen einer Sofortmaßnahme vorübergehend abgeschaltet wurden. Die Auswirkungen auf die personenbezogenen Daten von Beschäftigten der Kliniken sind zum Zeitpunkt dieses Berichts noch Gegenstand weiterer Untersuchungen.

An niedersächsischen Standorten konnte bisher kein Abfluss festgestellt werden.

Die Ameos-Gruppe hat nach dem Vorfall auf ihrer Webseite öffentlich über die Datenpanne informiert und zugesagt, sukzessive auch individuelle Benachrichtigungen nachzuholen. Unserem Wunsch, über den aktuellen Stand der Untersuchung auch Patientinnen und Patienten zu informieren, an deren Kliniken keine Daten entwendet wurden, ist die Ameos-Gruppe leider bisher nicht gefolgt. Dies hätte den dort behandelten Patientinnen und Patienten zumindest Gewissheit verschafft, dass ihre Daten nicht von dem Datenleck betroffen waren.

Die Arbeitsgruppe steht weiterhin im Austausch mit Ameos mit dem Ziel, die Ursachen und die Auswirkungen des Angriffs auf die personenbezogenen Daten Betroffener vollständig aufzuklären und die technisch-orga-

nisatorischen Maßnahmen zum Schutz personenbezogener Daten zu verbessern.

Gesundheitsdaten in der Forschung: DSK gibt Orientierung E.4.2

Die Datenschutzkonferenz (DSK) hat sich im Jahr 2025 intensiv mit der Forschung mit Gesundheitsdaten befasst. Durch Entwicklung einheitlicher Antragsformulare und weiterer Auslegungshilfen unterstützt sie forschende Stellen bei der rechtskonformen Nutzung von Gesundheitsdaten zu Forschungszwecken.

Bereits im Jahr 2024 trat das Gesundheitsdatennutzungsgesetz (GDNG) in Kraft. Dieses schafft zusätzliche Rechtsgrundlagen für die Sekundärnutzung von Gesundheitsdaten, ermöglicht den Datenaustausch bei länderübergreifenden Forschungsvorhaben im Gesundheitsbereich und modifiziert die bestehenden datenschutzaufsichtsrechtlichen Zuständigkeiten.

Der Bundesgesetzgeber verfolgt mit dem GDNG das Ziel, den Zugang zu Gesundheitsdaten insbesondere zu Forschungszwecken deutlich zu erleichtern. Bis dahin waren die dafür anzuwendenden datenschutzrechtlichen Normen in verschiedenen Gesetzen des Bundes und der Länder geregelt. Dies hatte institutions- und länderübergreifende Forschungsvorhaben deutlich erschwert.

Bedarf für datenschutzrechtliche Unterstützung bei der Anwendung des GDNG

Die DSK hatte frühzeitig erkannt, dass das GDNG eine Vielzahl von Auslegungsfragen aufwirft, welche die Durchführung von Forschungsvorhaben hemmen könnten. Eine Unterarbeitsgruppe der Task Force Forschungsdaten hat in mehreren Sitzungen Musterformulare und Auslegungshilfen entwickelt. Hierdurch werden Verfahrensabläufe verschlankt. Zugleich wird den forschenden Stellen die gebotene Rechtssicherheit bei der Anwendung der neuen Vorschriften gegeben.

Unter anderem schafft das GDNG eine bundeseinheitliche Rechtsgrundlage für die gemeinsame Nutzung und Verarbeitung von Gesundheitsdaten zu Forschungszwecken durch öffentlich geförderte Zusammenschlüsse

datenverarbeitender Gesundheitseinrichtungen.[1] Nicht nur die rechtlichen Voraussetzungen müssen erfüllt sein, es bedarf zudem der Zustimmung der jeweils zuständigen Datenschutzaufsichtsbehörde. Um das Zustimmungsverfahren möglichst effizient zu gestalten, hat die DSK-Arbeitsgruppe für die forschenden Stellen ein einheitliches Antragsformular erstellt.[2]

Das GDNG regelt zudem die Datenschutzaufsicht bei länderübergreifenden Gesundheitsforschungsvorhaben.[3] Sofern die verantwortlichen Stellen der Datenschutzaufsicht unterschiedlicher Aufsichtsbehörden unterliegen, kann einer Aufsichtsbehörde die Federführung (Absätze 1 bis 3) oder die alleinige Zuständigkeit (Absatz 4) übertragen werden. Eine Orientierungshilfe der DSK[4] dient den verantwortlichen Stellen als Hilfestellung für die entsprechenden Anzeigeverfahren. Eine weitere Auslegungshilfe zu konkreten Auslegungsfragen im Kontext des GDNG stand zum Redaktionsschluss des Tätigkeitsberichts kurz vor ihrer Finalisierung.

Medizinische Forschungskooperationen mit Stellen in Drittländern

Als Reaktion auf vielfältige Nachfragen wurden in einer weiteren Unterarbeitsgruppe Anwendungshinweise zu den Anforderungen an Datenübermittlungen an Drittländer im Rahmen wissenschaftlicher Forschung zu medizinischen Zwecken entwickelt und von der DSK am 17. September 2025 beschlossen.[5]

Hiermit wird den forschenden Stellen der Rechtsrahmen für medizinische Forschungskooperationen mit Stellen außerhalb der EU beziehungsweise des EWR aufgezeigt. Dabei werden für die Datenübermittlung auf der ersten Stufe die Rechtsgrundlagen beleuchtet und auf der zweiten Stufe die Anforderungen des internationalen Datentransfers dargestellt.

Der DSK ist es mit den benannten Unterstützungsangeboten gelungen, den forschenden Stellen die gebotene Rechtssicherheit zu vermitteln. Hierdurch wird die zunehmend wichtige Forschung mit Gesundheitsdaten un-

1 § 6 Abs. 3 Satz 4 GDNG.
2 Verfügbar unter https://lfd.niedersachsen.de/forschung
3 § 5 GDNG.
4 Orientierungshilfe zur Zusammenarbeit mehrerer Aufsichtsbehörden im Rahmen von § 5 GDNG, Kurzlink: https://t1p.de/dsk-gdng (PDF).
5 Kurzlink: https://t1p.de/dsk-datenuebermittlung (PDF).

terstützt. Zugleich wird erneut deutlich, dass wissenschaftliche Forschung und Datenschutz in keinem Widerspruch zueinanderstehen.

Mehr zum Thema Gesundheit finden Sie unter https://lfd.niedersachsen.de/gesundheit auf unserer Webseite.

E.5 Verwaltung, Kommunen und Schulen

E.5.1 Datenschutzkonforme Information der Öffentlichkeit durch Kommunen

Im vergangenen Jahr haben uns einige Hinweise zu Bekanntmachungen und Veröffentlichungen durch niedersächsische Kommunen erreicht. Diese betrafen unterschiedliche Bereiche von Altersjubiläen bis hin zu Wahlprüfungen.

Vor Sitzungen kommunaler Vertretungen werden häufig Dokumente und Informationen über sogenannte Bürgerinformationssysteme veröffentlicht. Regelmäßig geben Städte und Gemeinden Informationen heraus. Sind hierin personenbezogene Daten enthalten, ist das Datenschutzrecht zu beachten.

Zwischen Sitzungs- und Internetöffentlichkeit unterscheiden

Im September 2026 finden in Niedersachsen Kommunalwahlen statt. Bei den vorangegangenen Wahlen kam es insbesondere bei Bürgermeisterwahlen zu Einsprüchen nach dem Niedersächsischen Kommunalwahlgesetz (NKWG).[1] Über diese entscheidet der Rat in öffentlicher Sitzung und es werden die Beteiligten angehört.[2]

Den Ratsmitgliedern wird ein solcher Einspruch häufig im Vorfeld über das Ratsinformationssystem zur Verfügung gestellt. Die Mitglieder des Rates sind dabei zur Amtsverschwiegenheit[3] verpflichtet.

Sofern die Wahleinsprüche auch über das Internet bereitgestellt werden sollen, ist zu prüfen, ob diese personenbezogenen Daten enthalten. Denn: Wer konkret Wahleinspruch erhoben hat, ist für die Öffentlichkeit nicht relevant.

Zwar wird ein solches Wahlprüfungsverfahren öffentlich durchgeführt und der Rat hört die Beteiligten dabei an. Jedoch dürfen dabei oder im Vorfeld keine personenbezogenen Daten von Beteiligten offengelegt werden.

1 Nach §§ 46, 47 NKWG.
2 Nach § 47 Absatz 2 NKWG.
3 Nach § 40 Niedersächsisches Kommunalverfassungsgesetz (NKomVG).

Das NKWG regelt hierzu lediglich die Durchführung vor Ort während der Ratssitzungen. Es ist also zwischen der Sitzungsöffentlichkeit und der Internetöffentlichkeit zu unterscheiden, denn das NKWG legitimiert keine Offenlegung von personenbezogenen Daten für die Öffentlichkeit außerhalb der Ratssitzung. Es fehlt somit an einer Rechtsgrundlage, die die Veröffentlichung über das Internet erlaubt.

In Veröffentlichungen der Kommunen sind personenbezogene Daten zu schwärzen.

In Veröffentlichungen der Kommunen sind wegen der nicht vorhandenen Rechtsgrundlage personenbezogene Daten zu schwärzen, um die nicht rechtmäßige Preisgabe zu verhindern.[4]

Alters- und Ehejubiläen: Abruf aus Melderegister

Die in den Kommunen auf Grundlage des Bundesmeldegesetzes (BMG) geführten Melderegister enthalten naturgemäß eine Vielzahl personenbezogener Daten. Deren Nutzung ist nur auf Grundlage des BMG und den weiteren dazu ergangenen Gesetzen und Verordnungen zulässig.

Beispielsweise erhalten Jubilare zu besonderen Alters- und Ehejubiläen über die Kommunen Post und eine Anerkennung. Zu solchen Anlässen können personenbezogen Daten aus dem Melderegister übermittelt werden.[5]

Zudem dürfen Meldebehörden Angaben zu Alters- und Ehejubiläen auf Anfrage[6] unter anderem an die Presse übermitteln. Es besteht jedoch die Möglichkeit, den Datenübermittlungen zu einzelnen im BMG genannten Zwecken grundsätzlich zu widersprechen.[7] Die Offenlegung zu nicht im BMG genannten Zwecken ist nicht zulässig.

In der Praxis scheinen die Regelungen nicht immer klar zu sein. So wurde unserem Haus mitgeteilt, dass eine Samtgemeinde in Niedersachsen eine monatliche Hauswurfsendung mit Neuigkeiten aus der Kommune, unter anderem Daten von Ehejubiläen, verteilt. Zu den Jubilaren wurden auch

4 Hinweise zum Schwärzen von Dokumenten: https://lfd.niedersachsen.de/243671.html
5 Die entsprechenden Regelungen enthält das Niedersächsische Ausführungsgesetz zum Bundesmeldegesetz (Nds. AG BMG).
6 Nach § 50 Absatz 2 BMG.
7 Nach § 50 Absatz 5 BMG.

Namen und Anschriften veröffentlicht. Zwar hat die Samtgemeinde im Rahmen der Veröffentlichungen darauf hingewiesen, dass dem widersprochen werden kann, jedoch hat die Kommune nicht berücksichtigt, dass sie nach dem BMG nicht berechtigt ist, diese Angaben zu veröffentlichen. Hinzu kam, dass im vorliegenden Fall ein Betroffener der Veröffentlichung rechtzeitig widersprochen hatte, sein Widerspruch blieb jedoch unberücksichtigt.

Sofern Kommunen die örtliche Gemeinschaft über Alters- und Ehejubiläen informieren möchten, benötigen sie hierfür zwingend in jedem Einzelfall eine Einwilligung der betroffenen Personen. Ein Rückgriff auf das Melderecht ist nicht möglich, weil die Regelung im BMG eine solche Veröffentlichung eben nicht vorsieht.

E.5.2 Anwendung des geänderten Onlinezugangsgesetzes (OZG 2.0) – Fragen aus der Praxis

Ende 2024 hat die Datenschutzkonferenz (DSK) eine Orientierungshilfe für die Auslegung des geänderten und im Juli 2024 in Kraft getretenen Onlinezugangsgesetzes (OZG 2.0) veröffentlicht, die maßgeblich von unserer Behörde gestaltet wurde.[8] Im Jahr 2025 nahm die DSK diverse Fragen aus der Praxis zum Anlass, die Orientierungshilfe um die entsprechenden Antworten und Hinweise zu erweitern. Die Änderungen beziehen sich vor allem auf die folgenden drei Fragestellungen.

Zum einen hat die Orientierungshilfe präzisiert, wann ein „länderübergreifender Onlinedienst" gemäß dem OZG vorliegt. Dies hat Auswirkungen auf die kraft Gesetzes zugewiesene datenschutzrechtliche Verantwortlichkeit der betreibenden Behörde und die Rechtsgrundlage der Verarbeitung. Der Gesetzgeber hat sich im OZG bewusst für eine technikneutrale Definition entschieden, die von einem „eigenständigen" elektronischen Angebot spricht, das auch „verfahrensunabhängig" und „länderübergreifend" bereitgestellt werden kann.[9] Der Begriff „Onlinedienst" ist weit auszulegen, da sonst – bei einer zu engen Auslegung – durch die technische Ausgestaltung eines Dienstes oder durch etwaige Zusatzfunktionen die Regelungen

8 Siehe Tätigkeitsbericht 2024, Kapitel I.5.
9 § 2 Abs. 8 OZG.

des OZG[10] gezielt umgangen werden könnten. Die Orientierungshilfe erklärt anhand von Beispielen, wie die Begriffe „eigenständig", „verfahrensunabhängig" und „länderübergreifend" genau zu verstehen sind.

