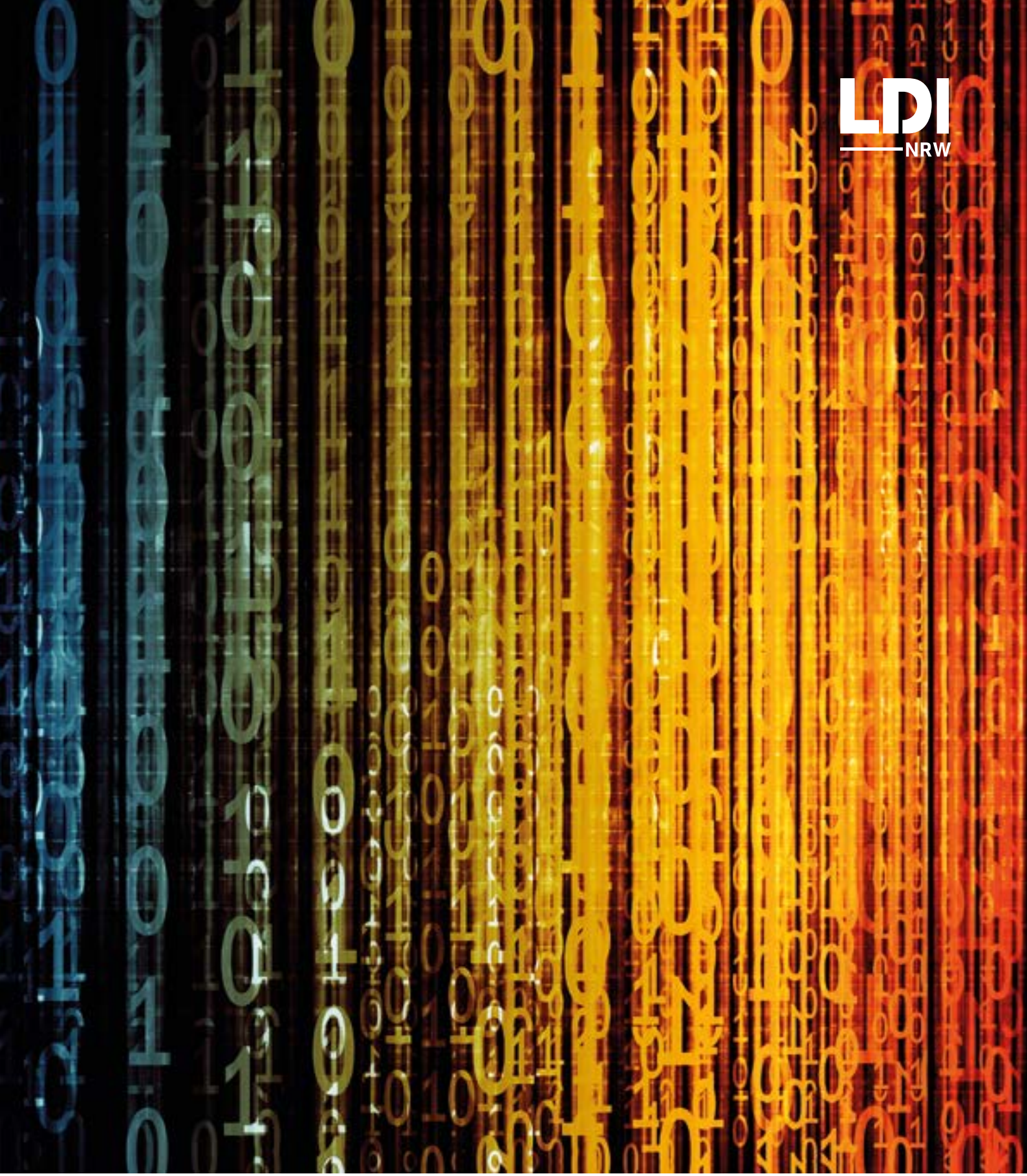


31. Bericht

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

31. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Bettina Gayk

zum Datenschutz
für die Zeit vom 1. Januar 2025
bis zum 31. Dezember 2025

Inhalt

1. Vorwort

Bettina Gayk
Landesbeauftragte für Datenschutz und Informationsfreiheit

Datenschutz schützt nicht Daten an sich, sondern diejenigen, um deren Daten es geht. Diesen Satz kann man gar nicht oft genug sagen – und heute mehr denn je. In einer zunehmend digitalisierten Welt sind die Kenntnis über Daten und die sich daraus ergebenden Möglichkeiten der Datennutzung ein Machtinstrument. Datenschutz zielt insoweit darauf ab, Macht zu begrenzen und die Bürger*innen vor Machtmissbrauch zu schützen.

In der Privatwirtschaft können Interessensprofile und Kaufverhaltensanalysen genutzt werden, um Verbraucher*innen zu ihrem eigenen Nachteil in ihren wirtschaftlichen Entscheidungen zu manipulieren. Sei es, dass sie veranlasst werden, über ihre finanziellen Verhältnisse hinaus Verträge einzugehen, sei es, dass sie im Interesse an maximalem Profit mit unlauteren Mitteln zu einem Handeln angereizt werden, das sich auf ihre körperliche oder gar psychische Gesundheit negativ auswirkt. Grenzen werden deutlich überschritten, wo derartige Profilbildungen zu einem für Betroffene intransparenten Handel mit Daten führen, dessen Auswirkungen kaum mehr überschaubar sind. Davon zeugt ein Fall des Handels mit Handystandortdaten, den Sie im Bericht finden. Gewinnerzielung ist zwar ein legitimes Ziel der Wirtschaft, aber eben nicht um jeden Preis. Hier sorgt das Datenschutzrecht dafür, dass zum Wohle der Betroffenen Grenzen eingehalten werden. Erhebliche wirtschaftliche Nachteile können Verbraucher*innen auch erleiden, wenn ihre Bonität aufgrund der Bewertung ihrer Daten schlecht ausfällt. Datenschutz soll zum einen die Richtigkeit der verwendeten Daten garantieren. Niemand soll aufgrund unrichtiger Daten in seinem wirtschaftlichen Handeln eingeschränkt werden können. Zum anderen verhindert der Datenschutz eine unbegrenzte Datenspeicherung. Wesentlich ist hier, wie lange ein belegtes Fehlverhalten von Verbraucher*innen sich auf die Einstufung der Kreditwürdigkeit auswirken darf. Wer einmal eine Rechnung zu spät bezahlt, darf dafür nicht unendlich in seiner Kreditwürdigkeit angezweifelt werden. Nach einer Zeit des Wohlverhaltens müssen die Betroffenen auch wieder unbelastet am Wirtschaftsverkehr teilnehmen können. Die Wirtschaft verfügt zusammengefasst über unfassbar viele Daten der Verbraucher*innen. Datenschutz begrenzt die Wirtschaft darin, diese Datenmacht zum Nachteil der Betroffenen auszunutzen.

Am stärksten und sehr unmittelbar verspüren die Bürger*innen die staatliche Macht im Sicherheitsbereich. Wer wegen falscher Daten oder unberechtigterweise noch nicht gelöschter Daten in den Fokus einer Sicherheitsbehörde gerät, kann mit erheblichen Schwierigkeiten konfrontiert sein. Auch berufliche Nachteile können daraus entstehen, wenn die Tätigkeit eine Sicherheitsüberprüfung erfordert. Jüngste Gesetzgebung in Nordrhein-Westfalen zu den Befugnissen von Polizei und Verfassungsschutz widmet sich der Frage der staatlichen Machtbegrenzung nach meiner Einschätzung nicht ausreichend. Die Machtbegrenzung der Sicherheitsbehörden findet verfassungsrechtlich ihre Verankerung im Prinzip der Verhältnismäßigkeit. Dieses gebietet nicht nur ausgewogene Einzelmaßnahmen der Behörden. Es verlangt auch, dass bereits im Gesetz Befugnisse klar beschrieben sind und durch Maßnahmen eingegrenzt werden, die mögliche erhebliche Eingriffe in die Privatsphäre der Bürger*innen ausgleichen. Sowohl beim Polizeigesetz, als auch beim Verfassungsschutzgesetz bin ich der Ansicht, dass die Grenzen der Eingriffsbefugnisse und die Schwere der die Eingriffe kompensierenden Maßnahmen besser hätten beschrieben werden müssen. Die erforderliche Balance zwischen staatlicher Machtbefugnis und Schutz der Privatsphäre ist in beiden Gesetzen noch nicht gelungen. So ist beispielsweise die pauschale Befugnis zum Einsatz von KI in beiden Gesetzen wenig hilfreich. Setzen die entsprechenden Behörden KI ein, um Schreiben an Bürger*innen verständlich zu fassen, bedürfte es dazu wahrscheinlich genauso wenig einer Befugnis, wie es dies für den Einsatz eines Computers oder einer Schreibmaschine bedarf. Soll indessen mittels KI das Internet auf verfassungsfeindliche Tendenzen durchforstet werden, muss das auch so eindeutig beschrieben sein. Hinzu kommt: Nicht alle Informationen im Internet sind richtig. Angesichts dessen bedarf es mindestens zusätzlich klarer Regelungen, um das Problem von falschen Daten und Fake News zu adressieren. Es muss sichergestellt sein, dass Bürger*innen nicht grundlos in die Beobachtung durch den Verfassungsschutz geraten. Ich wende mich hier nicht gegen neue Befugnisse für die Sicherheitsbehörden in einer zunehmend digitalisierten Welt. Aber ich halte es für erforderlich, dass die Gesetzgebung auch die Gefahren, die sich aus diesen Befugnissen für den Schutz der Privatsphäre für die Bürger*innen ergeben, durch geeignete gesetzliche Vorkehrungen eingrenzt. Weitere Einzelheiten zu den beiden Gesetzgebungsvorhaben finden Sie im Bericht.

Abschließend möchte ich anmerken, dass die für die Datenverarbeitung Verantwortlichen zunehmend und auch lauter darauf hinweisen, dass ihnen der Datenschutz lästig ist. Bei den Bürger*innen, um deren Schutz es dabei geht, sieht es ganz anders aus. Sie fragen die Unterstützung meiner Behörde mehr denn je nach. Allein bei den Einzelbeschwerden von Personen, die sich von einem Datenschutzverstoß betroffen sehen, gab es im Berichtsjahr einen Anstieg zum Vorjahr von rund 67 Prozent. In nackten Zahlen sind das 12.592 Beschwerden im Jahr 2025 gegenüber 7.539 Beschwerden in 2024. Das erreichte hohe Niveau hat sich zu Beginn des Jahres 2026 bestätigt. Ein solch enormer Beschwerdeanstieg ist eine

große Herausforderung und mit den vorhandenen Mitteln kaum mehr zeitlich angemessen zu bewältigen. Dennoch sehe ich meine Aufgabe darin, gemeinsam mit meinen Mitarbeiter*innen, so gut dies möglich ist, Betroffene aktiv vor unzulässiger und für sie nachteiliger Datenverarbeitung zu schützen.

Bettina Gayk
Frühjahr 2026

2. Datenschutz in Europa

Der Europäische Datenschutzausschuss (EDSA) soll die einheitliche Anwendung der DS-GVO und der EU-Datenschutz-Richtlinie im Bereich von Justiz und Inneres in der Europäischen Union sicherstellen. Dazu verfügt er über ein eigenes Sekretariat in Brüssel und ist von der EU unabhängig. Der EDSA setzt sich aus den Leiter*innen aller Aufsichtsbehörden im Europäischen Wirtschaftsraum sowie dem Europäischen Datenschutzbeauftragten zusammen. Gemeinsame Vertreterin für die deutschen Datenschutzbehörden im EDSA ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Ihr Stellvertreter in diesem Ausschuss ist der Bayerische Landesbeauftragte für den Datenschutz.

Der EDSA erstellt unter anderem Leitlinien zu wichtigen datenschutzrechtlichen Fragen sowie Stellungnahmen und trifft insbesondere verbindliche Entscheidungen.

Der EDSA wird bei seiner Arbeit von mehreren Fachuntergruppen (Expert Subgroups – ESG) unterstützt, in denen auch die nationalen Aufsichtsbehörden vertreten sind. Die LDI NRW ist in den Expert Subgroups

- Key Provisions (rechtliche Grundsatzfragen),
- Compliance, E-Government & Health (CEH) (Regelkonformitätsverfahren, digitale Verwaltung und Gesundheitsbereich),
- Financial Matters (Finanzangelegenheiten einschließlich Banken und Kreditwirtschaft) und
- Technology (technischer Datenschutz)

aktiv und vertritt dort die deutschen Aufsichtsbehörden.

Strategie und Arbeitsprogramm

Die Ziele seiner Arbeit hat der EDSA in seiner Strategie für 2024 bis 2027 festgelegt, und dabei die wichtigsten Maßnahmen benannt:

1. Säule: Verbesserung der Harmonisierung und Förderung der Einhaltung der Vorschriften

2. Säule: Stärkung einer gemeinsamen Durchsetzungskultur und effektiven Zusammenarbeit

3. Säule: Datenschutz bei der Entwicklung der digitalen und regulierungsübergreifenden Landschaft

4. Säule: Beitrag zum globalen Dialog über Datenschutz

Der besondere Fokus liegt auf dem Zusammenspiel der DS-GVO mit dem digitalen Regulierungsrahmen der EU (Europäische Datenstrategie). Neue digitale Gesetze, wie etwa der Digital Services Act (DSA), haben Auswirkungen auf den Datenschutz. Hier soll mit anderen Regulierungsbehörden zusammengearbeitet werden, um das Recht auf Datenschutz in die allgemeine Regulierungsarchitektur einzubetten.

Für die Jahre 2026–2027 hat der EDSA ein neues Arbeitsprogramm erarbeitet. Es ist das zweite Arbeitsprogramm zur Umsetzung der EDSA-Strategie bis 2027. Das Arbeitsprogramm basiert auf den in der EDSA-Strategie festgelegten Prioritäten sowie auf den von den Mitgliedern als besonders wichtig für die Stakeholder identifizierten Bedarfen. Es berücksichtigt außerdem die sog. Helsinki-Erklärung vom Juli 2025. Damit verpflichten sich die Datenschutzaufsichtsbehörden, die praktische Anwendung der DS-GVO berechenbarer und handhabbarer zu machen. So plant der EDSA, mehr konkrete Arbeitsmittel bereitzustellen, nämlich standardisierte Vorlagen, Entscheidungs- und Prüfschemata, verständliche Erläuterungen sowie konsolidierte Darstellungen der Behördenpraxis. Damit soll die Rechtsanwendung insbesondere für kleine und mittlere Unternehmen und Organisationen ohne eigene Datenschutz- oder Rechtsabteilung erleichtert werden. Zudem sollen nationale Unterschiede in der Anwendung der DS-GVO durch abgestimmte Leitlinien, koordinierte Verfahren und stärker gebündelte Veröffentlichungen die Vorhersehbarkeit behördlicher Bewertungen verbessern. Ergänzend plant der EDSA einen frühzeitigen Austausch mit Wirtschaft und Verbänden, um praktische Probleme bereits vor neuen Leitlinien zu erfassen. Ziel ist es, die Einhaltung der Datenschutzvorgaben zu erleichtern, Innovation verantwortungsvoll zu fördern und die Wettbewerbsfähigkeit in Europa zu unterstützen.

Zahlreiche Veröffentlichungen werden unter Mitarbeit der LDI NRW derzeit erarbeitet.

So findet etwa zu den vorbereitenden Arbeiten für die Einführung des **Digitalen Euro** in der Financial Matters Subgroup ESG eine intensive Befassung mit den datenschutzrechtlichen Aspekten des Projekts statt. Außerdem ist im Auftrag des EDSA ein Gutachten zu technischen Möglichkeiten des Datenschutzes bei der sog. „Offline-Variante" des Digitalen Euro erstellt worden, also der Möglichkeit, vor Ort im Geschäft mit der digitalen Währung zu zahlen. Die Entwicklungen im Hinblick auf die Gesetzgebungsvorschläge der Europäischen Kommission und die technischen Regelwerke der Europäischen Zentralbank verfolgt die LDI NRW auch weiter intensiv. Sie bringt ihre datenschutzrechtliche Expertise ein, da der Digitale Euro aus Sicht der LDI NRW nur durch einen starken Datenschutz einen tatsächlichen Mehrwert für den Zahlungsverkehr und die europäischen Bürger*innen bietet.

Die LDI NRW bringt sich auch aktiv bei Genehmigungen von sog. **Corporate Rules (BCR)** für europäische Konzerne ein, die Gesellschaften mit Sitz außerhalb des Europäischen Wirtschaftsraumes (EWR) haben. BCR sind verbindliche, von Datenschutzbehörden genehmigte interne Vorschriften, die solche multinationalen Unternehmensgruppen nutzen, um personenbezogene Daten innerhalb des Konzerns sicher und rechtskonform aus dem EWR in Drittländer außerhalb der EU/EWR zu übermitteln. Durch die BCR soll ein einheitliches, hohes Datenschutzniveau innerhalb des Konzerns geschaffen werden. Neben der Beratung von Unternehmen in NRW, die die Einführung von BCR im Konzern erwägen, hat die LDI NRW auch dieses Jahr wieder andere europäische Aufsichtsbehörden bei ihrer Prüfung von BCRs unterstützt und mehrere, sogenannte „Co-Reviews" durchgeführt. Hierbei werden die BCR im Wege des „Mehr-Augen-Prinzips" dahingehend überprüft, ob sie die gesetzlichen Voraussetzungen erfüllen. Die Genehmigung von BCR und die damit verbundene Rechtssicherheit für konzerninterne Datenströme lebt daher von einer engen europäischen Zusammenarbeit, an der sich die LDI NRW regelmäßig beteiligt.

Um die Zusammenarbeit auf europäischer Ebene zu stärken und eine Vernetzung mit den beteiligten Akteur*innen am Markt herzustellen, hat die LDI NRW zudem zusammen mit der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) einen internationalen Workshop veranstaltet, in dem sich die Mitglieder der CEH ESG mit Vertreter*innen aus der Wirtschaft über Nutzen und Verbreitung von Datenschutzzertifizierungen ausgetauscht haben.

3. Datenschutz in Deutschland

Die Aufsichtsbehörden in Deutschland stimmen sich in der Datenschutzkonferenz (DSK) ab. 2025 hat Berlin als Vorsitz die Sitzungen der DSK ausgerichtet, die Umsetzung der Arbeitsergebnisse veranlasst und die Konferenz nach außen vertreten.

Die DSK hat eine zentrale Rolle für die einheitliche Anwendung des Datenschutzrechts in Deutschland. Sie hat sich in ihrer Geschäftsordnung Regelungen auferlegt, die verbindliche Mehrheitsentscheidungen in Fragen der Rechtsanwendung ermöglichen. In Beschlüssen, Kurzpapieren, Anwendungshinweisen und Orientierungshilfen richtet sich die DSK an für die Datenverarbeitung Verantwortliche und gibt ihnen Hinweise für die richtige Rechtsanwendung. Die Inhalte dieser Papiere legen die Aufsichtsbehörden ihrer eigenen Aufsichtsarbeit zugrunde. Für Reaktionen auf datenschutzpolitische Entwicklungen nutzt die DSK in der Regel das Format der Entschließung. Sie erzielt mit dieser Arbeit homogene Ergebnisse und stellt eine einheitliche Datenschutzaufsicht in Deutschland sicher.

Die DSK hat zur Unterstützung ihrer Arbeit Arbeitskreise eingerichtet. Über unsere Vorsitze der Arbeitskreise wurden mehrere fachliche Impulse an die DSK geleitet. Im Rahmen der DSK leitet die LDI NRW die Arbeitskreise

- Wirtschaft,
- Statistik,
- Kreditwirtschaft sowie
- Adresshandel und Werbung
  (gemeinsam mit dem Bayerischen Landesamt für Datenschutzaufsicht).

Diese Facharbeitskreise stehen im Austausch mit Wirtschaft und Verwaltung. Sie können Vertreter*innen der Wirtschaft und Verwaltung oder Expert*innen etwa aus Verbänden oder Behörden zu Sitzungen einladen. Ihre Ergebnisse, die sie der Konferenz zur Entscheidung vorlegen, prüfen sie bei Bedarf durch Anhörungen von Interessenvertretungen oder auch der Allgemeinheit. Darüber hinaus nutzt die Konferenz die Facharbeitskreise, wenn aus Verwaltung und Wirtschaft Fragen zu Klärung an sie herangetragen werden, um zeitnah Rückmeldungen geben zu können. Über eine Vernetzung der nationalen Facharbeitskreise mit den Fachuntergruppen des EDSA ist Deutschland auch in Europa schnell und einheitlich sprachfähig.

Eine besondere Aufgabe innerhalb der Datenschutzkonferenz hat der **Arbeitskreis DSK 2.0** unter Leitung des rheinland-pfälzischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit. In diesem Arbeitskreis evaluieren die Beauftragten des Bundes und der Länder die Arbeit der DSK und ergreifen die notwendigen Maßnahmen, um eine effiziente Arbeit der Konferenz sicherzustellen. Die Aufgabe der Konferenz zur Koordinierung einer einheitlichen Anwendung des Datenschutzrechts in einer zunehmend digitalisierten Welt kann die Konferenz nur durch eine gute Zusammenarbeit und effiziente Strukturen bewältigen. Um hier mit der zunehmenden und immer anspruchsvolleren Digitalisierung Schritt zu halten, ergreift der AK DSK 2.0 die notwendigen Maßnahmen im Rahmen des Möglichen.

Bei wesentlichen Punkten, die die DSK für erforderlich hält, um den Erwartungen an sie gerecht zu werden, bedarf es allerdings politischer Unterstützung von außen. Dies betrifft die rechtliche **Institutionalisierung der DSK,** die der Geschäftsordnung und Beschlussfassung auch nach außen Rechtswirksamkeit verschafft und die Errichtung einer **Geschäftsstelle** der DSK. Eine Geschäftsstelle ist angesichts der steigenden Aufgaben der DSK und der Erwartungen an ihre Leistungsfähigkeit dringend erforderlich. Der jährlich unter den Aufsichtsbehörden wechselnde Vorsitz ist in der Koordinierung immer anspruchsvoller und zeitintensiver geworden. Die laufende Koordinierung der DSK während des Jahres bedarf einer Routine und ist eine ständig laufende Aufgabe, die nur von einer Geschäftsstelle in der gebotenen Professionalität geleistet werden kann. Dazu bedarf es einer nach dem erweiterten Königsteiner Schlüssel vorzunehmenden Finanzierung einer solchen Geschäftsstelle. Teils wird der Forderung nach einer Geschäftsstelle der DSK das Argument des Verbots der Mischverwaltung zwischen Bund und Ländern entgegengehalten. Das greift hier jedoch nicht, denn es handelt sich nur um eine unterstützende Tätigkeit. Durch eine solche Geschäftsstelle werden keine eigenen Verwaltungsentscheidungen getroffen. Sie organisiert lediglich die erforderliche Koordinierung der Abstimmungsprozesse in der DSK zu einer einheitlichen Rechtsauslegung und -anwendung durch die jeweils unabhängigen Datenschutzaufsichtsbehörden.

Eine solche Unterstützung der DSK durch eine Geschäftsstelle kann personell und sachlich relativ unaufwändig und bürokratiearm eingerichtet werden und bei einem Mitglied der DSK räumlich beheimatet sein. Sie kann einen effektiven Beitrag leisten, damit die DSK den Interessen der Wirtschaft Rechnung tragen kann, indem sie als Single Point of Contact beispielsweise Datenpannenmeldung entgegennimmt und in den Aufsichtsprozess steuert. Sie kann auch Fragestellungen aufnehmen, die nach Absprache mit dem Vorsitz im Interesse einer einheitlichen Rechtsanwendung in der Konferenz behandelt werden sollten.

Veröffentlichungen der DSK

Die Beschlüsse und Entschließungen des Jahres 2025 sind im Anhang abgedruckt und mit weiteren Veröffentlichungen auch auf der Website der Datenschutzkonferenz www.datenschutzkonferenz-online.de abrufbar.

4. Künstliche Intelligenz

4.1 Im Bereich KI gibt es noch viele Baustellen

Für die Entwicklung, das Training und den Betrieb von KI-Modellen sind spezifische Rechtsgrundlagen weiterhin Mangelware – sowohl auf europäischer wie nationaler Ebene. Zugleich stellt die Gewährleistung von Betroffenenrechten datenschutzrechtlich verantwortliche Stellen vor große Herausforderungen. Die Datenschutzkonferenz (DSK) dringt auf Reformen.

Künstliche Intelligenz ist ein weites Feld, in dem auch Experten schnell den Überblick verlieren können, weil es sich mit hoher Geschwindigkeit weiterentwickelt. Eine Aufgabe der Datenschutzaufsicht in diesem weiten Feld ist es, dafür zu sorgen, dass die Datenschutzrechte der Betroffenen gewährleistet bleiben, wenn ihre Daten mittels KI verarbeitet werden. Hier berücksichtigt die gesetzliche Regulierung, sei es auf nationaler wie internationaler Ebene, die spezifischen Besonderheiten der neuen Technik KI noch nicht ausreichend. Zwei Themen hat die DSK, deren Mitglied die LDI NRW ist, 2025 in den Blick genommen. In entsprechenden Entschließungen fordert das Gremium konkrete Veränderungen im Datenschutzrecht.

Im Mittelpunkt stehen dabei zwei miteinander verknüpfte Themen. Zum einen geht es darum, IT-Hersteller und -Anbieter stärker in die datenschutzrechtliche Verpflichtung einzubinden. Zum anderen besteht die Notwendigkeit, das wichtige Regelwerk für den Datenschutz, die DS-GVO, gezielter an die besonderen Anforderungen von KI anzupassen. Beide Entschließungen verfolgen das Ziel, mehr Rechtssicherheit und Praktikabilität herzustellen bei gleichzeitiger Wahrung eines hohen Grundrechtsschutzes.