Zum zweiten weist die Orientierungshilfe darauf hin, dass die Datenschutzerklärung des bestehenden länderübergreifenden Onlinedienstes aufgrund des OZG zu überprüfen und gegebenenfalls anzupassen ist. In der bisherigen Datenschutzerklärung war in vielen Fällen die jeweilige Fachbehörde als Verantwortliche anzugeben. Nun ist zu prüfen, welche Behörde für den Betrieb des länderübergreifenden Onlinedienstes nach dem Landesorganisationsrecht zuständig ist. Diese Behörde ist in der Folge auch für die Verarbeitung im länderübergreifenden Onlinedienst verantwortlich und in der Datenschutzerklärung als Verantwortliche anzugeben.[11]

Drittens klärt das Dokument, wie mit datenschutzrechtlichen Vereinbarungen über länderübergreifende Onlinedienste umzugehen ist, die vor dem Inkrafttreten des OZG 2.0 abgeschlossen wurden. Handelte die den länderübergreifenden Onlinedienst betreibende Behörde beispielsweise vor dem Inkrafttreten des OZG-Änderungsgesetzes als Auftragsverarbeiter für die nachnutzenden Behörden und hat sie mit diesen hierzu eine Auftragsverarbeitungsvereinbarung abgeschlossen, ist diese Vereinbarung mit dem Inkrafttreten des OZG-Änderungsgesetzes als überholt anzusehen.

Wir werden auch weiterhin die Entwicklungen um die Anwendung und Umsetzung des Onlinezugangsgesetzes beobachten und Fragestellungen aus der Praxis aufgreifen. Die überarbeitete Orientierungshilfe ist auf der Webseite der DSK veröffentlicht.[12]

Uneinheitlicher Einsatz privater Tablets im Schulunterricht schwächt Datenschutz E.5.3

Das Land Niedersachsen hat beschlossen, dass die Schülerinnen und Schüler ab Klasse 7 stufenweise beginnend mit dem Schuljahr 2026/2027 landeseigene Tablets für den Schulunterricht erhalten werden. Bis dieses Vorhaben umgesetzt ist, werden die Tablets in den meisten Schulen weiterhin

10 §§ Abs. 8, 8a OZG.
11 § 8a Abs. 4 OZG.
12 Kurzlink: https://t1p.de/dsk-ozg (PDF).

Der Einsatz privater Tablets in der Schule birgt zahlreiche datenschutzrechtliche Probleme.

durch die Eltern finanziert. Dies birgt vielfältige datenschutzrechtliche Probleme: Zum einen müssen die Schulen die Privatgeräte mittels eines Mobile Device Management (MDM) in ihre IT-Infrastruktur einbinden, damit es nicht zu einer Vermischung von schulischen und privaten Inhalten kommt. Mangels einer landeseinheitlichen Vorgabe handhaben die niedersächsischen Schulen dies jedoch zurzeit sehr unterschiedlich. Dadurch ist nicht gewährleistet, dass die schulischen Netzwerke tatsächlich vor Angriffen mittels Schadsoftware geschützt sind. Zudem haben die schulischen IT-Administrationen beim Aufspielen des MDM umfassende Einsichts- und Eingriffsmöglichkeiten in die privaten Daten auf den Endgeräten der Schülerinnen und Schüler.

Bedarf verbindlicher Vorgaben des Landes zur Verbesserung des Datenschutzes

Ein wirksamer Schutz der persönlichen Daten der Schülerinnen und Schüler ist nur mit den vom Land beschafften Tablets gewährleistet. Bis dahin ist die Landesregierung in der Pflicht, den Datenschutz auch beim Einsatz privat beschaffter Geräte im Schulunterricht zu verbessern. Wir haben dem Kultusministerium Anfang 2025 unsere Leitlinien zum MDM übermittelt. Demnach kann der Einsatz privater Endgeräte im schulischen Kontext aus Gründen der Datensicherheit nur akzeptiert werden, wenn ein an die

Schule gerichteter Erlass des Kultusministeriums folgende Vorgaben enthält:

- Die Administrationsrechte liegen vollumfänglich bei der schulischen Administration und nicht bei den Schülerinnen und Schülern. Dies betrifft sowohl den Bereich der schulischen als auch der privaten Nutzung der Geräte. Die schulische Administration entscheidet, welche Konfigurationen und Installationen (insbesondere Apps) auf dem privaten Endgerät vorgenommen beziehungsweise aufgespielt werden.
- Es ist durch Auswahl eines geeigneten MDM sicherzustellen, dass beispielsweise die Geräte unverzüglich die neuesten Sicherheitsupdates erhalten und die Schülerinnen und Schüler selber keine eigenen Konfigurationen und keine eigenen Installationen am Gerät vornehmen können.
- Das Kultusministerium erstellt eine „Whitelist“[13] der im Rahmen eines „Bring your own Device“ einsetzbaren datenschutzkonformen Produkte (MDM-Tools, Apps, weitere Softwareangebote), die sowohl die schulische als auch die private Nutzung der Geräte betrifft und sorgt somit für Rechtssicherheit und einheitliche Handhabung in den Schulen.
- Es ist eine Trennung zwischen dem Schulverwaltungsnetzwerk und dem pädagogischen Netzwerk vorzusehen.

Wir haben im Berichtsjahr in mehreren Arbeitsgesprächen versucht, das Kultusministerium von der Notwendigkeit eines an die Schulen gerichteten Erlasses zu überzeugen. Dies war bislang leider erfolglos. Stattdessen handhaben die Schulen den Einsatz privater Endgeräte im Schulunterricht weiterhin in Eigenregie, was zu Lasten des Datenschutzes der oftmals minderjährigen Schülerinnen und Schüler geht. Dieser Zustand bleibt also höchst unbefriedigend und problematisch.

Der Zustand bleibt höchst unbefriedigend und problematisch.

Ausblick

Mit dem Umsetzen unserer Datenschutzleitlinien würde das Kultusministerium nicht nur den Einsatz privater Tablets in der Übergangszeit datenschutzrechtlich sicher gestalten, sondern auch wichtige Vorarbeiten für die Einführung landeseigener Tablets leisten. Denn auch wenn sich viele der derzeitigen datenschutzrechtlichen Probleme mit landeseigenen Tablets

13 „Weiße Liste“, auch Positivliste genannte Zusammenstellung geprüfter und vertrauenswürdiger Apps und Dienste.

leichter lösen lassen: Auch danach bleiben erhebliche Steuerungspflichten für das Kultusministerium, zum Beispiel mit Blick auf die Auswahl geeigneter MDM oder Apps.

Wir werden unsere Bemühungen fortsetzen, für datenschutzkonforme digitale Lernmittel an den niedersächsischen Schulen zu sorgen.

Mehr zum Thema Kommunen finden Sie unter https://lfd.niedersachsen.de/kommunen und mehr zu Schulen unter https://lfd.niedersachsen.de/schulen auf unserer Webseite.

Videoüberwachung E.6

Gemeinsame Gewerbekontrollen mit Polizei, Zoll und kommunalen Partnern E.6.1

Im Berichtszeitraum nahmen Mitarbeiterinnen und Mitarbeiter des Landesbeauftragten an koordinierten Kontrollaktionen anderer Behörden teil, auch im Rahmen der deutschlandweiten Joint Action Days im November 2025. Bei diesen unangemeldeten Kontrollen in Cafés, Bars, Kiosken, Spielotheken und Gewerbeobjekten hat unsere Behörde die Anlagen zur Videoüberwachung erfasst und in den meisten Fällen Prüfverfahren nach der DSGVO eingeleitet.

Die Joint Action Days waren eine konzertierte Aktion zur Bekämpfung organisierter krimineller Strukturen im gewerblichen Umfeld. Polizei, Zoll und kommunale Behörden kontrollierten zahlreiche Betriebe. Als Datenschutzaufsicht führten wir in diesem Zuge unangekündigte Vor-Ort-Kontrollen durch und konnten dabei mit den Verantwortlichen in einen direkten Austausch treten, beraten und bei hinreichendem Verdacht auf Verstöße auch formelle Prüfverfahren einleiten.

In fast allen kontrollierten Betrieben waren Videoüberwachungsanlagen installiert. Häufig waren dabei Bereiche miterfasst, in denen eine Überwachung unzulässig ist, etwa Sitzbereiche der Gäste oder Pausenräume für Beschäftigte und deren Arbeitsbereiche. Oftmals fehlte auch ein Hinweis auf die Videoüberwachung.[1] Insgesamt waren bei der Mehrzahl der Anlagen augenscheinlich Verstöße gegeben. Einige der festgestellten Mängel konnten bereits während der Kontrollen vor Ort durch gezielte Hinweise behoben werden. In der Folge konnten diese Verfahren ohne weitere Maßnahmen abgeschlossen werden. In den meisten anderen Fällen dauert die Bearbeitung noch an.

Die Kontrollen verdeutlichen die Bedeutung einer sorgfältigen Überprüfung der Videoüberwachung in gewerblichen Bereichen, um den Schutz der personenbezogenen Daten der Bürgerinnen und Bürger zu gewährleisten.

1 Ausführliche Informationen und Beispiele für die Hinweisbeschilderung bei einer Videoüberwachung: https://www.lfd.niedersachsen.de/158959.html

E.6.2 Beobachtung kommunaler Wertstoffinseln mittels Videotechnik

Ein zunehmendes Problem vieler Kommunen ist die unsachgemäße Entsorgung von Abfall an den Standorten von Containern zur Sammlung von Wertstoffen wie Glas und Papier. Eine Videoüberwachung von Wertstoffinseln kann unter Erfüllung strenger Voraussetzungen eine zulässige Gegenmaßnahme sein.

Illegale Müllentsorgung

Recycling ist eine gute Sache. Leider werden an Wertstoffinseln auch immer wieder sonstige Abfälle abgelegt – teils in erheblichen Mengen und darunter auch Sperrmüll und Sondermüll. Den Kommunen entstehen für vermehrte Kontrollen, den Abtransport und die Entsorgung der Abfälle sowie die Reinigung der Flächen hohe Kosten.

Eine Stadt in Niedersachsen hatte bereits über Jahre verschiedene Maßnahmen durchgeführt, um der häufigen Vermüllung einer besonders stark betroffenen Wertstoffinsel entgegenzuwirken. Die Polizei führte auf Bitten der Stadt dort vermehrt Streifendienst durch, ebenso der kommunale Ordnungsdienst. Eine optische Abgrenzung des Ortes mittels einer Holzumrandung wurde errichtet und große, leicht verständliche Schilder mit Hinweisen zur zulässigen und zur unzulässigen Entsorgung am Eingangsbereich angebracht. Zusätzliche Container wurden aufgestellt und tägliche Reinigungen, auch am Wochenende, wurden beauftragt. Leider fruchteten diese Maßnahmen nicht.

Lösungsansatz Videoüberwachung

Deshalb plante die Stadt, eine offene Videobeobachtung der Wertstoffinsel in Form eines Livemonitorings zu starten. Echtzeit-Videobilder sollten auf einem Monitor in der Stadtverwaltung zu sehen sein, um so das Geschehen auf dem Platz überwachen zu können. Vor dem Start der Maßnahme informierte uns die Stadt. Daraus entstand ein Austausch über die Voraussetzungen, die für eine Videobeobachtung vorliegen müssen, aber auch über den Umfang möglicher anderer Maßnahmen. Problematisch war insbesondere die Frage, inwieweit eine Videobeobachtung überhaupt geeignet ist, schon das illegale Ablegen von Müll tatsächlich zu verhindern.

Im Ergebnis erweiterte die Stadt die Videoanlage um eine Lautsprecheranlage. Damit können nun Personen, bei denen ein Verdacht besteht, dass diese gegen die Entsorgungsvorschriften verstoßen, direkt angesprochen werden. Dies soll Medienberichten zu dem Thema zufolge zu guten Ergebnissen geführt haben.

Neben weiteren Medienanfragen erreichten uns zu dem Thema auch Anfragen anderer Gemeinden. In einem gemeinsamen Forum mit Datenschutzbeauftragten niedersächsischer Kommunen war es daraufhin Thema, inwieweit eine Videobeobachtung von Wertstoffinseln möglich ist. Die wesentlichen Gesichtspunkte dafür lassen sich wie folgt zusammenfassen.

Rechtlicher Rahmen

Der Einsatz von Videotechnik durch kommunale Stellen ist zum Zwecke der Gefahrenabwehr denkbar, also hier zur Verhinderung der illegalen Entsorgung von nicht dafür vorgesehenem Müll auf Wertstoffinseln. Allerdings müssen in jedem konkreten Einzelfall die Voraussetzungen der in Betracht kommenden Rechtsgrundlage[2] erfüllt sein.

Zum einen muss es auf der betroffenen Wertstoffinsel bereits wiederholt zu Straftaten oder nicht geringfügigen Ordnungswidrigkeiten gekommen sein. Dies muss nachweisbar dokumentiert worden sein. Zudem muss die Überwachung des Ortes für die Verhinderung weiterer illegaler Müllentsorgung erforderlich sein.

Das bedeutet zunächst, dass es stets einer transparenten Information der Bürgerinnen und Bürger bedarf, damit jederzeit die Anforderungen an eine „offene" Überwachung sichergestellt sind. Denn eine Videoüberwachung kann regelmäßig nur dann präventiv wirken, wenn diese auch seitens der handelnden Personen erkannt wird.

Weiter muss die Möglichkeit für ein unmittelbares Eingreifen seitens des Betreibers der Wertstoffinsel sichergestellt sein. Andernfalls wäre die Maßnahme nicht geeignet, weitere Taten zu verhüten.

Insofern kann nur dann eine Videoüberwachung rechtmäßig betrieben werden, wenn während des Betriebs der Videoanlage auch tatsächlich ein

2 § 32 Absatz 1 Nummer 1 des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG).

Live-Monitoring durch Beschäftigte der Gemeinde erfolgt und eine unmittelbare Eingriffsmöglichkeit zur Verhinderung der Müllablagerung besteht.

Zudem muss geprüft und gegebenenfalls auch erfolglos angewendet worden sein, ob weniger eingreifende, alternative Maßnahmen wie zum Beispiel vermehrte Vor-Ort-Kontrollen, Ausleuchtung, Hinweisbeschilderungen oder Einfriedungen für einen Erfolg gesorgt haben oder für Abhilfe sorgen könnten.

Schließlich muss auch geprüft werden, ob in jedem Einzelfall die mit der Videoüberwachung verursachten Eingriffe in die Grundrechte der sich in den allermeisten Fällen regelkonform verhaltenen Bürgerinnen und Bürgern durch die Verhinderung der illegalen Müllentsorgung aufgewogen werden können. Beispielsweise erscheint in diesem Zusammenhang eine regelmäßige Evaluierung der Notwendigkeit zum weiteren Betrieb der Videoüberwachung erforderlich.

Eine offene Videobeobachtung kann für Kommunen in der Form des Livemonitorings also ein Hilfsmittel bei der Bekämpfung illegaler Müllablagerungen sein. Es sind jedoch enge Voraussetzungen zu erfüllen, insbesondere die Eignung, zukünftige Taten zu verhindern sowie das Fehlen milderer Maßnahmen. Denn sich regelkonform verhaltene Bürgerinnen und Bürger sind ebenfalls von der Maßnahme betroffen. Dies gilt es bei allen erwünschten Effekten nicht zu vergessen.

Sicherheit E.7

Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes E.7.1

Mit dem aktuellen Gesetzentwurf zur Änderung des Niedersächsischen Polizei- und Ordnungsbehördengesetzes (NPOG)[1] will die Landesregierung diverse neue und erweiterte Befugnisnormen für die niedersächsische Polizei schaffen. Im Fokus steht dabei als weitreichende Neuerung der beabsichtigte Einsatz von Künstlicher Intelligenz (KI).

Neue Befugnisse im Gesetzentwurf

Der Gesetzentwurf sieht eine Vielzahl an neuen Befugnissen für die Polizei vor. Dies ist auf die Dynamik neuer technischer Entwicklungen und aktueller Bedrohungsszenarien zurückzuführen. Angesichts dessen entwickeln sich die Anforderungen an die Sicherheitsbehörden im Bereich der Gefahrenabwehr und der Kriminalitätsbekämpfung stetig weiter.

So sind etwa Regelungen zur intelligenten Videoüberwachung, zur biometrischen Echtzeit-Fernidentifizierung, zum nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet und zur automatisierten Datenanalyse vorgesehen.

Zudem soll eine Ausweitung des Einsatzes von Fußfesseln in Fällen von häuslicher Gewalt erfolgen. Auch sollen unter anderem Rechtsgrundlagen für den Einsatz von Drohnen geschaffen werden.

Schriftliche Stellungnahme gegenüber dem Innenministerium

Das Niedersächsische Ministerium für Inneres, Sport und Digitalisierung hatte uns im Rahmen der Verbandsanhörung die Möglichkeit zur Stellungnahme gegeben. Dabei äußerten wir mit unserer Stellungnahme vom 29. September 2025 schwerpunktmäßig Kritik an den geplanten neuen Befugnissen mit hoher Eingriffstiefe in Grundrechte.

1 Landtags-Drucksache 19/8942.

Zur intelligenten Videoüberwachung[2] forderten wir etwa aufgrund des besonderen Eingriffsgewichts durch Art und Umfang der Überwachung höhere Anforderungen an die Rechtfertigung des Eingriffs in Grundrechte.

Bei der Regelung zur biometrischen Echtzeit-Fernidentifizierung[3] rügten wir unter anderem den vorgesehenen Anwendungsbereich. Dieser erscheint uns insbesondere mit Blick auf die Vielzahl der von der Maßnahme betroffenen Personen und die räumliche Reichweite zu weitreichend.

Der geplante nachträgliche biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet[4] lässt nach unserer Bewertung eine hinreichende Auseinandersetzung mit den Vorgaben der europäischen KI-Verordnung[5] und der Einhaltung ihrer Vorgaben (zum Beispiel zu verbotenen KI-Praktiken) vermissen. Es fehlen Hinweise zur konkreten technischen Umsetzung. Diese sind allerdings entscheidend, da sich die Maßnahmen auf der Grenze zwischen Hochrisiko-KI-Systemen und in der KI-Verordnung geregelten Verboten von KI-Praktiken bewegen. Darüber hinaus erscheint auch die Menge an Datenbeständen, die für den automatisierten Abgleich herangezogen werden soll, zu ungenau definiert und damit zu unbestimmt und zu weitreichend.

Die Regelung zur automatisierten Datenanalyse[6] stellt nach unserer Einschätzung einen Paradigmenwechsel in der Polizeiarbeit dar. Die automatisierte Datenanalyse setzt voraus, dass alle bisher vorgangsbezogen gespeicherten Daten der Polizei auf einer Analyseplattform zusammengeführt werden. Damit würde die Zweckbindung aufgehoben. Zudem hält die Polizei nicht nur personenbezogene Daten von Verdächtigen, sondern auch von Zeugen, Opfern und auch Unbeteiligten vor, es sollen Daten aus strafrechtlichen Ermittlungsverfahren und

Die Regelung zur automatisierten Datenanalyse stellt einen Paradigmenwechsel in der Polizeiarbeit dar.

2 § 32 Abs. 4 des Gesetzentwurfs.
3 § 32b des Gesetzentwurfs.
4 § 32c des Gesetzentwurfs.
5 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz).
6 § 45a des Gesetzentwurfs.

aus Internetquellen einfließen. Verfassungsrechtlich höchst problematisch ist auch die Einbeziehung von Telekommunikationsdaten, wobei auch die Inhalte von Gesprächen umfasst wären. Zudem kritisierten wir die fehlende Begrenzung des Einsatzes von KI-Systemen.

Daneben gaben wir Empfehlungen zur datenschutzkonformen Ausgestaltung ab, wie etwa zu den Regelungen zur Ausweitung des Einsatzes von Fußfesseln in Fällen von häuslicher Gewalt oder zu der Schaffung von Rechtsgrundlagen für den Einsatz von Drohnen.

Begrüßt haben wir unter anderem die in Paragraf 33 Absatz 6 neu vorgesehene Prüfung, ob bei erlangten Informationen aus Datenerhebungen mit besonderen Mitteln und Methoden der Kernbereich privater Lebensgestaltung tangiert ist. Auch die darin enthaltene Festlegung, im Zweifelsfall den Datenschutzbeauftragten einzubinden, hoben wir ausdrücklich positiv hervor.

Anhörung im Ausschuss

Nach Ende des Berichtszeitraums hat uns der Ausschuss des Landtags für Inneres und Sport neben einer schriftlichen Stellungnahme im Rahmen einer öffentlichen Anhörung am 26. Februar 2026 die Möglichkeit zur Stellungnahme gegeben. Da – trotz der schwerwiegenden Kritik – das Innenministerium unsere Empfehlungen weitestgehend unberücksichtigt ließ oder sie ablehnte, erneuerten wir unsere Bewertungen, nun gegenüber dem Innenausschuss. Wir haben im Ausschuss deutlich gemacht, dass unsere Kritikpunkte nun umso dringender im aktuellen parlamentarischen Verfahren Gehör finden sollten. Das Ziel sollte es sein, einen angemessenen Ausgleich zwischen Sicherheitsinteressen und Grundrechten der Bürgerinnen und Bürger unter Einhaltung der datenschutzrechtlichen Vorgaben zu finden.

E.7.2 Parkraumüberwachung: Landeshauptstadt Hannover fotografiert ohne Rechtsgrundlage

Aufgrund einer datenschutzrechtlichen Beschwerde im Zusammenhang mit der Feststellung von Parkverstößen bei der Nutzung von Parkscheiben hat die Niedersächsische Datenschutzaufsicht die Landeshauptstadt Hannover (LHH) aufgefordert, die Rechtsgrundlage für die hier praktizierte Datenverarbeitung zu nennen.

Das bis dahin betriebene Vorgehen der LHH sah vor, dass zur Ermittlung von Parkraumverstößen mehrere Beweisfotos angefertigt wurden: Ein Foto während der gültigen Parkdauer zur Parkposition der Reifen und ein späteres Foto, um gegebenenfalls ein rechtswidriges Nachstellen der Parkscheibe bei identischer Parkposition zu dokumentieren.

Gegen Grundsatz der Rechtmäßigkeit verstoßen

Die LHH konnte auf mehrfache Nachfragen keine Rechtsgrundlage für das beschriebene Vorgehen im Rahmen der Parkraumüberwachung nennen. Da auch nach unserer Auffassung keine entsprechenden Befugnisnormen existieren, hat die LHH personenbezogene Daten, unter anderem Kfz-Kennzeichen, ohne gesetzliche Grundlage verarbeitet. Dies ist nicht mit dem datenschutzrechtlichen Grundsatz der Rechtmäßigkeit[7] vereinbar.

Die Landeshauptstadt hat personenbezogene Daten ohne gesetzliche Grundlage verarbeitet.

Damit war die Beschwerde gegen die Praxis der Landeshauptstadt Hannover begründet. Sie stellte in der Folge das bis dahin betriebene Verfahren ein. Gegenüber der LHH wurde eine aufsichtsbehördliche Warnung[8] ausgesprochen, um künftige Datenschutzverstöße nach Möglichkeit zu verhindern.

7 § 47 Nr. 1 BDSG/§ 25 Abs. 1 Nr. 2 NDSG.
8 § 57 Abs. 5 S. 1 NDSG.

F Abgeschlossene Bußgeldverfahren

Abgeschlossene Bußgeldverfahren

Die niedersächsische Datenschutzaufsicht hat Bußgelder in Höhe von rund 705.000 Euro im Jahr 2025 verhängt.[1] Viele der verhängten Geldbußen betrafen erneut die unzulässige Videoüberwachung – besonders hohe Summen waren für unzulässige Profilbildung zu Werbezwecken bei Kreditinstituten fällig.

Insgesamt hat unsere Behörde 80 neue Fälle unter Gesichtspunkten einer möglichen Geldbuße geprüft. Im gleichen Zeitraum haben wir 34 Erstbescheide in Bußgeldsachen erlassen, die sich zum Teil auf Fälle bezogen, die bereits in den Vorjahren eingeleitet wurden. Von diesen Erstbescheiden sind 26 rechtskräftig geworden, weil kein Einspruch eingelegt wurde. Die nicht mit Geldbußen abgeschlossenen Verfahren sind entweder noch anhängig, waren nicht bußgeldwürdig, wurden eingestellt oder wurden an andere zuständige Stellen abgegeben.

Die Erstbescheide wurden gegenüber Verantwortlichen aus den Bereichen Gastgewerbe, Handel, Finanzdienstleistungen, Fitnessstudios, Baugewerbe, Logistik, Produktion sowie gegen natürliche Personen erlassen. Die natürlichen Personen haben die Verstöße teilweise als Inhaberinnen beziehungsweise Inhaber von Unternehmen begangen.

Geahndet haben wir Verstöße gegen die Artikel 5, 6, 9, 13, 30, 31, 58 beziehungsweise 83 Absatz 5 Buchstabe e der Datenschutz-Grundverordnung (DSGVO). Bei den Verstößen handelte es sich um die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage, um die Verletzung von Betroffenenrechten (Verstoß gegen die Informationspflicht), die Nichtführung beziehungsweise Nichtvorlage von Verzeichnissen der Verarbeitungstätigkeit sowie um die Nichtbeachtung behördlicher Anweisungen.

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).