In der ersten Entschließung „DSGVO-Reform: IT-Hersteller in die Verantwortung nehmen!" vom 12. Dezember 2025 (Abdruck im Anhang) zu den Herstellerpflichten wird eine strukturelle Schwäche der DS-GVO aufgegriffen. Zwar verpflichtet Art. 25 DS-GVO die für eine Datenverarbeitung Verantwortlichen dazu, datenschutzfreundliche Technik und entsprechende Voreinstellungen einzusetzen. Tatsächlich richten sich diese Pflichten jedoch nicht an eine andere wichtige Zielgruppe – nämlich diejenigen, die über Architektur, Funktionen und Voreinstellungen von Hard- und Software entscheiden. In der Praxis tragen vor allem die Anwender*innen, häufig kleine und mittlere Unternehmen, die datenschutzrechtliche Verantwortung, obwohl sie auf die IT-Produkte und deren Festlegungen für die Art und Weise der Datenverarbeitung kaum Einfluss nehmen können. Eine Forderung der DSK ist daher, die derzeit in der Planung befindliche Reform der DS-GVO zu nutzen, um Hersteller und Anbieter*innen von Standardlösungen in das System der datenschutzrechtlichen Pflichten einzubeziehen. Dies würde rechtliche Pflichten dorthin verlagern, wo auch für KI die oft grundlegenden technischen Weichenstellungen erfolgen und zugleich Anwender*innen erheblich entlasten. Außerdem könnte damit eine Harmonisierung der DS-GVO mit anderen europäischen Digitalrechtsakten erreicht werden. Insbesondere der sog. Cyber Resilience Act und der sog. AI Act enthalten bereits Pflichten für Hersteller in Bezug auf Sicherheit, Risikomanagement und Produktkonformität. Eine datenschutzrechtliche Herstellerverpflichtung würde somit keine neuen Anforderungen schaffen, sondern bestehende Verpflichtungen systematisch ergänzen. Datenschutzrechtliche Pflichten sollen dort ansetzen, wo effektive Einflussmöglichkeiten bestehen. Auch die Auftragsverarbeiter sollten stärker in die Pflicht genommen werden, insbesondere im Hinblick auf datenschutzrechtliche Voreinstellungen.

Die zweite Entschließung „DS-GVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich" vom 12. Dezember 2025 (Abdruck im Anhang) widmet sich den besonderen Herausforderungen, die sich aus der Entwicklung und dem Einsatz von KI-Systemen ergeben. Entwicklung, Training und Betrieb von KI-Modellen – insbesondere großer Sprachmodelle – sind häufig mit massiven Datenverarbeitungen verbunden. Dies gilt zum Beispiel für das Extrahieren großer Datenmengen von Websites (sog. Web Scraping) oder die Weiterverwendung ursprünglich zu anderen Zwecken erhobener Daten. Kommt es dabei zu einer Datenverarbeitung mit einer hohen Eingriffsintensität, etwa bei der Polizeifahndung, braucht es deshalb neue, spezifische Rechtsgrundlagen. Dies ist aber nicht überall gewährleistet. Das zeigt sich nicht zuletzt in NRW, wo jüngst durch die Änderungen des Polizeigesetzes und des Verfassungsschutzgesetzes Rechtsgrundlagen für die Entwicklung und das Training von KI-Modellen geschaffen wurden, die in diesem Sinne unzureichend sind (siehe hierzu unter 8.1 und 8.2).

In einem ähnlichen Problembereich bewegt sich auch ein Vorschlag der EU-Kommission im Rahmen des sog. „Digital Omnibus", einem Gesetzes-

vorhaben, mit dem die EU Hand anlegen will an die DS-GVO und die KI-Verordnung. Konkret geht es um Art. 10 Abs. 5 des AI Act. Danach dürfen Anbieter*innen von Hochrisiko-KI-Systemen ausnahmsweise besondere Kategorien personenbezogener Daten verarbeiten, soweit dies für die Erkennung und Korrektur von Verzerrungen im Zusammenhang mit Hochrisiko-KI-Systemen unbedingt erforderlich ist. Dabei müssen sie dann angemessene Vorkehrungen für den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen treffen. In ihrer aktuellen Fassung hat diese Vorschrift allerdings einen eingeschränkten Anwendungsbereich, indem sie nur die Anbieter*innen von Hochrisiko-KI-Systemen privilegiert und sich auf besondere Kategorien personenbezogener Daten beschränkt. Auf Vorschlag der EU-Kommission im Rahmen des Digital Omnibus soll dieser Anwendungsbereich nunmehr in einem neuen Art. 4a auch auf alle anderen KI-Systeme und auf Betreiber ausgeweitet werden.

Ein weiterer Schwerpunkt der Entschließung liegt auf der Gewährleistung von Betroffenenrechten. Transparenz, Auskunft, Berichtigung, Löschung und Widerspruch gehören zu den fundamentalen Rechten der von einer Datenverarbeitung betroffenen Personen. Diese Rechte lassen sich jedoch bei vielen KI-Systemen technisch bedingt nur schwer oder gar nicht umsetzen. Deshalb dringt die DSK darauf, über funktionsäquivalente oder kompensatorische Schutzmaßnahmen nachzudenken, mit denen KI rechtskonform und unter Beachtung des Grundrechts auf Datenschutz eingesetzt werden kann. Ergänzend sollten Transparenzpflichten ausdrücklich auf den Einsatz von KI-Systemen erstreckt werden, sofern damit personenbezogene Daten verarbeitet werden. Hier sollten die gegenüber den Betroffenen bestehenden Informationspflichten zur Verarbeitung ihrer Daten um den Hinweis auf den Einsatz von KI erweitert werden.

Schließlich beschäftigt sich die DSK auch mit dem Entwurf eines Gesetzes zur Durchführung der KI-Verordnung, der im September 2025 durch das Bundesministerium für Digitales und Staatsmodernisierung vorgelegt wurde. Darin verzichtet das Ministerium zu Unrecht auf die in Art. 74 Abs. 8 KI-VO vorgesehen Möglichkeit, die Aufsicht über bestimmte Hochrisiko-KI-Systeme den Datenschutzaufsichtsbehörden zu übertragen. Stattdessen soll die Bundesnetzagentur eine umfassende Zuständigkeit erhalten. Damit verfehlt das Ministerium sein eigenes Ziel, bestehende Strukturen zu nutzen und Doppelstrukturen zu vermeiden.

Fazit

Datenschutz muss stärker auch dort verankert werden, wo technische und organisatorische Grundentscheidungen getroffen werden, nämlich bei Herstellern und Anbietern von IT-Produkten. Zugleich wird ein dringender Bedarf deutlich, die DS-GVO so weiterzuentwickeln, dass sie den besonderen Eigenschaften von KI-Modellen gerecht wird, ohne den Schutz der Grundrechte der betroffenen Personen zu schwächen.

4.2. Datenschutzkonferenz legt neue Orientierungshilfe für datenschutzkonforme KI-Systeme vor

Die Entwicklung sowie der Betrieb von KI-Systemen stellen hohe datenschutzrechtliche Anforderungen an Hersteller*innen und Entwickler*innen. So muss der Schutz personenbezogener Daten der betroffenen Personen auch technisch und organisatorisch gewährleistet sein. Um die Hersteller*innen, Entwickler*innen und letztendlich auch Verantwortlichen dabei zu unterstützen, hat die LDI NRW zusammen mit anderen deutschen Datenschutzaufsichtsbehörden nun ein Papier herausgegeben, das Orientierung gibt.

Künstliche Intelligenz (KI) betrifft in vielen Fällen personenbezogene Daten. Datenschutzanforderungen müssen deswegen bei der Entwicklung und beim Betrieb von KI-Systemen geprüft und beachtet werden. Neben der Bewertung, ob es eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten gibt, müssen auch geeignete technische und organisatorische Maßnahmen ausgewählt werden, um den Schutz dieser Daten während der Verarbeitung zu gewährleisten. Dabei ist es wichtig, diese Maßnahmen in allen Phasen des Lebenszyklus eines KI-Systems zu berücksichtigen, damit es vollständig datenschutzkonform in Verkehr gebracht wird.

Bereits 2019 hatte die DSK das Positionspapier zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen veröffentlicht. Die rasante Weiterentwicklung der Technik – insbesondere in Form von generativer, also datenproduzierender KI – macht jedoch eine regelmäßige Aktualisierung der Empfehlungen erforderlich. Zu diesem Zweck hat die LDI NRW in einer Arbeitsgruppe der DSK nunmehr im vergangenen Jahr eine Orientierungshilfe erarbeitet, welche den aktuellen Stand der KI-Entwicklung berücksichtigt. Die „Orientierungshilfe zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen – Version 1.0 (Stand: Juni 2025)” beschränkt sich nicht auf eine spezifische Kategorie von Systemen, sondern beschäftigt sich mit generativer KI ebenso wie mit klassischen Modellen, die Muster in Daten erkennen. Sie ist abrufbar unter www.datenschutzkonferenz-online.de/orientierungshilfen.html.

Im Vergleich zu traditionellen Datenverarbeitungssystemen sind KI-Systeme sowohl in der Entwicklung als auch im späteren Betrieb komplexer. Neben der Programmierung der Algorithmen und verschiedener Komponenten der Systeme müssen auch große Mengen an Trainings- und Testdaten gesammelt, aufbereitet und dem System zugeführt werden. Dies bringt viele Besonderheiten mit sich, die sich auch in der Auswahl der technischen und organisatorischen Maßnahmen widerspiegeln.

Um die Auswahl geeigneter Maßnahmen zu erleichtern, wurde in der neuen Orientierungshilfe deshalb eine Kategorisierung entwickelt, welche die verschiedenen Phasen des Lebenszyklus eines KI-Systems mit den Gewährleistungszielen des Standard-Datenschutzmodells in Verbindung setzt. Auf diese Weise entstehen 28 Kategorien, die systematisch durchgegangen werden können. Je nach Phase, in der sich die Entwickler*innen bzw. Hersteller*innen befinden, können sie so gezielt Maßnahmen auswählen, um den Anforderungen an den Datenschutz gerecht zu werden. Gleichzeitig enthält das Papier hilfreiche Tipps für die Umsetzung.

Exemplarisch dafür steht etwa das Gewährleistungsziel der Transparenz während der Design-Phase. Die „Blackbox"-Eigenschaften eines KI-Modells stellen hierbei eine besondere Herausforderung dar. In KI-Modelle kann nämlich nicht hineingesehen werden. Um die insoweit fehlende Transparenz zu kompensieren, wird in der Orientierungshilfe als geeignete Maßnahme eine umfangreiche Dokumentation der Verarbeitung der personenbezogenen Daten aufgeführt, welche auch die Trainingsdaten umfasst. Weiterhin wird die Anwendung von Methoden aus dem Gebiet der „Explainable AI" empfohlen, welche versuchen, KI-Modelle und die damit verbundenen Entscheidungsprozesse erklärbar zu machen.

Durch die Anwendung des vorgestellten Maßnahmenkatalogs können Hersteller*innen und Entwickler*innen also technische und organisatorische Maßnahmen in den verschiedenen Lebenszyklusphasen systematisch auswählen und implementieren. Allerdings kann eine Orientierungshilfe nur eine allgemeine Hilfestellung auf Basis des aktuellen Stands der Technik geben. Deshalb müssen Hersteller*innen und Entwickler*innen für Besonderheiten im jeweiligen Einzelfall möglicherweise noch weitere erforderliche technisch-organisatorische Maßnahmen treffen.

Fazit

Die neue Orientierungshilfe stellt einen Mehrwert bei der Herstellung und Entwicklung datenschutzkonformer KI-Systeme dar. Neben den Hersteller*innen und Entwickler*innen, die die unmittelbare Zielgruppe des Papiers sind, profitieren aber auch diejenigen, die die KI einsetzen wollen. Die aufgezeigten Maßnahmen können ihnen dabei helfen, ein passendes KI-System auszuwählen.

5. Internet, Medien und Digitales

5.1. Rechtswidrig Standortdaten verarbeitet – LDI NRW reagiert mit Bußgeldverfahren auf Praktiken eines Onlinedienstes

Für die LDI NRW steht fest: ein Unternehmen hatte über Jahre rechtswidrig Standortdaten von Nutzer*innen ihrer App zu Werbezwecken an Dritte weitergeleitet. Dies ist das Ergebnis umfassender Untersuchungen – die nicht ohne Konsequenzen geblieben sind.

Anfang 2025 berichteten die Medien darüber: Mutmaßliche Hacker hatten Daten des US-amerikanischen Databrokers Gravy Analytics veröffentlichet, zu denen auch Standortdaten gehörten, die mit einem Onlinedienste-Anbieter aus NRW in Verbindung gebracht wurden. Die Recherche der Journalist*innen hatte zudem ergeben, dass die Standortdaten der Nutzer*innen des Dienstes ohne Weiteres bei einem US-Databroker erworben werden konnten.

Die umfassenden Untersuchungen durch die LDI NRW, welche eine Anhörung, einen Vor-Ort-Termin sowie schriftliche Auskunftsersuchen gegenüber dem Unternehmen umfassten, führten daraufhin noch 2025 zur Einleitung eines Geldbußeverfahrens gegen den Online-Dienst. Die LDI NRW bemängelt vor allem, dass die Standortdaten ohne wirksame Rechtsgrundlage erhoben und an Dritte zu Werbezwecken weitergeleitet wurden.