Profilbildung zu Werbezwecken mit Smart-Data-Verfahren

Im Berichtszeitraum haben wir ein Bußgeldverfahren im Zusammenhang mit Smart-Data-Verfahren[2] mit Bußgeldbescheid abgeschlossen. Nachdem eine Verständigung mit dem Kreditinstitut scheiterte, ist eine Geldbuße in Höhe von 485.000 Euro festgesetzt worden. Die Entscheidung ist noch nicht rechtskräftig. Es gilt die Unschuldsvermutung.

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

Ziel der Institute war es, anhand der so gebildeten Profile Kundinnen und Kunden zu identifizieren, die für spezifische Produkte besonders zugänglich sein könnten. Solche Auswertungen vorhandener Daten sowie die Hinzuziehung und Verknüpfung weiterer Daten zu Werbezwecken waren von den Kundinnen und Kunden vernünftigerweise nicht zu erwarten. Die Unternehmen konnten sich daher nicht auf ein berechtigtes Interesse[3] als Rechtsgrundlage stützen.

Einzelfälle der Videoüberwachung

Zahlreiche Fälle betrafen auch im Jahr 2025 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.[4]

2 Siehe hierzu auch Tätigkeitsbericht 2023, H und G.3.3 sowie Tätigkeitsbericht 2024, H.
3 Art. 6 Abs. 1 Buchst. f DSGVO.
4 Siehe Tätigkeitsbericht 2019 J.9.4, Tätigkeitsbericht 2020 I.5 und Tätigkeitsbericht 2021 J.9.2.

Einzelne Fälle werden kurz exemplarisch dargestellt:

- 46.500 Euro gegen ein Logistikunternehmen, welches einzelne Arbeitsbereiche von Beschäftigten überwacht hat.
- 29.000 Euro gegen ein Unternehmen, welches Fleisch weiterverarbeitete und dabei seine Beschäftigten überwachte. Geschlachtet wurde in dem Betrieb nach unserer Kenntnis nicht. Die Entscheidung ist nicht rechtskräftig. Es gilt die Unschuldsvermutung.
- 14.200 Euro gegen den Inhaber einer Gastwirtschaft wegen Überwachung von Beschäftigten sowie Kundinnen und Kunden. Zudem wegen eines Verstoßes gegen die Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde.
- 11.200 Euro gegen ein Unternehmen, das eine Tankstelle betreibt und neben öffentlichen Verkehrsflächen auch die Arbeitsbereiche von Beschäftigten überwachte.
- 7.400 Euro gegen den Inhaber einer Gastwirtschaft wegen eines Verstoßes gegen die Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde, nachdem zuvor mehrere Zwangsgelder bestandskräftig festgesetzt wurden.

Übersicht über gerichtliche Entscheidungen

Im Jahr 2025 haben Gerichte Entscheidungen zu neun unserer Bußgeldverfahren getroffen. In der Mehrzahl der Fälle haben die Bußgeldadressaten die Verstöße im Wege einer gerichtlichen Verständigung[5] eingeräumt und ihre Einsprüche auf die Rechtsfolgenseite beschränkt. Bei solch einer Beschränkung wird die von unserer Behörde ausgesprochene Feststellung des Verstoßes unmittelbar rechtskräftig, sodass das Gericht nur noch zur Höhe der Geldbuße zu entscheiden hat.

Weitere gerichtliche Entscheidungen zu Bußgeldbescheiden unserer Behörde werden für das Jahr 2026 erwartet.

5 Siehe auch Tätigkeitsbericht 2021, I.4.

Entscheidung des Oberlandesgerichts Celle zur Videoüberwachung

Ein Verfahren zur Videoüberwachung wurde im Berichtszeitraum durch das Oberlandesgericht Celle entschieden. Die Entscheidung ist rechtskräftig. In dem Fall ging es um eine unrechtmäßige Videoüberwachung von Beschäftigten in großem Maßstab durch ein umsatzstarkes Unternehmen. Die Videoüberwachung wurde von uns im Jahr 2020 mit einem Bußgeldbescheid geahndet.[6]

Anlässlich dieses Falles wurde vom Bundesgerichtshof zunächst entschieden, dass die Oberlandesgerichte für die Entscheidung über Rechtsbeschwerden zuständig sind.[7] Das Oberlandesgericht setzte auf die Rechtsbeschwerde eine Geldbuße in Höhe von 900.000 Euro[8] fest, nachdem das Landgericht Hannover zuvor eine Geldbuße in Höhe von 700.000 Euro[9] festgesetzt hatte und die Staatsanwaltschaft Rechtsbeschwerde gegen jene Entscheidung einlegte. Das Landgericht hatte vorab klargestellt, dass eine Verwarnung einer Geldbuße nicht entgegensteht,[10] anders als es rechtsberatende Autoren und insbesondere Wirtschaftsanwälte vereinzelt annehmen.

Der Verstoß wurde gerichtlich bestätigt. Überraschend war für uns, dass die Überwachung von Beschäftigten in großem Maßstab sowohl vom Landgericht als auch vom Oberlandesgericht im Ergebnis als Verstoß von geringem Schweregrad im Sinne der Leitlinien des Europäischen Datenschutzausschusses[11] eingeordnet wurde. Selbst der für Verstöße dieses Schweregrades entwickelte Bußgeldrahmen wurde von den Gerichten zu weniger als einem Drittel ausgeschöpft. Was die Bußgeldhöhe angeht, zeigt sich so erneut, dass deutsche Gerichte den im Unionsrecht festgeleg-

6 Siehe Tätigkeitsbericht 2020, I.4.
7 Bundesgerichtshof, Beschluss vom 24.06.2025, Az. 6 AR 1/25.
8 Oberlandesgericht Celle, Beschluss vom 18.12.2025, Aktenzeichen 3 ORbs 113/25.
9 Landgericht Hannover, Beschluss vom 06.05.2024, Aktenzeichen 128 OWi-LG 5301 Js 114949/21 (1/21).
10 Landgericht Hannover, Hinweisbeschluss vom 09.05.2022, Aktenzeichen 128 OWi-LG 5301 Js 114949/21 (1/21).
11 Europäischer Datenschutzausschuss, Leitlinien 04/2022 für die Berechnung von Geldbußen im Sinne der DSGVO, Version 2.1 vom 24.05.2023.

ten Bußgeldrahmen bei ihrer eigenen Zumessungsentscheidung sehr zurückhaltend anwenden.[12]

Entscheidungen zur Informationserteilung bei externen Compliance-Maßnahmen

Im Jahr 2023 haben wir eine Geldbuße in Höhe von 4,3 Millionen Euro gegen ein Unternehmen festgesetzt, weil es nach unserer Ansicht die Beschäftigten unzureichend informiert hat.[13] Das Unternehmen legte Einspruch gegen den Bußgeldbescheid ein. Die Bußgeldsache wurde daraufhin über die Staatsanwaltschaft dem Landgericht Hannover vorgelegt. Zusätzlich war das Verwaltungsgericht Hannover mit Fragen in dem Kontext befasst, da unsere Behörde einen Bescheid im Verwaltungsverfahren erlassen hat.[14]

Das Landgericht hat das Unternehmen vom Vorwurf freigesprochen, da es keinen Informationspflichtverstoß erkannte.[15] Auf Initiative unserer Behörde hat die Staatsanwaltschaft Rechtsbeschwerde gegen die Entscheidung des Landgerichts eingelegt. Die Rechtsbeschwerde wurde später durch die Staatsanwaltschaft zurückgenommen. Grund war, dass Formvorschriften nicht eingehalten wurden. Die Begründung der Rechtsbeschwerde wurde nicht von einer Staatsanwältin oder einem Staatsanwalt unterschrieben. Der Freispruch des Landgerichts wurde daher nicht mehr durch das Beschwerdegericht überprüft und ist rechtskräftig geworden.

Im Verwaltungsstreitverfahren hat das Verwaltungsgericht drei unserer fünf Entscheidungen bestätigt und zwei aufgehoben.[16] Unter anderem bestätigte das Verwaltungsgericht unsere Auffassung, dass es nicht darauf ankomme, dass ein externer Auditor tatsächlich über den Zuordnungsschlüssel verfügte. Es genüge, wenn er die maßgeblichen rechtlichen Mittel habe, durch die der Personenbezug hergestellt werden könne.

12 Exemplarisch: Landgericht Bonn, Urteil vom 11.11.2020, Aktenzeichen 29 OWi 1/20.
13 Siehe auch Tätigkeitsbericht 2023, H.
14 Siehe auch Tätigkeitsbericht 2023, G.3.5.
15 Landgericht Hannover, Beschluss vom 26.02.2025, Aktenzeichen 128 OWiLG 1/24.
16 Verwaltungsgericht Hannover, Urteil vom 05.06.2025, Aktenzeichen 10 A 4017/23, abrufbar unter https://voris.wolterskluwer-online.de/browse/document/e742e709-fdbc-4386-bd78-3f41d507697b.

In aufwendigen Bußgeldverfahren kann der zugestellte Bußgeldbescheid mit der vollständigen Beweisführung viele hundert Seiten umfassen.

Diese Mittel sah das Verwaltungsgericht beim Auditor gegeben. Damit sah das Verwaltungsgericht einen Verstoß gegen datenschutzrechtliche Vorschriften, wegen der das Landgericht das Unternehmen zuvor freigesprochen hat. Die Entscheidung des Verwaltungsgerichts ist noch nicht rechtskräftig. Das Unternehmen hat Antrag auf Zulassung der Berufung gestellt, der beim Niedersächsischen Oberverwaltungsgericht in Lüneburg anhängig ist.

Heranziehung in Bußgeldverfahren

In zwei Fällen, die zu einem Bußgeldverfahren gegenüber Unternehmen führten, forderten wir im Laufe des Verfahrens Daten an. Dazu wendeten wir uns jedoch nicht an die Verantwortlichen (die Unternehmen) selbst, sondern an deren Auftragsverarbeiter, die diese Daten als Dienstleistung für die Unternehmen verarbeiteten. Wir hatten festgelegt, in welcher Form

uns die Daten übermittelt werden sollen und auch um gewisse Filter seitens der Verarbeiter gebeten. Die teilweise umfangreichen Daten haben wir erhalten und konnten sie damit in Bußgeldverfahren als Beweismittel verwenden.

Auftragsverarbeiter sind in solchen Fällen zur Herausgabe der Daten verpflichtet, weil sie einen „Gegenstand" in ihrem Besitz haben, der als Beweismittel von Bedeutung sein könnte.[17] Der Begriff des Gegenstands wird in diesem Kontext weit verstanden und umfasst auch Datenträger sowie darauf befindliche Daten.[18] Die Herausgabeanordnung kann durch unsere Behörde selbst erlassen werden. Einen Gerichtsbeschluss bedarf es dafür nicht, anders als bei der Durchsuchung bei anderen Personen.[19] Falls es zur Durchsetzung Ordnungs- oder Zwangsmittel bedarf, ist eine gerichtliche Entscheidung notwendig.

In einem der beiden Verfahren hatte die Verantwortliche (nicht die Auftragsverarbeiterin) gegen die Herausgabeanordnung einen Antrag auf gerichtliche Entscheidung gestellt. Die Verantwortliche war unter anderem der Auffassung, dass uns als Aufsichtsbehörde anonymisierte oder pseudonymisierte Daten für das Bußgeldverfahren genügen. Dem ist das Gericht nicht gefolgt.

Verfahrensrecht bei Bußgeldern verbesserungswürdig

In Bußgeldverfahren erlässt unsere Behörde einen Bescheid. Geht dagegen ein Einspruch ein, führen wir ein sogenanntes Zwischenverfahren. Wird dem Einspruch durch uns nicht abgeholfen, geben wir die Sache über die Staatsanwaltschaft an das zuständige Gericht ab. Mit Eingang bei der Staatsanwaltschaft gehen die Aufgaben der Verfolgungsbehörde auf diese über.[20] Unsere Behörde verliert die Zuständigkeit und hat im weiteren Verfahren nur noch wenige Befugnisse. Insbesondere können wir nicht selbst Rechtsbeschwerde gegen die Entscheidung der ersten Instanz einlegen. Dies kann nur die unterdessen das Verfahren führende Staatsanwaltschaft.

17 § 46 Abs. 1, 2 OWiG i.V.m. § 95 Abs. 1 Strafprozessordnung (StPO).
18 BVerfG, Beschl. vom 12.04.2005, Az. 2 BvR 1027/02.
19 § 46 Abs. 1 OWiG i.V.m. § 103 StPO.
20 § 69 Abs. 4 Satz 1 Gesetz über Ordnungswidrigkeiten (OWiG).

Das oben skizzierte Verfahren betreffend die Rechtsbeschwerde beziehungsweise deren Begründung zeigt, dass es sowohl für die Staatsanwaltschaft als auch für uns als Datenschutzbehörde von erheblichem praktischen Nutzen wäre, wenn wir im gerichtlichen Bußgeldverfahren über dieselben Rechte wie die Staatsanwaltschaft verfügten. Wir könnten die von uns begonnenen Verfahren ohne größeren Mehraufwand anderer Stellen auch im gerichtlichen Bußgeldverfahren fortführen und die Staatsanwaltschaften würden entlastet.