Standortdaten teilen den Aufenthaltsort eines Geräts und letztlich auch der Person mit, die das Gerät bei sich führt. Sie können etwa durch

GPS, das Mobilfunknetz oder WLAN-Verbindungen erhoben werden. Zahlreiche Onlinedienste, insbesondere Navigations-Apps, nutzen solche Daten. In Kombination mit anderen Daten können solche Standortdaten allerdings auch zur Erstellung von Bewegungsprofilen genutzt werden und potentiell tiefe Einblicke in das Leben der Betroffenen ermöglichen. Sie können beispielsweise – insbesondere, wenn sie mit anderen Daten der Nutzer*innen verknüpft werden – den Wohnort, den Arbeitsort, Reisen oder Besuche bei Ärzt*innen offenbaren.

Die Gefahr eines Missbrauchs ist deshalb groß, denn wer die von dem US-Broker angebotenen Standortdaten kauft, kann damit in der Regel alle Aufenthaltsorte der Person verfolgen, die ein Handy bei sich trägt, das sich in diesem Datensatz befindet. Schlimmstenfalls können sich daraus Schlüsse über intimste Lebensbereiche von Betroffenen ziehen lassen. Zudem bestand die Gefahr einer Nutzung für kriminelle Machenschaften, etwa für Stalking oder Spionage. Sogar die Staatssicherheit war betroffen, fanden die Journalist*innen heraus, da auch Personen aus sicherheitsrelevanten Bereichen wie Militär, Ministerium, Geheimdienst oder Polizei durch die Datenhändler exponiert worden waren.

Aus datenschutzrechtlicher Sicht kann das nur heißen, dass Unternehmen bei der Verarbeitung personenbezogener Informationen, insbesondere von Standortdaten oder vergleichbaren Metadaten, darauf achten müssen, dies nur auf Basis einer wirksamen Rechtsgrundlage zu tun. Dies gilt umso mehr, sofern die Daten zu Werbezwecken an Dritte weitergeleitet werden. Hierfür kommt in der Regel nur eine wirksame Einwilligung der betroffenen Personen in Betracht. Diese Einwilligung muss freiwillig und umfassend informiert erfolgen. Dies umfasst auch eine genaue Aufklärung der betroffenen Personen, in welche Datenverarbeitungen konkret eingewilligt wird, zu welchen Zwecken die Daten verarbeitet werden und an welche Dritten eine Weiterleitung der Daten zu welchen Zwecken erfolgt.

Fazit

Die potentielle Gefährdung von betroffenen Nutzer*innen von Online-Diensten, deren Standortdaten von Anbietern rechtswidrig erhoben und an Dritte weitergegeben werden, ist hoch. Die Kombination dieser Standortdaten mit anderen verfügbaren Daten der Nutzer*innen, ermöglicht die Erstellung präziser Bewegungsprofile. Der freie Handel dieser Daten in Werbenetzwerken und auf Auktionsplattformen führt zu einem völligen Kontrollverlust der Betroffenen über die eigenen Daten. Deswegen konnte es nicht nur bei einer Anordnung zur datenschutzgerechten Anpassung des Verfahrens bleiben. Im konkreten Fall ist darüber hinaus auch die Einleitung eines Geldbußeverfahrens sachgerecht.

5.2. Alt genug für meine Inhalte? So finden Online-Anbieter*innen das heraus

Manche Angebote im Internet dürfen erst ab einem gewissen Alter genutzt werden. Wie aber können Anbieter*innen ihre Nutzer*innen überprüfen, ohne dabei deren Datenschutzrechte zu verletzen? Der Europäische Datenschutzausschuss hat dazu nun unter Beteiligung der LDI NRW eine Hilfe veröffentlicht.

Ob Streaming-Dienste, Online-Kauf oder Soziale Medien – sobald sich Kinder im Internet bewegen, laufen sie auch Gefahr, an falsche Inhalte zu geraten. Der europäische Rechtsrahmen setzt deshalb auf einen stringenten Schutz von Kindern im digitalen Umfeld. Helfen kann dabei insbesondere auch die Altersfeststellung der Nutzer*innen, um sie vor Cybermobbing, Grooming, sexueller Ausbeutung und ungeeigneten Inhalten zu bewahren.

Die Altersfeststellung selbst birgt allerdings Risiken, etwa für den Datenschutz. Denn bei der Altersfeststellung werden personenbezogene Daten der Nutzer*innen verarbeitet, die einen erheblichen Informationswert haben können, beispielsweise eine Zuordnung von Personen zu einzelnen Interessen oder sogar eine umfassendere Profilbildung ermöglichen.

Aus diesem Grund hat der Europäische Datenausschuss (EDSA) eine Hilfe für Online-Anbieter zur Altersüberprüfung erarbeitet. Am 11. Februar 2025 wurde die „Erklärung 1/2025 zur Altersfeststellung" angenommen, an der die LDI NRW intensiv mitgewirkt hat. Die Erklärung zeigt in zehn Grundsätzen Wege auf, wie eine harmonisierte datenschutzkonforme Altersfeststellung zum Schutz von Kindern im digitalen Umfeld möglich gemacht werden kann.

Grundsätzlich gibt es zahlreiche Anwendungsfelder für die Altersfeststellung, bei der zugleich Datenschutzrechte tangiert werden können. Beispielsfälle sind etwa:

- **Streaming-Dienste:** Hier kann bei einem freigegebenem Kinder-Bereich mit angepassten Inhalten eine Selbsterklärung oder eine einfache Altersangabe genügen. Andere Bereiche der Streaming-Plattform entbindet das jedoch nicht von einer dort eventuell notwendigen Altersfeststellung.
- **Online-Kauf:** Geht es um altersbeschränkte Produkte, ist eine robuste Altersfeststellung nötig (z. B. durch Zahlungsprovider-Token). Aber auch dann muss der Datenschutz gewährleistet sein. Für die Altersfeststellung erhobene Daten der Nutzer*innen dürfen etwa nicht für Werbung genutzt werden.
- **Sozialen Medien:** Bei Anmeldungen dort kann für Kinder eine mehrlagige Absicherung eingeführt werden (unter anderem durch altersüberprüfende Token). Gleichzeitig muss technisch aber verhindert werden, dass Kinder öffentlich sichtbar oder identifizierbar werden.

- **Informative Websites mit Inhalten ohne Altersspere:** Hier ist eine Altersfeststellung unverhältnismäßig und datenschutzrechtlich unzulässig.

Der Begriff „Altersfeststellung" ist dabei der Oberbegriff für die Methoden, mit denen das Alter oder die Altersgruppe einer Person bestimmt wird. Die drei Hauptkategorien der Altersfeststellung sind Altersschätzung, Altersüberprüfung und Eigenangaben.

Die zehn Grundsätze des EDSA für die Feststellung beinhalten im Einzelnen folgende Aspekte:

1. **Uneingeschränkte und tatsächliche Wahrnehmung von Rechten und Freiheiten**

   Bei der Altersfeststellung müssen sämtliche Grundrechte aller natürlichen Personen vollumfänglich gewahrt werden. Insbesondere steht das Wohl des Kindes im Mittelpunkt. Es müssen alle Kinderrechte berücksichtigt werden (z. B. beim Datenschutz, Schutz vor Gewalt, Zugang zu Informationen, Meinungsäußerung).

2. **Risikobasierte Bewertung der Verhältnismäßigkeit der Altersfeststellung**

   Die Altersfeststellung muss risikobasiert und verhältnismäßig sein. Anbieter müssen die Notwendigkeit anhand einer Risikoanalyse nachweisen – zum Beispiel im Hinblick auf Gefährdung durch Inhalte oder schädliche Kontakte. Verhältnismäßigkeit bedeutet, dass Eingriffe nur dort erfolgen dürfen, wo wirklich ein Risiko besteht.

3. **Vermeidung von Datenschutzrisiken**

   Altersfeststellung darf keine zusätzlichen Datenschutzrisiken erzeugen. Sie darf nicht zur Identifizierung, Lokalisierung, Profilbildung oder Nachverfolgung genutzt werden. Auch muss vermieden werden, dass über die Altersfeststellung hinausgehend weitere unerlaubte Zwecke verfolgt werden (z. B. personalisierte Werbung).

4. **Zweckbindung und Datenminimierung**

   Es dürfen nur die altersbezogenen Attribute verarbeitet werden, die für einen klar definierten, legitimen Zweck zwingend erforderlich sind. Daten dürfen nicht weiterverarbeitet oder kombiniert werden, wenn das zielwidrig ist. Technische und organisatorische Maßnahmen sollten eingesetzt werden, um eine abweichende Verwendung zu verhindern.

5. Wirksamkeit der Altersfeststellung

Die Verfahren zur Altersfeststellung müssen effektiv den beabsichtigten Zweck erfüllen. Dabei sind drei Dimensionen wichtig.

Zugänglichkeit: Verfahren müssen allgemein zugänglich sein, auch für Personen ohne Ausweisdokument oder mit einer Behinderung. Es braucht barrierefreie Methoden.

- Zuverlässigkeit: Verfahren müssen in der Altersfeststellung sachlich richtig und konsistent sein. Bei automatisierter Anwendung sind Rechtsbehelfe und menschliche Eingriffsmöglichkeiten erforderlich.
- Robustheit: Systeme müssen Manipulationsversuchen standhalten. Anbieter und Dritte sollten nachweisen können, wie sie diese Anforderungen erreichen.

6. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Die Verarbeitung personenbezogener Daten zur Altersfeststellung muss auf einer Rechtsgrundlage beruhen. Sie muss in Treu und Glauben erfolgen und den Nutzer*innen umfassend und verständlich transparent gemacht werden, insbesondere bei Beteiligung Dritter. Dies gilt auch für die Dauer der Speicherung, die Rechte der Betroffenen und mögliche Beschwerdewege. Kinder müssen Informationen kindgerecht erhalten.

7. Automatisierte Entscheidungsfindung

Automatisierte Verfahren zur Altersfeststellung unterliegen den Vorschriften der DS-GVO. Sie können erhebliche Auswirkungen haben (z. B. Einschränkungen im Zugang) und müssen daher mit Rechtsbehelfsmechanismen, menschlichem Eingreifen und ggf. kindgerechter Information versehen sein – insbesondere, wenn Kinder betroffen sind. Vollautomatisierte Entscheidungen sind nur ausnahmsweise zum Schutz des Kindeswohls zulässig.

8. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Systeme zur Altersfeststellung müssen gemäß Privacy by Design und Privacy by Default (Art. 25 DS-GVO) gestaltet sein. Sie sollen besonders datenschutzfreundliche Technologien (z. B. lokale Verarbeitung, Unverkettbarkeit, selektive Offenlegung, Zero Knowledge Proofs, Batch Issuance von Tokens) nutzen und stetig aktualisiert werden, um dem Stand der Technik zu entsprechen.

9. Sicherheit der Altersfeststellung

Anbieter und Dritte müssen angemessene technische und organisatorische Schutzmaßnahmen umsetzen z. B. Verschlüsselung, Pseudonymisierung, No Log Policy. Zudem brauchen sie Governance, das heißt ein Steuerungs- und Regelungssystem, Vorbereitung auf Datenschutzverstöße, Wiederherstellungsmaßnahmen sowie systemische Resilienz, um Zugangsunterbrechungen zu verhindern.

10. Rechenschaftspflicht

Es muss ein verbindlicher Governance-Rahmen etabliert sein, der Verantwortlichkeiten, Prozesse und Dokumentation für die Altersfeststellung klar regelt. Dieser Rahmen ermöglicht die Nachweisbarkeit und schafft Vertrauen sowohl für interne Prüfungen als auch gegenüber Behörden und Betroffenen.

Der EDSA arbeitet unter Mitwirkung der LDI NRW an weiteren Veröffentlichungen zu Datenschutzrechten von Kindern einschließlich weiteren Ausführungen zur Altersfeststellung.

Fazit

Altersfeststellung im digitalen Umfeld findet in einem Spannungsfeld von Kinderrechten und Datenschutz für Kinder und Erwachsene statt. Aus der Altersfeststellung können eigene Risiken für personenbezogene Daten erwachsen. Die zehn Grundsätze des EDSA ermöglichen eine rechtskonforme, abgesicherte Umsetzung und einen Ausgleich der Interessen.

5.3. Wenn Reiseveranstalter*innen Werbevideos auf Facebook posten

Kunden anlocken mit kleinen Filmen in den Sozialen Medien – auch in der Reisebranche sind solche Werbemittel mittlerweile beliebt. Doch das Ganze hat datenschutzrechtliche Grenzen. Etwa, wenn leicht bekleidete Badegäste gezeigt werden.

Wer findet sie nicht faszinierend, die Bilder von Sonne, Wasser und fröhlichen Urlauber*innen? Sie vermitteln gute Stimmung, Entspannung und unbeschwerte Tage. Kein Wunder, dass entsprechende Werbefilme immer häufiger den Weg in die Sozialen Medien finden. Und je echter sie wirken, desto mehr Wirkung haben sie.

Genau an diesem Punkt aber wird es grenzwertig. Denn sobald reale Personen ins Spiel kommen, werden auch Fragen nach dem Datenschutz laut. Das zeigt exemplarisch ein Fall, mit dem sich die LDI NRW beschäftigt hat.

Die LDI NRW war durch einen Hinweis auf ein Werbevideo aufmerksam geworden, das ein Veranstalter von Kreuzfahrten auf seinem geschäftlichen Facebook-Profil hochgeladen hatte. In dem Video wurde der auf dem Dach eines Hotels befindliche Skypool in Dubai gezeigt, in dem sich zahlreiche Reisende zum Abschluss ihrer Kreuzfahrt vergnügten. Der überwiegende Teil der Reisenden trug dabei Badebekleidung, ruhte auf Liegen oder schwamm im Pool.

Anders als die LDI NRW fand das Unternehmen darin nichts Problematisches. Die Geschäftsführung berief sich bei der Verarbeitung der Aufnahmen auf ein berechtigtes Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Nach dieser Norm ist die Verarbeitung rechtmäßig, wenn sie zur

Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist – sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der von der Verarbeitung betroffenen Person überwiegen. Dies gilt insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Außerdem führte der Unternehmer an, die aufgenommenen Personen seien lediglich „Beiwerk" nach § 23 Abs. 1 Nr. 2 des Kunsturhebergesetzes (KUG) und ohne erhebliches Zusatzwissen nicht identifizierbar.

Die LDI NRW sieht dies grundlegend anders. Zwar stellt die Bewerbung von Reisen auch über die Sozialen Medien ein berechtigtes Interesse von Reiseveranstalter*innen dar. Gleichwohl überwiegen hier die Interessen der betroffenen Personen, nicht in ihrem Urlaub gefilmt und leicht bekleidet einem weltweiten Publikum auf der Plattform „Facebook" dauerhaft zur Schau gestellt zu werden.

Sofern sich das Unternehmen auf Ausnahmen durch das KUG berufen will, sind diese gar nicht einschlägig. Denn die Vorschriften der DS-GVO stehen der Anwendung der §§ 22, 23 KUG nur im journalistischen, wissenschaftlichen, künstlerischen oder literarischen Bereich nicht entgegen. Nur dann, wenn die Datenverarbeitung zu solchen Zwecken erfolgt, sind Abweichungen oder Ausnahmen von den Datenschutzbestimmungen der DS-GVO durch nationale Regelungen zulässig. Im konkreten Fall hat der Reiseveranstalter die Daten aber nicht zu diesen Zwecken verarbeitet. Hinzu kommt, dass entgegen der Ansicht des Unternehmers die aufgenommenen Personen auch relativ leicht identifizierbar sind, da es sich um Daten handelt, die aufgrund ihrer videografischen Darstellung aus sich heraus einer Person zuordenbar sind. Auch das Argument, es handele sich um einen beliebten Ort von Influencer*innen führt nach Ansicht der LDI NRW nicht dazu, dass die betroffenen Personen damit rechnen müssten, in einem Werbevideo veröffentlicht zu werden. Vielmehr ist der Umstand, dass sich die betroffenen Personen im Urlaub und damit im Rahmen ihrer Freizeitgestaltung an diesem Ort befinden, besonders schutzwürdig, da sie damit ihre grundrechtlich geschützte Freiheit der persönlichen Entfaltung ausüben. Letztlich konnte auch das Argument nicht überzeugen, keiner der Reisenden habe sich gegen die Aufnahmen gewehrt. Den Betroffenen dürfte nämlich bei der Aufnahme kaum bewusst gewesen sein, dass sie gerade zum Gegenstand eines Werbevideos durch ihren Reiseveranstalter gemacht wurden.

Trotz mehrmaliger Aufforderungen durch die LDI NRW, die in dem Video befindlichen Personen unkenntlich zu machen oder das Video zu löschen, hat sich das Unternehmen bislang geweigert, den Vorgaben nachzukommen. Die LDI NRW hat es daher letztendlich förmlich angewiesen, die in dem Video befindlichen Personen unkenntlich zu machen, sofern keine Einwilligung vorliegt. Gegen diese Anordnung hat der Unternehmer Klage eingereicht. Über den Ausgang des Verfahrens wird die LDI NRW zu gegebener Zeit berichten.

Fazit

Unternehmen sollten Werbung datenschutzgerecht ausgestalten. Bei bildhaften Darstellungen von Personen, etwa in Videos, noch dazu in besonders schutzwürdigen Lebenssituationen, sind die Interessen der betroffenen Personen hinreichend zu berücksichtigen. Eine Interessenabwägung geht hier regelmäßig zu Gunsten der betroffenen Personen aus.

6. Schule und Bildung

6.1. „Ich frag' einfach Chatty" – Einsatz von KI macht Schule

Ein Gedicht interpretieren, eine Präsentation erstellen, Rat bei persönlichen Problemen einholen – immer mehr Schüler*innen nutzen KI-Modelle wie etwa ChatGPT. Für Schulen heißt das: Sie müssen mit datenschutzgerechten Lösungen einen verantwortungsvollen Umgang mit diesen Large Language Models vermitteln.

Noch vor wenigen Jahren waren sie weitgehend unbekannt, mittlerweile sind sie selbst aus dem Schulalltag kaum wegzudenken: Large Language Models, kurz LLMs, die auf Smartphones genutzt werden können und nahezu auf jede Frage eine Antwort parat haben. Nicht nur bei Schüler*innen, auch bei Lehrkräften ist deren Einsatz verständlicherweise beliebt. Bei unmittelbarer Nutzung frei zugänglicher LLMs wie GPT-4 oder Gemini erhält der*die Anbieter*in allerdings Kenntnis von den bei der Nutzung anfallenden Daten. Und das bringt datenschutzrechtliche Probleme mit sich. Die LDI NRW hat sich deshalb 2025 eingehend mit der Thematik beschäftigt.

Zunächst: Werden Fragen an LLMs gestellt, werden nicht nur technische Daten über das verwendete Gerät den Anbieter*innen zugänglich gemacht ebenso sowie IP-Adresse oder Logdateien, sondern auch die sog. Prompts selbst. Prompt ist die mittlerweile gängige Bezeichnung für eine Eingabe. Solche Prompts lassen allerdings – unabhängig von der Eingabe von Namen – Rückschlüsse auf die jeweilige Person zu, die die Eingabe macht. Ihre individuelle Sprache, typische Fehler bis hin zu sensiblen Daten wie persönlichen oder familiären Problemen oder Gesundheitsdaten können anhand der Prompts ablesbar sein. Je

nach Sprachmodell besteht deshalb das Risiko, dass diese Daten von Anbieter*innen ausgewertet, zu eigenen Zwecken, wie Werbung oder Training der Modelle, verwendet oder in Länder übermittelt werden, die nicht den europäischen Datenschutzstandard garantieren.

Schulen sollten die Schüler*innen daher für diese Situation ebenso sensibilisieren wie für KI-spezifische Probleme, etwa überzeugend formulierte, aber falsche KI-Resultate (KI-Halluzinationen), mit KI-Techniken verfälschte Medieninhalte (Deep-Fakes) oder diskriminierende Ergebnisse durch verzerrte Dateneingabe (BIAS). Zu diesem Zweck ist es wichtig, den Umgang mit KI im Schulunterricht zu thematisieren und zu üben.

Bei der Nutzung von LLMs sollten die Schulen darüber hinaus die Risiken für die Schüler*innen und Lehrkräfte durch geeignete technisch und organisatorische Maßnahmen im größtmöglichen Umfang reduzieren (Art. 24, 25 und 32 DS-GVO). Hierzu zählen insbesondere, zuverlässige Anbieter*innen auszuwählen, so wenig personenbezogene Daten wie möglich einzugeben und die Verarbeitung personenbezogener Daten zu eigenen Zwecken der Anbieter*innen auszuschließen.

Soweit dennoch personenbezogene Daten verarbeitet werden, bieten § 120 Abs. 5 bzw. § 121 Abs. 1 Satz 1 und 2 SchulG (Einsatz von Lehr- und Lernsystemen) einstweilen eine mögliche Rechtsgrundlage. Die beim Einsatz von KI-Technologien durchzuführende Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) kann möglicherweise jedoch auch zu dem Ergebnis führen, dass einzelne Aspekte der KI-Nutzung einer speziellen rechtlichen Regelung bedürfen. Eine Datenschutz-Folgenabschätzung ist eine Pflicht nach der DS-GVO, geplante Verarbeitungen personenbezogener Daten auf ein hohes Risiko für Betroffene zu prüfen und dieses zu minimieren, bevor die Verarbeitung startet.

Da die einzelnen Schulen mit der Umsetzung hinreichender technischer und organisatorischer Maßnahmen häufig überfordert sein dürften, begrüßt die LDI NRW das länderübergreifende Projekt „telli". Diese KI-Chatbot-Anbindung ermöglicht die Nutzung verschiedener LLMs über pseudonymisierte Accounts. Die Datenverarbeitung erfolgt im Rahmen eines Auftragsverarbeitungsvertrags mit dem Medieninstitut der Länder der Bundesrepublik Deutschland. Hierin soll unter anderem geregelt werden, dass bereits vortrainierte Modelle verwendet und Daten nicht für das weitere Training der Modelle genutzt werden. Die Datenverarbeitung soll ausschließlich in der EU stattfinden und Chatverläufe sollen regelmäßig gelöscht werden. Die LDI NRW wurde vom Schulministerium NRW in das Projekt eingebunden und berät das beauftragte Medieninstitut gemeinsam mit anderen Datenschutzaufsichtsbehörden in datenschutzrechtlichen Fragen.

Fazit

LLMs haben auch im Schulalltag eine Menge Potential, ihre Nutzung ist aber zugleich mit Risiken für Schüler*innen und Lehrkräfte verbunden. Um die Betroffenen für einen verantwortungsvollen Umgang mit KI zu sensibilisieren, brauchen die Schulen datenschutzfreundliche Lösungen. Hierzu leistet die LDI NRW ihren Beitrag.

6.2. iPads im Unterricht: Noch gibt es keine Entwarnung, aber die Entwicklung ist positiv

Schulen, die iPads einsetzen, stehen vor der Herausforderung, datenschutzgerechte Backup-Lösungen zu gewährleisten. In einem Regierungsbezirk von NRW werden dazu Gespräche mit Apple geführt, an denen sich die LDI NRW beteiligt. Noch fehlt letzte Sicherheit.

Sog. Tablets sind mittlerweile im deutschen Schulunterricht angekommen. Laut einer Untersuchung von Statista haben über 50 Prozent aller Schüler*innen hierzulande bereits mit diesen flachen, tragbaren Computern gearbeitet. Insbesondere das iPad des US-Konzerns Apple kommt dabei zum Einsatz. Das allerdings ist nach wie vor nicht völlig unproblematisch. So wollen Schulen und Schulträger verständlicherweise Geräte-Backups einsetzen, um defekte und verlorengegangene iPads von Schüler*innen und Lehrkräften schnellstmöglich ohne Datenverlust ersetzen zu können. Für iPads sind solche Geräte-Backups aktuell aber nur über die iCloud möglich. Und hier sind noch Fragen offen.

Im letzten Tätigkeitsbericht hatte die LDI NRW Schulen und Schulträgern empfohlen, auf die Nutzung der iCloud zu verzichten. Gründe hierfür waren insbesondere Anhaltspunkte in den Vertragsunterlagen, dass von Apple erfasste Nutzungsdaten zur Produktentwicklung sowie weiteren unternehmensinternen Zwecken verwendet werden. Außerdem gibt es Hinweise auf eine Datenübermittlung in Drittländer ohne angemessenes Datenschutzniveau (siehe dazu 30. Bericht unter 7.2).

Um eine datenschutzgerechte Backup-Lösung für Schulen zu finden, hat sich die LDI NRW deshalb beratend an Gesprächen mit Apple und einem Schulträger beteiligt, die von einer Bezirksregierung initiiert wurden. Dabei hat Apple klargestellt, dass für Schulen der Apple-Schoolmanager-Vertrag relevant sei, abrufbar unter **www.apple.com/legal/education/apple-school-manager/ASM-DE-DE.pdf**. Laut Angaben von Apple findet in diesem Zusammenhang keine Verarbeitung zu eigenen Zwecken statt. Die Daten würden nur zum Zweck der Bereitstellung und Unterstützung der Dienste verarbeitet. Internationale Datentransfers würden auf Standardvertragsklauseln (Standard Contractual Clauses – SCCs) der EU gestützt.

Die Daten deutscher Nutzer*innen würden regelmäßig ausschließlich in den USA und im Europäischen Wirtschaftsraum verarbeitet.

Diese Darstellung von Apple geht allerdings aus dem vorgelegten Apple-Schoolmanager-Vertrag für deutsche Schulen nicht klar hervor. Er enthält teilweise nicht eindeutige und schwer verständliche Passagen. So ergeben sich aus diesem Vertrag jedenfalls nach wie vor Anhaltspunkte dafür, dass Apple Daten der Nutzer*innen zur Verbesserung seiner Produkte verwendet oder sich dies zumindest vorbehält. Auch die Datenübermittlung in weitere Drittländer – über die USA hinaus – ist vertraglich nicht ausgeschlossen.