Eine solche Regelung gibt es bereits für die Kartellbehörde,[21] sodass kein Neuland betreten würde. Im Kartellrecht wird die Regelung unserer Kenntnis nach erfolgreich genutzt und entlastet die Staatsanwaltschaft zumindest teilweise von komplexen Verfahren, die ihrer üblichen Tätigkeit fremd sind. Wir setzen uns intensiv dafür ein, dass für die Datenschutzaufsichtsbehörden eine vergleichbare Regelung geschaffen wird, um auch hier die Justiz zu entlasten und unseren Sachverstand noch erfolgversprechender als bisher einbringen zu können.

Musterrichtlinien für das Verfahren über Geldbußen der Datenschutzaufsichtsbehörden

Die Datenschutzkonferenz des Bundes und der Länder hat im Juni 2025 Musterrichtlinien für das datenschutzrechtliche Bußgeldverfahren beschlossen und veröffentlicht. Damit haben die Aufsichtsbehörden gemeinsame Standards für die Bearbeitung von Bußgeldverfahren transparent gemacht.

Die Musterrichtlinien stellen Praxishandreichungen für die Bearbeiterinnen und Bearbeiter von Bußgeldverfahren dar. Inhaltlich wurden insbesondere solche Themen und Fragestellungen in die Richtlinien aufgenommen, die mit einer gewissen Regelmäßigkeit auftreten. Ähnliche, weit umfangreichere Richtlinien gibt es bereits für die Staatsanwaltschaften in Form der Richtlinien für das Strafverfahren und das Bußgeldverfahren (RiStBV).

Die Musterrichtlinien sind in unserer Behörde für die Bearbeiterinnen und Bearbeiter von Bußgeldverfahren verbindlich anzuwenden. Andere Daten-

21 § 82a Abs. 1 Satz 3 Gesetz gegen Wettbewerbsbeschränkungen.

schutzaufsichtsbehörden setzen sie ähnlich um. Sie sind auf der Internetseite der Datenschutzkonferenz veröffentlicht.[22]

Merkblatt zu Verständigungen in datenschutzrechtlichen Verfahren über Geldbußen

Ein Merkblatt der DSK aus dem Dezember 2025 beschreibt gemeinsame Standards der Aufsichtsbehörden des Bundes und der Länder.

Mit dem Merkblatt weisen die Aufsichtsbehörden transparent auf die Möglichkeit von Verständigung in Bußgeldverfahren hin. Es verdeutlicht, dass Verständigungen ein rechtlich zulässiges Instrument sind, das von den Behörden genutzt wird. Verständigungen ermöglichen sowohl den von Geldbußen Betroffenen als auch den Aufsichtsbehörden in geeigneten Fällen eine legitime, effiziente und ressourcenschonende Beendigung eines Bußgeldverfahrens. Eine Verpflichtung das Instrument der Verständigung zu nutzen geht damit nicht einher. Sowohl Behörde als auch Adressat einer etwaigen Geldbuße können eine Verständigung ablehnen.

Das Merkblatt kann von der Internetseite der Datenschutzkonferenz heruntergeladen werden.[23]

22 Siehe Kurzlink: https://t1p.de/dsk-blatt1 (PDF).
23 Siehe Kurzlink: https://t1p.de/dsk-blatt2 (PDF).

G Datenschutzkonferenz

G.1 Arbeitskreis Beschäftigtendatenschutz: Das Warten auf Regeln für die digitalisierte Arbeitswelt

Aufgabe des von uns geleiteten Arbeitskreises Beschäftigtendatenschutz der Datenschutzkonferenz (DSK) ist es, einheitliche Positionen aller Aufsichtsbehörden zu datenschutzrechtlichen Fragen im Beschäftigtenkontext zu erarbeiten. Er bereitet zudem Entscheidungen der Datenschutzkonferenz vor und bespricht aktuelle Themen und Urteile.

Ein Schwerpunkt im Jahr 2025 lag erneut auf dem Gesetzgebungsvorhaben der Bundesregierung für ein Beschäftigtendaten(schutz)gesetz.

Die Fallgestaltungen aus der Praxis haben auch im Jahr 2025 aufgezeigt, dass es an normenklaren Regelungen für die Verarbeitung von Beschäftigtendaten mangelt, insbesondere soweit es um neue und zunehmend digitalisierte Prozesse im Arbeitsalltag geht. Beispielhaft sind hier Themen wie der Einsatz von algorithmischen Systemen bei Personalverfahren einschließlich Künstlicher Intelligenz, oder Möglichkeiten zur Produktivitätsmessung bei der Arbeit im Homeoffice zu nennen.

Seit vielen Jahren fordern die Datenschutzaufsichtsbehörden wiederkehrend ein eigenständiges, umfassendes Beschäftigtendatenschutzgesetz, das den Anforderungen einer digitalisierten Arbeitswelt entsprechende Regelungen enthält.[1]

Die Forderungen der Datenschutzkonferenz sind weiterhin hochaktuell. Der Druck auf den Gesetzgeber ist auch aufgrund der Ausführungen des Europäischen Gerichtshofs zu diesem Thema[2] und dem daran anknüpfenden Urteil des Bundesarbeitsgerichts (BAG)[3] gestiegen. Nach dem BAG-Urteil ist die derzeitige im Bundesdatenschutzgesetz enthaltene Generalklausel[4], die regelt, unter welchen Voraussetzungen Beschäftigtendaten

1 Siehe Entschließung der DSK vom 4. Mai 2022, abrufbar unter https://t1p.de/dsk-be-2022 (Kurzlink, PDF), sowie die Entschließung der DSK vom 11. Mai 2023, abrufbar unter https://t1p.de/dsk-be-2023 (Kurzlink, PDF)

2 Europäischer Gerichtshof, Rechtssache C-34/21, Urteil vom 30. März 2023.

3 Bundesarbeitsgericht, Aktenzeichen 8 AZR 209/21, Urteil vom 8. Mai 2025.

4 § 26 Abs. 1 Satz 1 des Bundesdatenschutzgesetzes.

verarbeitet werden dürfen, zu unbestimmt: Deren Regelungen erfüllen nicht die europarechtlichen Anforderungen[5] an spezifischere Vorschriften. Sie sind daher nicht als nationale Rechtsgrundlage heranzuziehen.

Wie bereits im letzten Tätigkeitsbericht ausgeführt[6], fiel der zuletzt von der Bundesregierung vorgelegte Gesetzentwurf Ende 2024 jedoch der Diskontinuität zum Opfer.

Gesetzgebung auf Eis?

Umso mehr ließ daher Mitte 2025 eine Ankündigung der Bundesregierung zum Koalitionsvertrag aufhorchen, dass zeitnah die Wiederaufnahme des Gesetzgebungsverfahrens für ein Beschäftigtendatenschutzgesetz geplant sei. Hierzu erfolgte im Juni 2025 eine Sondersitzung des AK Beschäftigtendatenschutz, bei der Angehörige der für das Gesetzgebungsverfahren zuständigen Fachressorts über den Sachstand berichteten. Seitdem hat der Arbeitskreis jedoch keine neuen Informationen zum Stand des Gesetzgebungsverfahrens erhalten.

Es wird davon ausgegangen, dass sich der AK Beschäftigtendatenschutz im Jahr 2026 erneut mit den Gesetzgebungsverfahren zu einem Beschäftigtendatenschutzgesetz sowie zur Verarbeitung von Beschäftigtendaten bei der „Plattformarbeit“[7] befassen wird. Wir werden im nächsten Tätigkeitsbericht zum Fortgang der Gesetzgebungsverfahren berichten.

5 Siehe Art. 88 DSGVO.
6 Siehe Tätigkeitsbericht 2024, I.1.
7 Siehe Tätigkeitsbericht 2024, I.1.

G.2 Arbeitskreis Versicherungswirtschaft: Verhaltensregeln und Mustereinwilligung

Wir leiten den Arbeitskreis Versicherungswirtschaft der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK). Im Berichtsjahr hat dieser Arbeitskreis zwei Dokumente verabschiedet, die eine einheitliche Rechtsanwendung in Deutschland sicherstellen und den Unternehmen der Versicherungswirtschaft die Einhaltung der datenschutzrechtlichen Vorgaben erleichtern.

Verhaltensregeln der Versicherungswirtschaft

Datenschutzrecht gilt als kompliziert und nur schwer umsetzbar. Die Datenschutz-Grundverordnung (DSGVO) sieht allerdings vor, dass Verbände bei der für sie zuständigen Aufsichtsbehörde sogenannte Verhaltensregeln genehmigen lassen können. Solche Verhaltensregeln sollen die Anwendung der DSGVO erleichtern, indem die abstrakten datenschutzrechtlichen Vorgaben für bestimmte Verarbeitungssituationen konkretisiert werden. Sie können beispielsweise typische Verarbeitungen personenbezogener Daten in einer bestimmten Branche beschreiben und darstellen, wie die datenschutzrechtlichen Anforderungen dabei konkret umzusetzen sind. Leider wurde bislang von dieser Möglichkeit in Deutschland kaum Gebrauch gemacht.

Der Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) hatte bei der für ihn zuständigen Datenschutzaufsichtsbehörde (der Berliner Beauftragten für den Datenschutz und die Informationsfreiheit) die Genehmigung sogenannter Verhaltensregeln für die Verarbeitung personenbezogener Daten durch Versicherungsunternehmen beantragt. Um eine einheitliche Bewertung der Verhaltensregeln in Deutschland sicherzustellen, beteiligten die Berliner Kolleginnen und Kollegen den Arbeitskreis Versicherungswirtschaft. Die intensiven Beratungen zu den Verhaltensregeln innerhalb des Arbeitskreises konnten nunmehr abgeschlossen werden und die DSK hat in ihrer 110. Sitzung die Genehmigung der Verhaltensregeln

durch die Berliner Beauftragte für den Datenschutz und die Informationsfreiheit befürwortet.

Muster-Einwilligung

Der GDV hatte dem Arbeitskreis zudem eine Mustereinwilligung für die Verarbeitung von Gesundheitsdaten und anderen sogenannten besonderen Kategorien personenbezogener Daten in der Kranken- und Lebensversicherung vorgelegt. Solche Einwilligungen sind in vielen Konstellationen nötig, weil die gesetzlichen Grundlagen sehr eng gefasst sind und beispielsweise keine Verarbeitung von Gesundheitsdaten für die Erfüllung eines Vertrages erlauben. Grund hierfür ist die besondere Sensibilität dieser in Artikel 9 DSGVO genannten Daten und damit einhergehend deren besondere Schutzbedürftigkeit.

Das vorgelegte Muster wurde im Arbeitskreis angepasst und ebenfalls in der 110. Sitzung der DSK genehmigt. Der GDV kann das Muster nun seinen Mitgliedern als mit den deutschen Datenschutzaufsichtsbehörden abgestimmt zur Nutzung empfehlen, was sowohl zu einem erhöhten Schutz der genannten Daten als auch zu einer Erleichterung auf Seiten der Versicherer führt.

G.3 Orientierungshilfen, Beschlüsse und Entschlüsse der Datenschutzkonferenz

Die Datenschutzkonferenz (DSK) veröffentlicht regelmäßig Entschließungen, Beschlüsse und Orientierungshilfen zu aktuellen datenschutzrechtlichen Fragestellungen. Im Jahr 2025 standen dabei Themen wie Künstliche Intelligenz, internationale Datenübermittlungen und die Innere Sicherheit besonders im Fokus. Nachfolgend finden Sie eine Auswahl der wichtigsten Veröffentlichungen, eine komplette Übersicht finden Sie in der Infothek der Datenschutzkonferenz unter https://datenschutzkonferenz-online.de.

Entschließung zur automatisierten Datenanalyse durch Polizeibehörden

https://lfd.niedersachsen.de/dsk-polizeianalyse
Die DSK fordert, dass automatisierte Datenanalysen durch Polizeibehörden nur auf klaren, verfassungskonformen Rechtsgrundlagen erfolgen dürfen. Besonders betont die DSK den Schutz unbeteiligter Personen, die Begrenzung und Transparenz der Datenverarbeitung und die Sicherung digitaler Souveränität. Datenschutzrechtliches Ziel ist es, Grundrechte auch bei modernen Analyseverfahren zu wahren.

Orientierungshilfe zu technischen und organisatorischen Maßnahmen bei KI-Systemen

https://lfd.niedersachsen.de/dsk-ki
KI-Systeme verarbeiten regelmäßig extrem große Datenmengen, darunter auch personenbezogene Daten. Wegen des damit einhergehenden potenziell hohen Risikos für Betroffene, hat der Datenschutz bei der Nutzung von KI-Systemen eine besondere Relevanz. Datenschutz sollte daher von Anfang an bei der Entwicklung und Anwendung von KI-Systemen mitgedacht werden. Die Orientierungshilfe der DSK beschreibt konkrete technische und organisatorische Maßnahmen für alle Phasen des KI-Lebenszyklus, um Risiken zu minimieren und die Einhaltung der DSGVO sicherzustellen.

Die Datenschutzkonferenz veröffentlicht regelmäßig Beschlüsse, Entschließungen und Orientierungshilfe auf ihrer Webseite https://datenschutzkonferenz-online.de/.