Aus Sicht der LDI NRW ist eine Ende-zu-Ende-Verschlüsselung der in der iCloud gespeicherten Daten, bei der die Schlüssel nicht bei Apple liegen, die datenschutzrechtlich nachhaltigste Lösung. Auch eine Öffnung der Geräte-Backup-Funktion für alternative Cloud-Lösungen wäre eine Option. Apple hat angekündigt, die von der LDI NRW vorgebrachten Punkte zu prüfen.

Fazit

Trotz der Bemühungen um eine datenschutzgerechte Backup-Lösung für iPads konnten Bedenken bislang noch nicht vollständig ausgeräumt werden. Die LDI NRW ist aber optimistisch, dass sich die angesprochenen Fragen auch vertraglich nachzeichnen lassen. Bis dahin bleiben Schulen auf der datenschutzrechtlich sicheren Seite, wenn sie auf die Nutzung der iCloud bis zur vollständigen Klärung verzichten.

6.3. Sind Bildaufnahmen auf Schüler*innen-Handys für Lehrkräfte und Schulleitung tabu?

Ob in der Schule oder auf Klassenfahrten: Schüler*innen machen oft Fotos und Filme, um diese weiterzuschicken oder in den Sozialen Medien hochzuladen. Doch nicht immer ist das rechtens. Dürfen Lehrkräfte oder die Schulleitung die Aufnahmen einsehen? Oder können sich die Schüler*innen und ihre Eltern auf den Datenschutz berufen?

Smartphones und die Sozialen Medien sind aus dem Schulalltag nicht mehr hinwegzudenken. Sie gehören zur Lebenswelt vieler Schüler*innen wie selbstverständlich dazu. In datenschutzrechtlicher Hinsicht allerdings ist der freie Umgang mit diesen Alltagsbegleitern nicht immer unproblematisch. Manche Bilder etwa zeigen andere Schüler*innen oder Lehrkräfte, zum Teil in bloßstellender Weise, ohne dass diese hierin eingewilligt haben. Auf anderen Aufnahmen sind teilweise Regelverstöße in der Schule oder sogar strafrechtlich relevantes Verhalten von Schüler*innen zu sehen, wie zum Beispiel Sachbeschädigung oder das Skandieren verfassungswidriger Parolen.

Der LDI NRW ist es deshalb auch 2025 ein Anliegen gewesen, Hinweise zu geben, wo in solchen Fällen die Grenzen liegen – und welche Rechte Schüler*innen und deren Eltern ebenso wie Lehrer*innen und Schulleitung haben.

Grundsätzlich dürfen Schüler*innen bei schulischen Veranstaltungen Bildaufnahmen von anderen nur machen, sofern eine Einwilligung vorliegt oder diese Aufnahmen später ausschließlich im Familien-, Freundes- oder

Bekanntenkreis gezeigt werden (sog. Haushaltsausnahme). Nähere Einzelheiten sind der Veröffentlichung der LDI NRW „Bildaufnahmen in der Schule? Was ist erlaubt? Wo ist die Grenze?" zu entnehmen, abrufbar unter **www.ldi.nrw.de/Bildaufnahmen-in-der-Schule**.

Sofern es darum geht, welche Kontrollrechte die Lehrkräfte und Schulleitung in diesem Zusammenhang haben, gehen Schüler*innen und ihre Eltern häufig davon aus, dass der Datenschutz den Schulen verbietet, sich die gefertigten Bildaufnahmen auf privaten Handys anzuschauen. Das trifft in dieser Allgemeinheit jedoch nicht zu. Vielmehr ist hier zu differenzieren: Geht es um die Aufklärung von möglichen Regelverstößen, ist das Ansehen von Bildern unter gewissen Voraussetzungen erlaubt. Ein eigenmächtiges Durchsuchen von Handys ist allerdings nicht zulässig.

Konkret: Wenn Schulen Bildaufnahmen auf den Handys von Schüler*innen anschauen, verarbeiten sie deren Daten. Dies ist erlaubt, soweit es zur Erfüllung der ihnen durch Rechtsvorschrift übertragenen Aufgaben erforderlich ist (§ 120 Abs. 1 Satz 1 Schulgesetz NRW – SchulG NRW). Die Schule unterrichtet und erzieht Kinder und Jugendliche auf der Grundlage des Grundgesetzes und der Landesverfassung NRW (§ 2 Abs. 1 SchulG NRW). Sie verwirklicht damit die in Art. 7 der Landesverfassung NRW bestimmten allgemeinen Bildungs- und Erziehungsziele, die unter anderem die Achtung der Menschenwürde beinhalten. Verstoßen also Schüler*innen gegen Regeln oder zeigen sie sogar strafrechtlich relevantes Verhalten, ist die Schule nicht nur berechtigt, sondern – beim Verdacht auf eine Straftat unter Hinzuziehung der Strafverfolgungsbehörden – möglicherweise sogar verpflichtet, den Sachverhalt aufzuklären, um hierauf mit geeigneten pädagogischen Maßnahmen zu reagieren. Solche Maßnahmen kommen dabei auch dann in Betracht, wenn das Fehlverhalten nicht in der Schule stattgefunden hat (vgl. hierzu den Runderlass „Zusammenarbeit bei der Verhütung und Bekämpfung der Jugendkriminalität" vom 19. November 2022).

Beim Verdacht eines Regelverstoßes kann die Schule dementsprechend den*die Schüler*in auffordern, ihr Zugang zu konkreten Bildaufnahmen auf dem Handy zu gewähren, um den Sachverhalt weiter zu ermitteln. Kommt der*die Schüler*in der Aufforderung nach, darf die Schule sich die Bildaufnahmen ansehen und diese zu Beweiszwecken sichern. Dabei muss sie die Grenzen des Erforderlichen einhalten und darf die Daten in der Schule nur den für pädagogische Maßnahmen zuständigen Personen zugänglich machen (§ 120 Abs. 1 Satz 1 und 2 SchulG NRW).

Nicht erlaubt ist der Schule hingegen, das Handy eigenmächtig zu durchsuchen. Wenn die Schulleitung den begründeten Verdacht hat, dass sich auf dem Handy eines*einer Schüler*in strafrechtlich relevante Bildaufnahmen befinden und diese*r sich weigert, ihr Zugang hierzu zu gewähren, hat sie die Möglichkeit, die Polizei einzuschalten. Diese verfügt über Befugnisse, den auf dem Smartphone befindlichen Inhalt zu untersuchen und weitere Schritte einzuleiten.

Generell ist es aber sicher am besten, Datenschutzverstöße von Schüler*innen durch die Nutzung privater Handys gleich im Vorhinein zu vermeiden. Die LDI NRW begrüßt deshalb, dass das Schulministerium NRW den Schulen vorgegeben hat, sich altersgerechte Regelungen für die private Handynutzung zu geben und diese in die Schulordnung aufzunehmen. Mehr dazu findet sich auf der Webseite des Ministeriums unter **www.schulministerium.nrw/handynutzung-schule**.

Fazit

Schulen sollten ihre Schüler*innen für den Umgang mit Fotos und Filmen sensibilisieren und Nutzungsregeln für den Gebrauch digitaler Geräte (Mobiltelefone, Tablets etc.) festlegen. Kommt es trotzdem zu Rechtsverstößen, darf die Schule ihre pädagogischen Möglichkeiten nutzen, um den Sachverhalt aufzuklären.

7. Inneres, Justiz und Verwaltung

7.1. Überarbeitetes Polizeigesetz NRW bleibt unzureichend – neue Probleme bei Nutzung und Training von KI

Nach Entscheidungen des Bundesverfassungsgerichts musste das Land NRW sein Polizeigesetz überarbeiten – und hat dies zum Anlass genommen, die polizeilichen Befugnisse zur Datenanalyse und KI-Training auszuweiten. Notwendige Anpassungen zum Schutz der Bürger*innen, blieben aus.

Eigentlich waren die Vorgaben klar umrissen. Im November 2024 machte das Bundesverfassungsgericht deutlich, dass und wo es das Polizeigesetz NRW (PolG NRW) für verfassungswidrig hält. Den Richter*innen waren die dort festgelegten Voraussetzungen nicht ausreichend, ab wann eine Überwachung von Bürger*innen mittels einer Kombination aus Observation und begleitender technischer Überwachung zu Gefahrenabwehrzwecken erlaubt ist. Dem Land NRW gaben sie bis zum 31. Dezember 2025 Zeit, das zu ändern.

Das Innenministeriums nahm dies zum Anlass, um zusätzlich zu den Vorgaben gleich neue Regelungen ins PolG NRW aufzunehmen, die die Befugnisse der Polizei noch erweitern. Die LDI NRW hat sich intensiv damit beschäftigt und in Ihrer Stellungnahme darauf hingewiesen, dass einige Regelungen dem Grundsatz der Verhältnismäßigkeit nicht ausreichend Rechnung tragen und damit die Rechte der Bürger*innen gefährden. Trotz mehrfacher Intervention wurden ihre Einwände jedoch im Gesetzgebungsverfahren nicht berücksichtigt.

Konkret geht es zum einen um die umstrittene Datenanalyse-Software „Palantir", in NRW als Software für „Datenanalyse- und Recherche" (DAR) bekannt. Ihr Einsatz wird in NRW auf § 23 Abs. 6 PolG NRW gestützt. Dabei bestehen gegen diese Norm bis heute erhebliche verfassungsrechtliche Bedenken. Beim Bundesverfassungsgericht ist eine Verfassungsbeschwerde anhängig. Die Verfassungsrichter*innen hatten zudem im Februar 2023 zu ähnlichen Normen aus Hessen und Hamburg entschieden, dass die gesetzlichen Vorgaben für den Einsatz von Datenanalysetools umso höher sein müssen, je stärker mit der Datenanalyse in die Grundrechte der Betroffenen eingegriffen wird. Die mit den Analysen verbundenen Eingriffe wiegen dabei umso schwerer, je mehr und je sensiblere Daten in die Analyse einbezogenen werden und je komplexer die Methoden sind, mit der die Analysesoftware sie auswertet.

Gemessen an diesen vom Bundesverfassungsgericht getroffenen Aussagen sieht die LDI NRW schon beim ursprünglichen Text des PolG NRW die Notwendigkeit zu gesetzlichen Ergänzungen. Sie hat dies auch in ihrer Stellungnahme zum damals noch im Gesetzgebungsverfahren befindlichen überarbeiteten Gesetz deutlich gemacht.

Doch die Landesregierung ist darauf nicht nur nicht eingegangen – sie hat im überarbeiteten PolG NRW das Eingriffsgewicht möglicher polizeilicher Datenanalysen sogar noch einmal verschärft. Das hat zur Folge, dass das neue Gesetz erst recht nicht die Anforderungen an eine verfassungskonforme Norm erfüllen dürfte.

Konkret: Vor der Anpassung durften Daten ausdrücklich nicht mittels statistisch-mathematischer Verfahren oder in sonstiger Weise selbständig auf Zusammenhänge analysiert werden. Das auf § 23 Absatz 6 PolG NRW gestützte Verfahren DAR funktioniert daher bisher eher wie eine Suchmaschine im Polizeidatenbestand. Schon das hat ein hohes Eingriffsgewicht, da damit systematisch der Grundsatz der Zweckbindung der Daten durchbrochen wird. Betroffene, deren Daten sich in Polizeiakten befinden, haben nämlich keinerlei Kontrolle mehr darüber, für welche anderen Zwecke diese Daten noch herangezogen werden.

Die nun beschlossene Änderung des PolG NRW geht aber noch weit darüber hinaus. Künftig dürfen insbesondere Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt werden. Es dürfen zudem unbedeutende Informationen und Erkenntnisse ausgeschlossen, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden – und das auch mittels selbstständig arbeitender oder selbstlernender Systeme, also mittels KI. Damit besteht bei den einsetzbaren Analysetechniken überhaupt keine nennenswerte Einschränkung mehr. Diese sind nicht mehr nur auf die schlichte Suche nach bestimmten Personen beschränkt, die die Polizei bereits in Verdacht hat, oder nach bekannt gewordenen Daten, etwa Telefonnummern oder Fahrzeugkennzeichen. Das überarbeitete PolG NRW lässt, kurz gesagt, höchst

eingriffsintensive Durchforstungen des polizeilichen Datenbestands zu – und das bei ungenügender Regelung der entsprechenden Voraussetzungen dafür.

Mindestens ebenso kritisch ist die neu eingeführte KI-Trainingsregelung zu sehen. Danach ist es der Polizei in NRW künftig erlaubt, die von ihr rechtmäßig gespeicherten Daten zum Training von IT-Produkten – also auch von KI-Anwendungen – zu verwenden. Hierfür sieht die Norm so gut wie keine Einschränkungen oder Voraussetzungen vor. Zwar sollen die verwendeten Daten grundsätzlich anonymisiert werden. Das kann jedoch laut Gesetz unterbleiben, wenn dies „voraussichtlich mit einem hohen Aufwand verbunden" ist. Angesichts der Vielzahl der bei der Polizei gespeicherten Daten dürfte die Versuchung groß sein, die Anonymisierung in einer nennenswerten Anzahl von Fällen für „zu aufwändig" zu erklären.