Anwendungshinweise zu Datenübermittlungen an Drittländer in der medizinischen Forschung

https://lfd.niedersachsen.de/dsk-forschung

Im Rahmen internationaler medizinischer Forschungs- und Entwicklungsvorhaben werden häufig personenbezogene Daten in Drittländer übermittelt. Die Verantwortlichen müssen dabei besondere Anforderungen im Hinblick auf Transparenz, Datenminimierung, Pseudonymisierung und die Information der Betroffenen beachten. Die DSK gibt hierzu praxisnahe Anwendungshinweise.

Forderungen zu einem besseren Datenschutz für Kinder

https://lfd.niedersachsen.de/dsk-kinderschutz
Kinder sind besonders schutzbedürftig, doch die DSGVO enthält bislang nur wenige spezielle Regelungen, Kinderrechte betreffend. Die Datenschutzkonferenz fordert deshalb, den Schutz von Kindern in der Datenschutz-Grundverordnung gezielt zu stärken. Die Entschließung schlägt vor, Kinderrechte bei der Datenverarbeitung stärker zu berücksichtigen, Einwilligungen für Werbung und Profiling einzuschränken und Schutzmaßnahmen bei Systemgestaltung, Voreinstellungen und Datenschutzverletzungen zu verbessern.

Eckpunkte für eine grundrechtsorientierte digitale Zukunft

https://lfd.niedersachsen.de/dsk-zukunft
Die Datenschutzkonferenz fordert die Bundesregierung auf, Datenschutz und Grundrechte bei der Digitalisierung konsequent zu stärken. Dazu gehören die zügige Novellierung des Bundesdatenschutzgesetzes (BDSG), ein wirksamer Beschäftigtendatenschutz[8], ein systematischer Grundrechte-Check bei Sicherheitsgesetzen und eine bessere Abstimmung von EU-Digitalrechtsakten mit der DSGVO. Ziel ist eine menschenzentrierte, vertrauenswürdige und innovative digitale Verwaltung und Gesellschaft.

Weitere Infomaterialien der Datenschutzkonferenz finden Sie unter https://www.datenschutzkonferenz-online.de.

8 Siehe auch Beitrag G1.

H Europa

Digitaler Omnibus: EU-Kommission schlägt DSGVO-Reform vor

2025 veröffentlichte die EU-Kommission im Zuge ihrer übergreifenden Pläne zur Vereinfachung verschiedener EU-Regelungen zum Zweck des Bürokratieabbaus und der Verbesserung der Wettbewerbsfähigkeit von EU-Unternehmen Vorschläge zur Änderung der Datenschutz-Grundverordnung (DSGVO). Im vergangenen Jahr haben wir diese Änderungsvorschläge analysiert und bewertet. Sie werden uns auch im Jahr 2026 weiter beschäftigen.

Die EU-Kommission hat sich für die nächsten Jahre auf die Fahnen geschrieben, die bestehenden Vorschriften einerseits auf ihre Effizienz und ihre Auswirkungen in der Praxis, auch im Zusammenspiel miteinander, und andererseits auf ihre Innovationsfreundlichkeit hin zu überprüfen. Gegebenenfalls sollen Regelungen vereinfacht beziehungsweise besser miteinander in Einklang gebracht werden. Vorrangig sollen spürbare Erleichterungen für EU-Unternehmen in der Anwendung der Regelungen geschaffen werden. Im Rahmen hiervon sollen insbesondere die EU-Digitalrechtsakte wie die KI-Verordnung[1], der Data Act[2] sowie der Data Governance Act[3] vereinheitlicht beziehungsweise geändert werden. In diesem Zuge soll auch die DSGVO Änderungen mit dem Ziel der Vereinfachung und des Bürokratieabbaus erfahren.

Digitaler Omnibus

Am 19. November 2025 veröffentlichte die Kommission dazu ein umfassendes Gesetzespaket, welches die Digitalgesetze und die DSGVO ändern soll. Im sogenannten Omnibusverfahren werden mehrere bestehende Ge-

1 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz.
2 Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates vom 13. Dezember 2023 über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung.
3 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724.

setze gebündelt geändert. Eine wesentliche geplante Änderung betrifft den Data Governance Act und ähnliche Gesetze zur freien Datennutzung, welche künftig in den Data Act mit aufgenommen werden sollen. Die daneben bedeutsamste neue Regelung im Data Act betrifft die Möglichkeit für europäische Unternehmen, künftig eine Weitergabe von Daten zu verweigern, wenn das Risiko der Weitergabe von Informationen an ein Drittland mit einem geringeren Schutzniveau als in der EU zu befürchten ist. Weiter soll der Wechsel von einem Cloud-Dienste-Anbieter zu einem Konkurrenten vereinfacht werden. Es soll eine deutlichere Abgrenzung zwischen der sogenannten „Cookie-Regelung" in der E-Privacy-Richtlinie, die den Datenschutz in der elektronischen Kommunikation regelt, und der DSGVO geben. Die Änderungen der KI-Verordnung sind in einem eigenen Gesetzesentwurf dargestellt und betreffen vor allem die Umsetzungsfristen bei Hochrisiko-KI-Systemen und einige Verfahrenserleichterungen.[4] Datenschutzrechtlich relevant ist vor allem die Einführung von Artikel 4a der KI-Verordnung (KI-VO), der den bisherigen Artikel 10 Absatz 5 der KI-VO ersetzen soll und auch inhaltlich verändert wird.

Die DSGVO soll nach den Plänen der EU-Kommission deutliche Änderungen erfahren. Einige enthalten echte Verfahrenserleichterungen und stehen damit im Einklang mit dem Ziel des Bürokratieabbaus. Andere wiederum betreffen zentrale Grundsätze des Datenschutzes und hätten weitreichende Auswirkungen auf das nach der EU-Grundrechtecharta (GRCh) verbriefte Grundrecht auf Datenschutz und den Schutz personenbezogener Daten.

Insbesondere sind folgende wesentlichen Änderungen geplant:

- Ein Personenbezug soll bei pseudonymisierten Daten nur dann anzunehmen sein, wenn der konkrete Dateninhaber über Mittel verfügt, die vernünftigerweise wahrscheinlich zu einer Identifikation führen würden.
- Die Nutzung von besonderen Kategorien personenbezogener Daten, wie beispielsweise Gesundheitsdaten, für die Entwicklung von KI-Modellen und -Systemen soll künftig erlaubt sein, wenn besondere Schutzmaßnahmen ergriffen werden.
- Der Rückgriff auf Betroffenenrechte, wie beispielsweise das Recht auf Auskunft, soll künftig ausgeschlossen werden können, wenn die betroffene Person datenschutzfremde Ziele verfolgt.

4 Zur KI-Verordnung siehe auch Beiträge E.1.1 und E.1.2.

- Automatisierte Entscheidungen sollen künftig zulässig sein, wenn sie auf einer Einwilligung, einem geschlossenen Vertrag oder dem Gesetz beruhen; es soll dann unerheblich sein, ob diese Entscheidung auch durch einen Menschen getroffen werden könnte.
- Bei Datenpannen soll künftig eine Meldung an die Aufsichtsbehörde nur bei einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen erforderlich sein. Außerdem soll die Meldefrist des Verantwortlichen auf 96 Stunden nach Bekanntwerden angehoben werden.
- Für Datenschutz-Folgeabschätzungen sollen künftig Vorlagen und Methoden zur Durchführung geschaffen werden.
- Klarstellung, dass Tracking-Techniken bei einem Webseiten-Besuch, wie z. B. Cookies, mit einem Klick abgelehnt werden können müssen. Außerdem sollen automatische Ablehnungen über automatisierte Systeme ermöglicht werden.
- Klarstellung, dass Verarbeitungen personenbezogener Daten für Entwicklung und Betrieb von KI-Modellen und KI-Systemen gegebenenfalls auf ein überwiegendes berechtigtes Interesse[5] des Verantwortlichen gestützt werden können.

Einordnung

Das Vorhaben der Entbürokratisierung und Vereinfachung komplexer Regelungen für die Anwendungsseite ist zu begrüßen. Mit den von der EU-Kommission vorgelegten Änderungsvorschlägen sind allerdings weit darüber hinaus gehende Einschnitte in den grundlegenden Schutz von personenbezogenen Daten verbunden. Da die Änderungsvorschläge über bloße Klarstellungen hinausgehen, ist es zu kritisieren, dass die EU-Kommission diese in einem Omnibusgesetz beschließen möchte. Hier wäre ein gesondertes Gesetzgebungsverfahren zu jedem Rechtsakt vorzuziehen gewesen. Die Kommission sollte die Erfahrungen der Datenschutzaufsichtsbehörden ohne Zeitdruck in den Gesetzgebungsprozess einbeziehen, um das gesetzte Ziel der Entlastung von kleinen und mittleren Unternehmen (KMU) tatsächlich zu erreichen.

5 Nach Art. 6 Abs. 1 lit. f DSGVO.

Vor allem ist die weitreichende Änderung der Definition des Personenbezugs zu kritisieren. Diese geht über die bisherige Rechtsprechung des Europäischen Gerichtshofes (EuGH) hinaus[6] und würde zu einer restriktiveren Auslegung des Begriffs und damit zu einer eingeschränkteren Anwendbarkeit der DSGVO an sich führen. Viele weitere Änderungsvorschläge der EU-Kommission enthalten zudem erneut unklare Rechtsbegriffe und würden zu neuen Rechtsunsicherheiten bei den Verantwortlichen führen.

Stellungnahme des Europäischen Datenschutzausschusses

Am 11. Februar 2026 verabschiedete der Europäische Datenschutzausschuss (EDSA) eine gemeinsame Stellungnahme mit dem Europäischen Datenschutzbeauftragten (EDSB) zum Digital-Omnibus der EU-Kommission. Hierin äußern die europäischen Datenschutzaufsichtsbehörden teils erhebliche Bedenken bezüglich einiger der geplanten Änderungen wie beispielsweise zum Personenbezug von Daten und zu den Regelungen zur Künstlichen Intelligenz. Insbesondere befürchten die Aufsichtsbehörden neue Rechtsunsicherheiten und insgesamt negative Auswirkungen auf das Schutzniveau der DSGVO. EDSA und EDSB haben daher auf notwendige Anpassungsbedarfe bei einigen Kommissions-Vorschlägen hingewiesen. Seitens der Aufsichtsbehörden befürwortet wird unter anderem die Anhebung der Risikoschwelle für die Meldepflicht bei Datenschutzverletzungen und die Harmonisierung des Begriffs „wissenschaftliche Forschung".

Deutsche Datenschutzkonferenz unterbreitet Vorschläge

Die Konferenz der Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat zudem zwei eigene Vorschläge zur sinnvollen Anpassung der DSGVO im Hinblick auf die Entlastung von Unternehmen beschlossen.

Im Hinblick auf die Entwicklung und Verbreitung von KI-Modellen und KI-Systemen fordert die DSK spezielle Rechtsgrundlagen für deren Entwicklung und Betrieb. In diesem Bereich mangelt es nach Einschätzung der

6 Zuletzt: EuGH Urteil vom 04.09.25 (C-413/23 P).

Datenschutzaufsichtsbehörden an Rechtssicherheit und es bedarf besserer Vorgaben zum Schutz der Rechte betroffener Personen.

Des Weiteren fordert die DSK, die Hersteller und Anbieter von digitalen Diensten und Produkten in die datenschutzrechtliche Verantwortung mit einzubeziehen. Insbesondere KMU sehen sich oft großen Anbietern von IT-Produkten gegenüber und sind derzeit oftmals nicht in der Position, eine datenschutzkonforme Ausgestaltung der Prozesse in den genutzten Produkten durchzusetzen. Die rechtliche Verantwortung für einen rechtmäßigen Einsatz dieser Produkte tragen bisher allein die KMU als Anwender. Deshalb ist es geboten, bereits bei der Gestaltung von IT-Produkten die Einhaltung der Datenschutzgrundsätze gesetzlich vorzusehen. Auch für Auftragsverarbeiter sollte die Verpflichtung vorgesehen werden, ihre Dienste von vornherein datenschutzkonform auszugestalten.

Erstes Signal der Mitgliedstaaten

Zum Redaktionsschluss erreichte uns noch ein erster Positionierungsentwurf des EU-Rats zum Gesetzentwurf der Kommission. Darin wird deutlich, dass die EU-Mitgliedstaaten voraussichtlich mit den geplanten Änderungsvorschlägen zur DSGVO nicht einverstanden sind. Die Arbeitsgruppe zur Erstellung einer Stellungnahme unter Leitung der zypriotischen Ratspräsidentschaft nahm etwa in ihrem ersten Entwurf eine vollständige Streichung der geplanten Neuregelung zum Begriff der personenbezogenen Daten vor. Die Bewertung eines Personenbezugs nach Pseudonymisierung soll ausschließlich durch die Anwendung von Leitlinien erfolgen. Die geplanten Änderungen bezüglich der Verwendung besonderer Kategorien von personenbezogenen Daten im Kontext von KI-Entwicklung soll nach Auffassung der Mitgliedstaaten nur unter besonderen Voraussetzungen erlaubt sein. Auch der Vorschlag der Kommission zur Einschränkung des Auskunftsrechts bei rechtsmissbräuchlichen Ansinnen soll deutlich entschärft werden: Nur bei eindeutig alleiniger Absicht einer Schädigung des Verantwortlichen und bei übermäßiger Anzahl gleichartiger Auskunftsaufforderungen soll das Recht auf Auskunft abgelehnt werden dürfen. Die geplante weitergehende Erlaubnis der Nutzung automatisierter Entscheidungen möchte der Rat vollständig streichen.

Weiterer Gang des Gesetzgebungsverfahrens

Das digitale Omnibusgesetz der EU-Kommission durchläuft nun das weitere europäische Gesetzgebungsverfahren: Europäisches Parlament und Rat diskutieren den Kommissionsentwurf und stimmen Änderungen in Form eigener Positionen ab. Der Abschluss des Gesetzgebungsverfahrens wird im Laufe des Jahres 2026 angestrebt.

I Neues aus dem IT-Labor

Neues aus dem IT-Labor der niedersächsischen Datenschutzaufsicht

Das IT-Labor unserer Behörde unterstützt die Arbeit der im Schwerpunkt juristisch tätigen Fachreferate durch technische Prüfungen und Analysen. Ein spezialisiertes Team untersucht dabei digitale Systeme wie Server, Webseiten und Apps auf Schwachstellen und datenschutzrelevante Aspekte. 2025 war das zum Beispiel bei der fortlaufenden Prüfung zur Microsoft-Exchange-Lücke[1] oder zum Einsatz von Cookies auf Webseiten der Fall.

Mithilfe moderner technischer Ausstattung führt unser Team IT-forensische Untersuchungen und Beweissicherungen durch. Das IT-Labor arbeitet eng mit den weiteren Bereichen der Behörde zusammen und beteiligt sich am fachlichen Austausch mit anderen Datenschutzbehörden, um gemeinsame Standards weiterzuentwickeln.

Prüfergebnisse als Beweismittel

Eine wichtige Aufgabe des Labors ist es, bei den zahlreichen Beschwerden gegen Webseiten den Einsatz von Cookies und anderen Trackingtechniken zu prüfen. Bei den Webseiten-Audits des Labors liegt der Fokus darauf, die Anzahl und das Verhalten der Cookies und anderen Tracking-Elementen in den verschiedenen Phasen der Webseitennutzung vom Erstaufruf und nach unterschiedlichen Einstellungen im Einwilligungsbanner zu testen. Denn regelmäßig werden bereits mehrere Cookies auf Webseiten gesetzt, ohne dass zuvor eine Interaktion des Nutzers mit dem Einwilligungsbanner stattgefunden hat. Darüber hinaus klassifiziert das IT-Labor die eingesetzten Trackingtechniken insbesondere als First- und Third-Party-Cookies und ordnet sie konkreten Drittdiensten zu. Dies ist die Basis für die Entscheidung, ob diese Elemente einwilligungsbedürftig sind.

Wird ein Bescheid auf Anordnung zur datenschutzkonformen Gestaltung von Webseiten gerichtlich angegriffen, müssen die Testergebnisse des IT-Labors beweissicher sein. Das bedeutet, dass nachweisbar standardisierte Webseiten-Audits mit behördlich entwickelten oder in forensischen Fach-

1 Vgl. Kapitel E.3.3.

kreisen anerkannten Tools durchgeführt und diese Ergebnisse mit einem hohen Schutz der Integrität und Authentizität gespeichert werden, um sie einem Gericht vorlegen zu können.

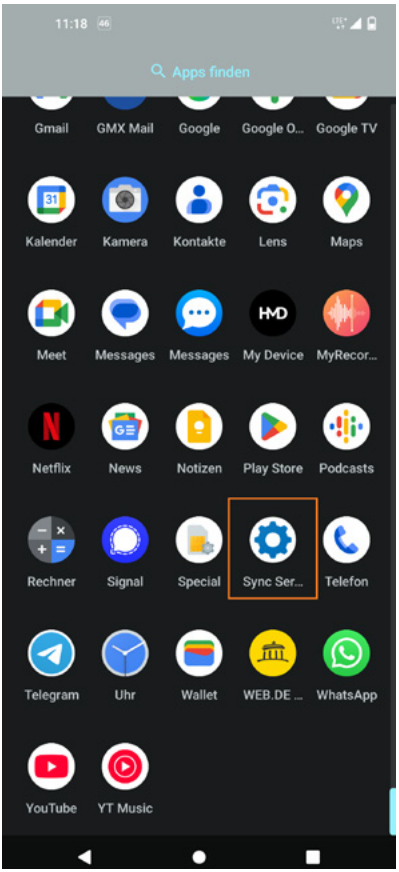
Diese Prüfergebnisse wurden bisher von den Verwaltungsgerichten immer vollumfänglich anerkannt, so beispielsweise im Jahr 2025 im Rahmen eines Urteils des Verwaltungsgerichts Hannover zum Einsatz von Cookies.[2] Nachdem die Klägerin die Prüfergebnisse angezweifelt hat, wurden im Gerichtsverfahren umfassend zu der verwendeten Testumgebung sowie der genutzten Tools und Methoden vorgetragen. In seinem Urteil zugunsten des Landesbeauftragten für den Datenschutz Niedersachsen hat das Gericht nicht infrage gestellt, dass die Prüfergebnisse des IT-Labors korrekt waren.

Spyware auf Smartphones

Das IT-Labor untersuchte in 2025 die Überwachungsmöglichkeiten durch Spionage-Apps auf Smartphones, auch Spyware oder Stalkerware genannt. Dabei handelt es sich um Überwachungssoftware, die auf einem zu überwachenden mobilen Gerät installiert wird und anschließend sowohl die Überwachung als auch Steuerung des Endgeräts ermöglicht. Mit solchen Anwendungen können etwa heimlich Gespräche mitgehört, das Kamerabild und die Bildschirmanzeige oder Eingaben in Messengern aufgezeichnet und übertragen werden. Angepriesen werden solche Produkte für Zwecke wie „elterliche Aufsicht über ihre minderjährigen Kinder" und „qualitative Mitarbeiterüberwachung". Als Verkaufsargument werben diese Apps weiterhin damit, dass sie sich gut im Smartphonesystem „verstecken lassen".

Auf dem Markt sind mehrere solcher Apps verfügbar. Das IT-Labor der niedersächsischen Datenschutzaufsicht hat 2025 eine der marktführenden Spyware-Apps beispielhaft untersucht. In der Testinstallation wurde geprüft, ob und wie eine solche App für die Nutzer erkennbar ist. Verschleiernd bezeichnet als eine systemnahe App namens „Sync Service" war die getestete Spionage-App tatsächlich in der Liste der auf dem Smartphone installierten Anwendungen für den unbedarften Anwender nicht

2 Siehe Kapitel E.2.2.



Spionage-Apps tarnen sich auf Android-Smartphones hinter harmlos klingenden Namen, in diesem Fall als „Sync Service".

auffällig (s. Abbildung). Für die Installation und Einrichtung der notwendigen Berechtigungen muss die überwachende Person mindestens einmalig einen uneingeschränkten Zugriff auf das Endgerät erhalten. Für die Ausübung der Steuerungsfunktionen sowie die Einsicht in die abgegriffenen Überwachungs-Daten stellen die App-Anbieter eine Online-Zugangsmöglichkeit für die überwachende Person zur Verfügung.

Überprüft wurde im IT-Labor, ob die Funktionsfähigkeit einer Spionage-App von Konfigurations- und Berechtigungseinstellungen des Nutzers beeinflusst werden kann. Im Testergebnis konnte zumindest für die überprüfte App nachgewiesen werden, dass eine nachträgliche Berechtigungsverweigerung durch den Nutzer die App-Zugriffsmöglichkeiten einschränkte.

In einer hausinternen Schulung hat das IT-Labor neben der Vorstellung der Möglichkeiten einer Spionage-App auch wirksame Schutzmaßnahmen dagegen vorgestellt. Dazu gehört der physische Zugriffsschutz auf das Smartphone, das Überprüfen der Kabelverbindungen sowie der drahtlosen Netzwerkverbindungen des Smartphones sowie die Kontrolle der installierten Apps und deren Berechtigungen. Der Entzug von Berechtigungen und die Löschung von nicht vertrauenswürdigen Anwendungen stellen den wirksamsten Schutz dar.

Austausch und Kooperation

Aufgrund der Komplexität und Dynamik technischer Entwicklungen befinden sich die Mitarbeiterinnen und Mitarbeiter des IT-Labors im engen

Austausch mit Kolleginnen und Kollegen auf europäischer und deutscher Ebene und nehmen an Workshops teil, die vom Europäischen Datenschutzausschuss (EDSA) organisiert werden. Halbjährlich tauschen sich die IT-Labore deutscher Aufsichtsbehörden über neue Entwicklungen zum Betrieb ihrer Hard- und Software aus sowie über gemeinsame Projekte. Darüber hinaus kooperieren unsere Technik-Expertinnen und -Experten eng mit den IT-Laboren der Datenschutzaufsichten in Hamburg und Bremen.

Themen wie die Automatisierung von Webseitenprüfungen, Audit-Tools sowie IT-Forensik in der aufsichtsbehördlichen Praxis bildeten im Jahr 2025 die Schwerpunkte des Austauschs.

Neue Online-Prüfumgebung

Die Infrastruktur und das Netzwerk des IT-Labors werden vom Netz der Landesverwaltung separat und unabhängig betrieben, um technische Prüfergebnisse nicht durch Filterregeln und sonstige Netzwerk-Sicherheitsmechanismen des Landesnetzes zu verfälschen. Aus diesem Grund haben derzeit nur die Mitarbeiterinnen und Mitarbeiter des IT-Labors die Möglichkeit, auf die installierten und stets fortentwickelten Testumgebungen und Audit-Tools zuzugreifen.

Zur Steigerung der Effizienz bei der Bearbeitung von Fällen durch die Fachreferate testet das IT-Labor derzeit ein neues Verfahren, um die bestehende Laborinfrastruktur um eine On-Premise betriebene Online-Prüfumgebung zu erweitern. Damit sollen unter anderem etablierte Audittools wie das Website Auditing Tool[3] des Europäischen Datenschutzausschusses (EDSA) oder der Website Evidence Collector[4] des Europäischen Datenschutzbeauftragten (EDPS) allen Fachreferaten für Prüfzwecke zur Verfügung gestellt werden.

3 https://www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/edpb-website-auditing-tool_en

4 https://code.europa.eu/EDPS/wec-online

J Öffentlichkeitsarbeit

J.1 Schulbesuche und Vernetzung: Schwerpunkt Datenschutz- und Medienkompetenz ausgebaut

Die Förderung von Datenschutz- und Medienkompetenz war auch im Jahr 2025 ein wichtiger Bestandteil der Arbeit der niedersächsischen Datenschutzaufsicht. Angesichts der fortschreitenden Digitalisierung des Alltags für Kinder und Jugendliche gewinnt ein bewusster und verantwortungsvoller Umgang mit persönlichen Daten weiter an Bedeutung.

Zahlreiche Institutionen in Niedersachsen engagieren sich im Bereich der Medienkompetenz. Auch der Landesbeauftragte für den Datenschutz bringt in diesem Bereich seine Expertise ein. Der Schwerpunkt liegt dabei auf dem sicheren Umgang mit persönlichen Daten im Internet und in sozialen Netzwerken sowie auf der Sensibilisierung für digitale Risiken wie Datenmissbrauch, Desinformation oder Cybermobbing.

Im Rahmen des Netzwerks Medienkompetenz Niedersachsen hat sich die Datenschutzbehörde an der Weiterentwicklung der „Ziellinie 2030 Medienkompetenz in Niedersachsen“ beteiligt. Ziel dieser gemeinsamen Strategie ist es, Medienkompetenz langfristig zu stärken und entsprechende Bildungsangebote im Land weiter auszubauen und besser zu vernetzen.

Maßnahmen und Umsetzung

Die direkte Vermittlung von Datenschutzkompetenz an Schülerinnen und Schüler bleibt ein zentraler Baustein unserer Arbeit. Die bereits 2024 begonnenen Schulbesuche wurden im Berichtsjahr weiter verstetigt und ausgebaut. Im Rahmen der bundesweiten Initiative „Datenschutz geht zur Schule“ konnten rund um den Aktionstag mehr als 600 Schülerinnen und Schüler in Niedersachsen erreicht und für Datenschutzthemen sensibilisiert werden. Darüber hinaus haben wir im Lauf des Jahres zahlreiche Schulen in Niedersachsen besucht und dabei an die individuellen Anforderungen und Themenwünsche der Lehrkräfte angepasst.

In den Unterrichtseinheiten werden praxisnahe Inhalte vermittelt, etwa zum sicheren Umgang mit Passwörtern, zu Privatsphäre-Einstellungen in sozialen Netzwerken oder zu Risiken bei der Weitergabe personenbezoge-

ner Daten im Internet. Darüber hinaus werden grundlegende Fragen des Datenschutzes und der digitalen Selbstbestimmung thematisiert. Ziel ist es, jungen Leuten frühzeitig ein Verständnis dafür zu vermitteln, welche Bedeutung personenbezogene Daten haben und wie sie diese im digitalen Alltag schützen können.