Hierzu ist anzumerken, dass die KI darauf ausgelegt ist, Zusammenhänge zwischen Daten zu erkennen. Zusammenhänge zu einer Person können deshalb auch dann hergestellt werden, wenn der Name weggelassen wurde. Eine Anonymisierung gestaltet sich damit generell schwierig. Insgesamt sind im Gesetz nicht ansatzweise ausreichende Maßnahmen geregelt, um den mit der Nutzung zu Trainingszwecken einhergehenden Risiken für sämtliche Bürger*innen, deren Daten beispielsweise auch als Opfer oder Zeug*innen gespeichert sind, angemessen zu begegnen.

Zur Rechtfertigung, die ursprüngliche Befugnis zur Datenanalyse einzuführen, wurde zudem stets angeführt, dass dieser Eingriff keine große Intensität aufweise – da KI gerade nicht zum Einsatz komme und auch der Zugriff des Programmanbieters auf Polizeidaten nicht möglich sei. Wenn nun das Training von KI mit Polizeidaten oder gar das Training des Datenanalyseprogramms durch externe Anbieter*innen und gegebenenfalls explizit „Palantir" vorgenommen wird, wirft dies zusätzliche Probleme auf. Sie dürften für die Beurteilung der Zulässigkeit des Verfahrens und auch für die das Verfahren ermöglichende Norm wesentlich sein. Denn wird beim KI-Training kein für die Polizei NRW speziell entwickeltes Modell trainiert, besteht das Risiko, dass die Informationen aus den Trainingsdaten auch anderen Kund*innen des US-Anbieters über das zentrale Modell zur Verfügung gestellt werden. Die LDI NRW hat die Landesregierung darauf hingewiesen, dass der Programmanbieter der US-amerikanischen Gesetzgebung unterliegt. Die wiederum gibt den US-Behörden gemäß dem sog. Cloud Act und dem sog. Foreign Intelligence Surveillence Act weitreichende Möglichkeiten, auf die Daten des Anbieters zuzugreifen. Da das Programm den Polizeidatenbestand nahezu vollständig einbezieht, würde dieser Datenbestand dann, wenn er im Zusammenhang mit KI-Training auch dem Programmanbieter zur Verfügung steht, nicht kontrollierbaren Zugriffen der US-Behörden unterliegen.

Schließlich: Mit der Überarbeitung des PolG NRW sollte auch die sog. BKAG II-Entscheidung des Bundesverfassungsgerichts umgesetzt werden. Darin hat sich das Gericht erstmals grundlegend zu den verfassungsmäßigen Anforderungen an die Fortspeicherung von personenbezogenen polizeilichen Daten für den Fall geäußert, dass die Speicherung zu einem anderen

Zweck erfolgt als zu dem, der der Erhebung der Daten zugrunde lag. Es ging also um Zulässigkeit der Datenspeicherung für eine künftige Aufgabenerfüllung (Gefahrenabwehr bzw. Straftatenverhütung).

Die Vorgaben der Verfassungsrichter*innen sind hier eindeutig: Die vorsorgende Speicherung stellt eine Zweckänderung dar und bedarf als solche einer gesetzlichen Grundlage. Dabei darf der Staat grundsätzlich nicht alle Daten, die er rechtmäßig erhoben hat, über den primären Zweck hinaus vorsorgend mit der Begründung speichern, die Daten könnten künftig noch einmal benötigt werden. Schon die Speicherung für künftige Zwecke muss an ausreichende gesetzliche Voraussetzungen geknüpft werden (sog. Schwellen). Dies ist bei der gesetzlichen Änderung des § 22 PolG NRW nur zum Teil gelungen.

Aus der Entscheidung des Bundesverfassungsgerichts ergibt sich nämlich noch weiterer Änderungsbedarf, der unberücksichtigt geblieben ist. Der Vorschrift fehlt es insbesondere an einer ausreichenden Differenzierung hinsichtlich der unterschiedlichen Speicherzwecke. Mit der Norm wird die Speicherung polizeilicher Daten zu ganz unterschiedlichen Zwecken „in einem Abwasch" geregelt. Hierzu gehören die Speicherung zur Gefahrenabwehr, die Speicherung zur Dokumentation, die Betroffenen auch die (gerichtliche) Überprüfung der Rechtmäßigkeit der Verarbeitung ihrer Daten ermöglichen soll, sowie die – im BKAG II-Urteil behandelte – Fortspeicherung zur künftigen Aufgabenerfüllung, also gewissermaßen eine Speicherung „auf Vorrat". Diese drei genannten Speicherzwecke haben jedoch ganz unterschiedliche Eingriffswirkungen und sind daher nach dem Gebot der Verhältnismäßigkeit unterschiedlich zu betrachten. Beispielsweise besteht bei den zur Dokumentation gespeicherten Daten keine Notwendigkeit, sie suchfähig für andere Zwecke zu speichern. Vielmehr ist eine Nutzungsbeschränkung auf die Zwecke der Dokumentation festzulegen. Außerdem ist bei lediglich zur Dokumentation gespeicherten Daten eine regelmäßige Speicherdauer von mehr als zwei Jahren unverhältnismäßig. Die Speicher- und Löschvorgaben im Polizeigesetz sind – insbesondere nach der BKAG II-Entscheidung – im Ganzen überarbeitungsbedürftig.

Auf diese und weitere mit dem überarbeiteten Gesetz einhergehenden Risiken für die Grundrechte der Bürger*innen hat die LDI NRW das Innenministerium hingewiesen und dies zusätzlich in einer an den Landtag NRW gerichteten Stellungnahme deutlich gemacht. Keiner dieser Hinweise wurde im Gesetzgebungsverfahren berücksichtigt.

Fazit

Die vom Bundesverfassungsgericht gestellten Pflichtaufgaben wurden mit der Änderung des PolG NRW durch das 8. Änderungsgesetz teilweise umgesetzt. Die darüberhinausgehenden zusätzlichen Regelungen begründen jedoch neue Zweifel an der Verfassungsmäßigkeit der Normen. Leider konnte die LDI NRW keine Auseinandersetzung mit ihren Bedenken feststellen. Vermutlich wird auch das überarbeitete Gesetz vor dem Bundesverfassungsgericht landen.

7.2. Neues Verfassungsschutzgesetz NRW: Landesregierung weitet Befugnisse deutlich aus

Das Verfassungsschutzgesetz NRW hatte gut dreißig Jahre auf dem Buckel; es war schon lange nicht mehr zeitgemäß. Mit der Neugestaltung wird manches verbessert, die neuen Befugnisse tragen allerdings teils selbst dem Anspruch der Verfassung noch nicht ausreichend Rechnung.

Der Verfassungsschutz soll, wie sein Name schon sagt, die Bundesrepublik und ihre verfassungsmäßige Grundordnung vor Bedrohungen durch Extremismus, Terrorismus und Spionage schützen. Dafür steht ihm ein großer Werkzeugkasten zur Verfügung, der zugleich auch intensive Eingriffe in die Freiheitsrechte der Bürger*innen erlaubt. Indem der Verfassungsschutz unzählige Daten sammelt und auswertet, soll er in die Lage versetzt werden, Gefahren frühzeitig zu erkennen, damit sie abgewehrt werden können.

Umso wichtiger ist es daher, dass die Rechtsgrundlagen für derartige Eingriffe selbst der Verfassung entsprechen. Hier offenbarte sich allerdings zuletzt erheblicher Nachbesserungsbedarf, wegen vieler in den letzten Jahren ergangener Entscheidungen des Bundesverfassungsgerichts. So hatte das Gericht mehrfach die verfassungsrechtlichen Vorgaben in dem noch aus dem 20. Jahrhundert stammenden Verfassungsschutzgesetz NRW kritsiert. Die Landesregierung hat daraufhin im vergangenen Jahr das Gesetz vollständig überarbeitet. Aus Sicht der LDI NRW enthält das Ergebnis neben Licht auch Schatten.

Insgesamt umfasste der Entwurf rund 340 Seiten. Ebenfalls sehr umfangreich war die Stellungnahme der LDI NRW, in der sie verdeutlichte, dass verfassungsrechtlich Ergänzungen geboten sind, die die Verhältnismäßigkeit und Rechtsklarheit der Normen sicherstellen. Doch das Ministerium berücksichtigte nur beiläufige, redaktionelle Hinweise. Die materiellen verfassungsrechtlichen Kritikpunkte wurden gänzlich ignoriert. Nicht einmal eine Nachfrage gab es dazu.

Neben weiteren Sachverständigen hat die LDI NRW daher im parlamentarischen Verfahren erneut auf die kritischsten Punkte des Entwurfs hingewiesen. Die Stellungnahme der LDI NRW ist als Landtagsdrucksache 18/2862 abrufbar unter **https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/MMST18-2863.pdf**. Danach wurde dieser zwar in einigen Bereichen verbessert. Aus Sicht der LDI NRW bestehen jedoch weiterhin große Bedenken, ob das nunmehr in Kraft getretene Gesetz der Verfassung ausreichend Rechnung trägt. Die Bedenken beziehen sich vor allem auf:

- ein im Wesentlichen unbeschränkt mögliches Web-Crawling,
- die nicht näher eingegrenzte und nun erlaubte Nutzung von Datenanalysetools auch mittels KI,

- die Nutzung von Daten des Verfassungsschutzes zu Trainingszwecken von KI-Produkten sowie
- die neu eingeräumten Zugriffsmöglichkeiten des Verfassungsschutzes auf die Videoüberwachung durch Private.

Bei der Durchforstung des Internets (Web-Crawling) und des beim Verfassungsschutz vorhandenen Datenbestands (Datenanalyse) sind jeweils riesige Datenpools betroffen. Dabei werden sowohl im vorhandenen Datenbestand als auch im Internet keineswegs nur Daten von Personen ausgewertet, die unter der Beobachtung des Verfassungsschutzes stehen. Betroffen sind auch Personen, die selbst nicht unter Beobachtung des Verfassungsschutzes stehen und dafür auch keinen Anlass geben. Im Fall des Web-Crawlings wissen die Betroffenen womöglich selbst nicht einmal, dass ihre Daten im Internet veröffentlicht wurden. So kann es dazu kommen, dass Personen vom Verfassungsschutz gespeichert werden, weil sich aus dem Internet ein Zusammenhang zu extremistischen Personen ergibt, ohne dass die Betroffenen selbst davon wissen oder ihr eigenes Verhalten Anlass für die Annahme extremistischer Aktivitäten gibt. Gleichwohl wird die Durchforstung mit komplexen Analysemethoden zugelassen. Dieser hohen Eingriffsintensität begegnet das Gesetz nicht mit ausreichend hohen Eingriffsschwellen und anderen verfassungsmäßig gebotenen Schutzvorkehrungen wie Vorabkontrolle oder Datenverifizierung.

Des Weiteren wird mit dem neuen Gesetz die Nutzung von Daten des Verfassungsschutzes zum Training von IT-Produkten erlaubt. Hierzu ist schon grundsätzlich anzumerken, dass die zweckändernde Nutzung von mit heimlichen staatlichen Überwachungsmaßnahmen erhobenen Daten grundsätzlich verfassungsrechtlich problematisch und somit gesondert zu rechtfertigen ist. Darüber hinaus sind aber auch die im Gesetz getroffenen Schutzmaßnahmen unzureichend. So ist beispielsweise nicht ausreichend sichergestellt, dass aus den zum Training genutzten Informationen auch später noch im laufenden Betrieb Daten personenbezogen wieder ausgegeben werden, die für die jeweilige Aufgabenerfüllung nicht erforderlich sind.

Dieses Risiko wird noch dadurch verschärft, dass bereits dann Klardaten zum Training verwendet werden dürfen, wenn die Anonymisierung oder Pseudonymisierung nur mit unverhältnismäßigem Aufwand möglich ist. Solche Formulierungen bergen regelmäßig die Gefahr, dass von derartigen Ausnahmen umfassend Gebrauch gemacht wird. Bei großen Datenmengen, wie sie insbesondere zum Training von KI herangezogen werden, ist in den meisten Fällen von einem sehr hohen Aufwand auszugehen, um den Personenbezug zu entfernen. Das Anonymisierungsgebot droht deshalb zu einem Feigenblatt zu verkommen.

In der Rechtsgrundlage wird zudem nicht nach unterschiedlichen Einsatzzwecken unterschieden. Dabei ist es für die Bewertung der Eingriffsintensität der Nutzung von Daten von Bedeutung, ob ein Produkt

entwickelt wird, um allgemeine Schreiben oder Informationen sprachlich schön zu fassen oder um beispielsweise Prognoseentscheidungen hinsichtlich der Überwachungsbedürftigkeit bestimmter Gruppierungen zu erstellen. Je nach Belastungswirkung der Zwecke müssten unterschiedlich hohe Voraussetzungen für die Nutzung zu Trainingszwecken vorgesehen werden. Zwar soll der Verfassungsschutz soweit möglich Daten aus öffentlichen Quellen zum Training nutzen. Hierbei wird jedoch verkannt, dass das nicht unbedingt bedeutet, dass die dort veröffentlichen Daten rechtmäßig vorhanden sind und die betroffenen Personen diese entweder selbst veröffentlicht oder in eine Veröffentlichung eingewilligt haben. Auch die Richtigkeit der Daten ist bei veröffentlichten Daten nicht ohne Weiteres gewährleistet. Deshalb sind Schutzvorkehrungen notwendig, die dafür sorgen, dass die Verarbeitung unrichtiger personenbezogener Daten unterbleibt.