Kooperationen und langfristige Strategie

Um die Datenschutzkompetenz nachhaltig zu stärken, setzt die niedersächsische Datenschutzaufsicht weiterhin auf Kooperationen mit Schulen, Bildungseinrichtungen und weiteren Akteuren im Bereich der Medienbildung. Die Mitarbeit im Netzwerk Medienkompetenz Niedersachsen ermöglicht dabei einen kontinuierlichen Austausch sowie die gemeinsame Entwicklung langfristiger Strategien zur Förderung der Medienkompetenz im Land.

Durch die fortlaufende Weiterentwicklung unserer Bildungsangebote und die enge Zusammenarbeit mit Partnerinstitutionen stellen wir sicher, dass unsere Inhalte aktuellen technischen Entwicklungen und gesellschaftlichen Herausforderungen Rechnung tragen. Über die Fortschritte und Aktivitäten im Bereich der Datenschutz- und Medienkompetenz unterrichten wir regelmäßig den Landtag.

Mit diesem Engagement leistet die niedersächsische Datenschutzbehörde weiterhin einen wichtigen Beitrag zur digitalen Bildung und stärkt das Bewusstsein für Datenschutz als zentrale Kompetenz in einer zunehmend digitalen Gesellschaft.

An einer Zusammenarbeit interessierte Schulen und Schulträger in Niedersachsen können sich über medienkompetenz@lfd.niedersachsen.de gerne an uns wenden.

J.2 Veranstaltungen, Schulungen und Vorträge

Wie bringt man Künstliche Intelligenz und Datenschutz unter einen Hut, und wer übernimmt künftig die Aufsicht über KI-Systeme in Deutschland? Im Jahr 2025 zählten Themen rund um Künstliche Intelligenz zu den am häufigsten nachgefragten Inhalten für Vorträge und Workshops unserer Behörde.

Um diesem großen Interesse gerecht zu werden, haben wir erstmals eine spezielle Fortbildung zum Einsatz von KI in der öffentlichen Verwaltung konzipiert. Im Rahmen dieser Veranstaltung haben wir praxisnahe Lösungsansätze vorgestellt, wie sich die datenschutzrechtlichen Anforderungen bei der Einführung und Nutzung von KI-Systemen umsetzen lassen.

Der Landesbeauftragte für den Datenschutz Denis Lehmkemper auf einem Diskussionspanel mit Jutta Löwe (Continental Reifen Deutschland GmbH) und Dr. Horst Baier (CIO der niedersächsischen Landesregierung).

Teilnehmerinnen und Teilnehmer sollten befähigt werden, bereits in der Planungsphase zum Einsatz von KI-Systemen in ihren Organisationseinheiten die datenschutzrechtlichen Anforderungen zu erkennen und erfolgreich auf deren Einhaltung hinzuwirken. Die in dieser Fortbildung vermittelten Inhalte können als Baustein zum Nachweis der KI-Kompetenz gemäß der KI-Verordnung dienen.[1] Aufgrund der enorm hohen Nachfrage – beide

1 Gemäß Art. 4 KI-VO.

Termine für den Workshop waren innerhalb kurzer Zeit ausgebucht – bieten wir den Kurs im Jahr 2026 in höherer Frequenz an.[2]

Außer diesen Workshops waren Expertinnen und Experten aus unserem Haus auf verschiedenen Konferenzen und Veranstaltungen präsent, um über Datenschutz bei der Nutzung Künstlicher Intelligenz zu informieren, zu beraten und den fachlichen Austausch zu fördern. Darüber hinaus richtete unsere Behörde im November 2025 ein KI-Symposium zur rechtssicheren Nutzung von Künstlicher Intelligenz aus. Die Veranstaltung im Forum des Niedersächsischen Landtags bot vielfältige Beiträge aus Wirtschaft, Verwaltung und Wissenschaft.[3]

Darüber hinaus nahmen Vertreterinnen und Vertreter unserer Behörde im Jahr 2025 an zahlreichen weiteren Veranstaltungen, Podcasts und Workshops teil, um u. a. über die Einwilligungsverwaltungsverordnung[4], den Beschäftigungsdatenschutz[5] und digitale Souveränität zu sprechen.[6]

Schulungen für öffentliche Stellen und Vereine

Im vergangenen Jahr konnten wir über das Datenschutzinstitut Niedersachsen (DsIN) mehr als 200 Teilnehmerinnen und Teilnehmer im Bereich Datenschutz weiterbilden. Die Kurse richten sich an Datenschutzbeauftragte sowie an andere Beschäftigte öffentlicher Stellen, die mit Datenschutzfragen oder IT-Sicherheit betraut sind. Unter anderem bieten wir Kurse zu Maßnahmen des technisch-organisatorischen Datenschutzes, zu Datenschutzfolgenabschätzungen oder auch Beschäftigtendatenschutz an.

Darüber hinaus führt unser Haus regelmäßig kostenlose Datenschutzschulungen für Ehrenamtliche aus niedersächsischen Vereinen durch, in denen wir auch auf konkrete Fragestellungen aus der Praxis der Teilnehmenden eingehen und allgemein beraten.

2 Mehr zum Schulungsangebot des Datenschutzinstituts Niedersachsen (DsIN): https://www.lfd.niedersachsen.de/dsin/
3 Siehe Kapitel E.1.1.
4 Siehe Tätigkeitsbericht 2024, Kapitel G.3.2.
5 Siehe Kapitel G.1.
6 Siehe Kapitel Tätigkeitsbericht 2024, Kapitel B.

J.3 Informationsmaterial: Von Patientenakte bis Wahlwerbung

Wir erhalten regelmäßig Anfragen zum Thema Datenschutz von Bürgerinnen und Bürgern, Unternehmen sowie öffentlichen Einrichtungen. Antworten auf die häufigsten und wiederkehrenden Fragen stellen wir in Form von FAQs unter lfd.niedersachsen.de/faq zur Verfügung.

Auf unserer Webseite finden Sie darüber hinaus Merkblätter, Checklisten, Handreichungen und weiteres Informationsmaterial. Nachfolgend geben wir Ihnen einen Überblick über neue und aktualisierte Beiträge.

FAQ zur elektronischen Patientenakte

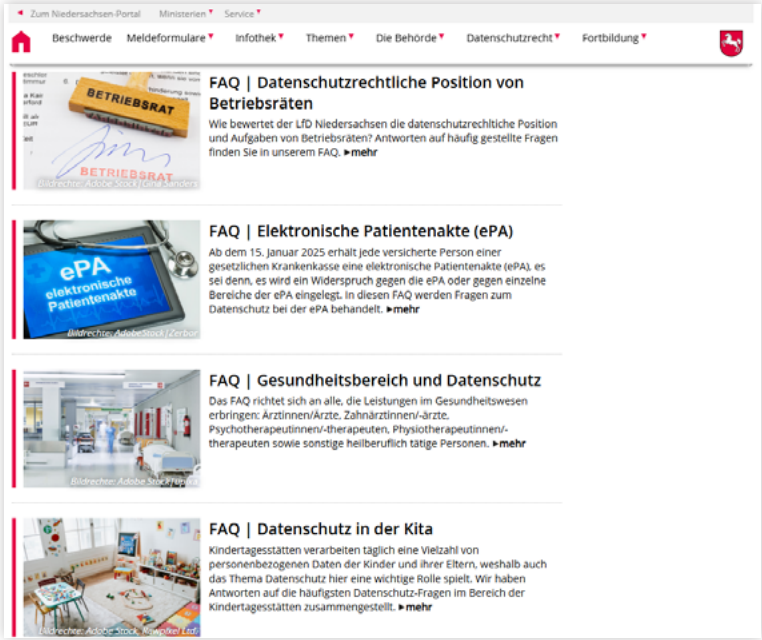
https://www.lfd.niedersachsen.de/238522.html
Seit Januar 2025 erhält jede versicherte Person einer gesetzlichen Krankenkasse eine elektronische Patientenakte (ePA), es sei denn, es wird ein Widerspruch gegen die ePA oder gegen einzelne Bereiche der ePA eingelegt. Wir geben Antworten auf Datenschutzfragen, zum Beispiel, welche Informationen in der ePA gespeichert werden, wer darauf Zugriff hat und wie vollständig oder teilweise Widerspruch eingelegt werden kann.

Wahlwerbung per Post: Datenschutzrechtliche Aspekte und Widerspruchsrecht

https://www.lfd.niedersachsen.de/56252.html
Regelmäßig erreichen uns Beschwerden von Betroffenen, die Wahlwerbung per Post erhalten haben und darin ein Datenschutzverstoß vermuten. Nach dem Bundesmeldegesetz dürfen Meldebehörden Parteien und anderen Wählergruppen zum Zweck der politischen Ansprache im Rahmen von Wahlkämpfen Adressdaten aus dem Melderegister aushändigen, aber nur unter klar definierten Voraussetzungen.

EU-Verordnung zu Online-Wahlwerbung im Überblick

https://www.lfd.niedersachsen.de/245555.html
Am 10. Oktober 2025 kam die EU-Verordnung zu Transparenz und Targeting bei politischer Werbung (TTPW-VO) EU-weit zur Anwendung. Sie soll



Über 20 Datenschutz-FAQs finden Sie auf unserer Homepage, unter anderem zu Videoüberwachung, Dashcams und Datenschutz in Vereinen.

demokratische Wahlen in der EU vor Manipulation insbesondere aus Drittstaaten schützen. Auf unserer Webseite finden Sie eine Zusammenfassung der Bestimmungen.

Europäischer Data Act: Fairer Datenzugang für alle?

https://www.lfd.niedersachsen.de/244809.html
Seit dem 12. September 2025 ist die EU-Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang – der sogenannte Data Act – weitgehend anwendbar. Der Data Act verfolgt das Ziel, Wirtschaft und Verbrauchern den Austausch und die Nutzung von Daten internetfähiger Produkte zu ermöglichen.

Datenverarbeitung im Bürgerbüro – Checkliste und Infoblatt

https://www.lfd.niedersachsen.de/56237.html

Fast alle Städte und Gemeinden bieten Dienstleistungen in sogenannten „Bürgerbüros" beziehungsweise in multifunktionalen Servicebereichen unter ähnlicher Bezeichnung an. Wir haben im Oktober 2025 unser Infoblatt und unsere Checkliste zum Datenschutz in Bürgerbüros veröffentlicht.

Abkürzungsverzeichnis

Abs.	Absatz (juristische Abkürzung)
AK	Arbeitskreis
Art.	Artikel (juristische Abkürzung)
Az.	Aktenzeichen
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
BMG	Bundesmeldegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
Buchst.	Buchstabe/Unterpunkt (juristische Abkürzung)
BVerfG	Bundesverfassungsgericht
CEF	Coordinated Enforcement Framework
CIO	IT-Leiter (Chief Information Officer)
DMStV	Digitale Medien-Staatsvertrag
DPA	Data Protection Addendum
DSA	Digital Services Act
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DsIN	Datenschutzinstitut Niedersachsen
DSK	Datenschutzkonferenz
EDPS	Europäische(r) Datenschutzbeauftragte(r)
EDSA	Europäischer Datenschutzausschuss
ePA	elektronische Patientenakte
EuGH	Europäischer Gerichtshof
FAQ	Frequently Asked Questions
GDV	Gesamtverband der Deutschen Versicherungswirtschaft e. V.
GG	Grundgesetz
GGO	Gemeinsame Geschäftsordnung der Landesregierung und der Ministerien in Niedersachsen
GDNG	Gesundheitsdatennutzungsgesetz
ID	Identifikationsnummer
JI-Richtlinie	EU-Datenschutzrichtlinie zur Zusammenarbeit im Bereich Justiz und Inneres

KI	Künstliche Intelligenz
KJM	Kommission für Jugendmedienschutz
KI-VO	Verordnung über Künstliche Intelligenz der EU
KMU	Kleine und mittlere Unternehmen
LfD	Landesbeauftragter für den Datenschutz
LKA	Landeskriminalamt
LLM	Large Language Model
MDM	Mobile Device Management
MÄStV	Medienänderungsstaatsvertrag
MStV	Medienstaatsvertrag
NDSG	Niedersächsisches Datenschutzgesetz
NKomVG	Niedersächsisches Kommunalverfassungsgesetz
NKWG	Niedersächsisches Kommunalwahlgesetz
NOOTS	National Once-Only-Technical-Systems
NPOG	Niedersächsisches Polizei- und Ordnungsbehördengesetz
NPsychKG	Niedersächsisches Gesetz über Hilfen und Schutzmaßnahmen für psychisch Kranke
NSchG	Niedersächsisches Schulgesetz
NVerfSchG	Niedersächsisches Verfassungsschutzgesetz
OWiG	Ordnungswidrigkeitengesetz
OZG	Onlinezugangsgesetz
PWTG	Politische-Werbung-Transparenz-Gesetz
SGB	Sozialgesetzbuch
StPO	Strafprozessordnung
TTPW-VO	Verordnung über die Transparenz und das Targeting politischer Werbung
TDDDG	Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz
VG	Verwaltungsgericht
VLOP	Sehr große Online-Plattform (Very Large Online Platform)
VwVfG	Verwaltungsverfahrensgesetz
VO	Verordnung