Soweit nach dem Gesetz zugleich vorgeschrieben ist, dass beim IT-Training Diskriminierungen nach Möglichkeit zu vermeiden sind, ist diese Vorgabe nicht eng genug. Zu einfach wird es danach sein zu argumentieren, dass die Diskriminierung nicht zu vermeiden war. Die Nutzung eines erkannt diskriminierenden Produkts darf gar nicht erst zugelassen werden. Dies wird durch das Gesetz jedoch gerade nicht untersagt.

Eine weitere problematische Neuerung ist die Befugnis, nach der der Verfassungsschutz (unentgeltlich!) auf Videoüberwachungsanlagen von Privaten zugreifen kann – sei es, dass er sich die Datenträger aushändigen lässt oder dass er sich technisch auf die Überwachung aufschaltet. Dies birgt die Gefahr einer nahezu flächendeckenden Beobachtung durch den Verfassungsschutz. Geschäfte, Kaufhäuser, Einkaufspassagen sowie Bahnhöfe und Flughäfen sind mittlerweile zu großen Teilen videoüberwacht. Der im Landtag geladene Sachverständige Prof. Mark A. Zöller hat dies wie folgt scharf kritisiert: „In einem Rechtsstaat vollkommen inakzeptabel ist die in § 20 VSG-E vorgeschlagene Regelung. Mithilfe dieser Bestimmung soll dem nordrhein-westfälischen Verfassungsschutz – noch dazu kostenlos und in Echtzeit – Zugriff auf alle im öffentlichen Raum vorhandenen, privaten wie öffentlichen Videokamerasysteme verschafft werden. Wie ein solcher Regelungsvorschlag in einem Gesetzentwurf einer demokratisch gewählten Landesregierung enthalten sein kann, ist aus juristischer Sicht schlicht nicht nachvollziehbar.” (Stellungnahme 18/2838, Seite 9).

Wenigstens wurde diese Neuerung im Gesetzgebungsverfahren noch etwas enger gefasst. Unter anderem muss der Verfassungsschutz die geforderten Daten nun genauer hinsichtlich Zeit und Ort eingrenzen. Es wurde außerdem eine verpflichtende Vorabkontrolle für alle Anwendungsfälle der Norm eingeführt. Dennoch bleibt die Regelung hoch problematisch, weil dadurch eine Vielzahl von Personen in die Beobachtung des Verfassungsschutzes einbezogen werden, die nur beiläufig auf den Aufnahmen erscheinen. So ist beispielsweise auch weiterhin

kritisch zu sehen, dass – trotz des entsprechenden Hinweises der LDI NRW – rechtswidrige Videoüberwachungsanlagen nicht von der Regelung ausgenommen sind.

Die LDI NRW wird genau beobachten, wie oft und in Bezug auf wie große Flächen die Regelung künftig zum Einsatz kommt. Wegen der Eingriffsintensität wäre eine gesetzliche Befristung des Einsatzes nebst Evaluierungsklausel angemessen gewesen. Auch dieser Empfehlung der LDI NRW ist das Innenministerium jedoch nicht gefolgt.

Fazit

Das Verfassungsschutzgesetz NRW hatte eine Überarbeitung dringend nötig. Strukturierung, Lesbarkeit und Transparenz haben tatsächlich eine Verbesserung erfahren. Die gleichzeitig eingebauten massiven Verschärfungen in Form neuer eingriffsintensiver Befugnisse sind dagegen verfassungsrechtlich nicht akzeptabel.

7.3. Wie sollen Behörden bei Verkehrsverstößenvorgehen? Noch immer fehlen präzise Vorgaben

Ob Blitzer-Foto oder Parkticket – viele Verkehrsteilnehmer*innen kommen im Laufe des Lebens in Kontakt mit der Ordnungsbehörde. Missachtet diese dabei den Datenschutz, kann das schwerwiegende Folgen für die Betroffenen und die Behörde selbst haben. Dabei ließen sich solche Fälle leicht vermeiden.

Das kommt immer wieder vor: Der Ordnungsbehörde flattert ein Blitzer-Foto auf den Tisch, darauf das Konterfei einer Frau. Der Halter des Autos aber ist ein Mann. Manch ein*e Behördenmitarbeiter*in verfällt in solchen Fällen schnell auf die Idee, das Blitzer-Foto bei der Passbehörde mit dem Bild der Ehefrau des Fahrzeughalters abzugleichen. Grundsätzlich ist das auch erlaubt, nur: nicht auf eine vage Vermutung hin und auch nicht ohne vorherige Anhörung des Fahrzeughalters. Denn wird diese Reihenfolge nicht eingehalten, kann die Sache schnell schief gehen. Sendet die Behörde den Anhörungsbogen nämlich gleich an die Ehefrau, ist die Frau auf dem Blitzer-Foto ihr aber nur sehr ähnlich, stehen unangenehme Fragen an den Ehemann ins Haus – und womöglich erhebliche eheliche Turbulenzen. Auch der handelnden Ordnungsbehörde droht dann schwerer Ärger.

Dabei muss es gar nicht dazu kommen. Würden den Behörden klarere Regeln für den Umgang mit dem Datenschutz an die Hand gegeben, ließen sich diese Fälle, die häufig zu Beschwerden bei der LDI NRW führen, deutlich reduzieren. Die LDI NRW hat das zuständige Innenministerium NRW bereits im Jahr 2022 darauf hingewiesen. Die Neuregelung des entsprechenden Erlasses des Ministeriums steht allerdings noch aus.

Tatsächlich konkretisiert dieser Erlass, wie die Verfolgungsbehörden bei der Ahndung von Verkehrsverstößen vorzugehen haben. Es fehlen darin allerdings präzise Angaben, etwa, in welchen Schritten und in welcher Reihenfolge die Identifizierung der in Verdacht stehenden Person erfolgen soll. Denn selbst wenn einer Verfolgungsbehörde bei der Ahndung von Verkehrsordnungswidrigkeiten umfangreiche Ermittlungsbefugnisse zur Verfügung stehen. Auch diese gehen nur so weit, wie es für die Aufgabenerfüllung erforderlich und verhältnismäßig ist. Wer eine Ordnungswidrigkeit begeht oder Zeug*in einer Ordnungswidrigkeit ist, verliert damit keineswegs seine Datenschutzrechte. Zwar konkretisiert der Erlass hier, welche Datenverarbeitung im Einzelnen bei der Bearbeitung von Ordnungswidrigkeiten erforderlich und verhältnismäßig ist. Dabei bestehen jedoch in der Anwendung bei mehreren Regelungen Unsicherheiten, wie die LDI NRW in ihrer Prüfpraxis festgestellt hat.

Ein sich wiederholender Fehler besteht darin, dass Behörden das Verwarnungsverfahren mit der Anhörung für ein Bußgeldverfahren kombinieren und dabei bereits etwaige Zeug*innen nennen. Da die Verwarnstufe dem Bußgeldverfahren vorgeht und der Vorwurf durch einfache Zahlung eines Verwarngeldes erledigt werden kann, ist hier gesetzlich keine Anhörung vorgesehen. Dementsprechend ist auch die Kenntnis der oder des Betroffenen von der Identität der Zeug*innen bzw. Anzeigeerstatter*innen zu Verteidigungszwecken – anders als im späteren Bußgeldverfahren – zu diesem Zeitpunkt noch nicht erforderlich und deshalb unzulässig (siehe hierzu 30. Bericht unter 8.6). Leider begünstigt der Erlass des Ministeriums diesen Fehler, da ihm ein widersprüchlich aufgebauter Vordruck beigefügt ist, der die Übermittlung von Namen und Wohnort der Zeug*innen zulässt. Neben dem Datenverlust, den die Zeug*innen dadurch erleiden und der Schadensersatzansprüche auslösen kann, kommt es in Einzelfällen zusätzlich zu abschreckenden Begleiterscheinungen. Mitunter suchen verärgerte, einer Ordnungswidrigkeit beschuldigte Personen Zeug*innen an ihrer Wohnadresse auf. Da die Ordnungsbehörden grundsätzlich auf die Mithilfe von Dritten angewiesen sind und dafür stellenweise sogar werben, dürfte auch aus Sicht der Behörden ein solcher Effekt unerwünscht sein.

Zudem ist den Ordnungsbehörden oftmals unklar, wie ein Lichtbildabgleich datenschutzrechtskonform zu erfolgen hat. Als eingriffsintensive Maßnahme ist darüber grundsätzlich vorab zu informieren. Betroffene erhalten so die Chance, die Ordnungswidrigkeit zuzugeben. Der Bildabgleich darf deshalb erst nach Ablauf der Anhörungsfrist der betroffenen Person durchgeführt werden. Ein vorheriges Tätigwerden widerspricht dem datenschutzrechtlichen Grundsatz der Datenminimierung bzw. Datensparsamkeit. Im eingangs geschilderten Fall hätte zunächst der Fahrzeughalter angehört werden müssen. Nur wenn er nicht bereit gewesen wäre, die Fahrerin zu benennen, hätten eingriffsintensivere Maßnahmen wie ein Lichtbildabgleich genutzt werden dürfen.

Um in der Praxis die Datenverarbeitung auf ein notwendiges Minimum zu begrenzen, für Klarheit zu sorgen und die Ordnungsbehörden als

Anwendende zu entlasten, hat die LDI NRW gegenüber dem Innenministerium angeregt, im Erlass eine regelmäßige Reihenfolge der zu nutzenden Aufklärungsmaßnahmen verbindlich vorzugeben. Dabei ist mit der Maßnahme zu beginnen, die die betroffene Person am wenigsten belastet. In der Regel ist das die Anhörung. Wenn diese nicht zum Erfolg führt, darf die nächst eingriffsintensivere Maßnahme angewendet werden und so weiter.

Das Innenministerium hatte sich bereits 2022 den Vorschlägen der LDI NRW gegenüber offen gezeigt und eine Überarbeitung des Erlasses zugesagt. Leider ist das bisher nicht umgesetzt worden. Dabei besteht Dringlichkeit. Wegen der hohen Zahl von Bußgeldverfahren wegen Verkehrsordnungswidrigkeiten ist auch das Beschwerdeaufkommen bei der LDI NRW in diesem Bereich hoch. Die Beschwerdebearbeitung der LDI NRW ist aber immer nur anlassbezogen und erreicht nur einzelne Ordnungsbehörden. Ein Erlass wirkt viel besser und flächendeckend auf ein rechtmäßiges und einheitliches Handeln aller Behörden hin. Das vermeidet nicht nur unnötige Arbeit bei der LDI NRW, sondern auch in den Behörden, die mit der Überprüfung der Beschwerde durch die LDI NRW konfrontiert sind. All das sichert schließlich die Rechte der Betroffenen am effektivsten.

Fazit

Mit einer Anpassung des Erlasses zum Vorgehen bei Verkehrsordnungswidrigkeiten und seiner Anlagen wäre sowohl der Verwaltung als auch den Bürger*innen gedient. Die Ordnungsbehörden würden entlastet, da die Anwendung in der Praxis keine Unsicherheiten mehr hervorbringen würde. Gleichzeitig würden alle Bürger*innen profitieren, die entweder als Beschuldigte oder als Anzeigenerstatter*innen mit einer Datenverarbeitung der Behörden konfrontiert sind.

7.4. Wenn Anwält*innen personenbezogene Daten Dritter in den Prozess einbringen

In zivilgerichtlichen Verfahren verarbeiten Rechtsanwält*innen regelmäßig personenbezogene Daten – oft nicht nur der eigenen Mandantschaft, sondern auch von Dritten. Die Daten erhalten sie meist von ihren Mandant*innen, die damit ihr Recht erstreiten wollen. Aber ist die Verwendung überhaupt erlaubt?

Es klingt simpel, ist es aber nicht. In Rechtsstreitigkeiten vor Gericht tragen Anwält*innen oft Informationen vor, die sie von ihren Mandant*innen bekommen haben und die deren Ansprüche untermauern sollen. Das ergibt Sinn, denn jedes Detail kann wichtig sein, um Rechte durchzusetzen. Was aber, wenn es sich bei diesen Details um personenbezogene Daten des Gegners oder Dritter handelt? Ist das ein Datenschutzproblem?

Im vergangenen Jahr hat diese Frage die LDI NRW mehrfach in Beschwerdeverfahren beschäftigt. Und die Antwort ist nicht immer leicht zu geben. Anwält*innen sollten in jedem Fall nicht leichtfertig über das Thema hinweggehen. Es kommt auf den Einzelfall an.

Grundsätzlich gilt: Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Zivilprozess durch Rechtsanwält*innen ist in der Regel Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Dieser setzt voraus, dass die Verarbeitung zur Wahrung der „berechtigten Interessen" des Verantwortlichen oder eines Dritten „erforderlich" ist, „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen". Bei besonderen Kategorien personenbezogener Daten – etwa Gesundheitsdaten – greift zusätzlich Art. 9 Abs. 2 lit. f DS-GVO, sofern die Verarbeitung „zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen" erforderlich ist.

Dabei ist recht leicht nachzuvollziehen, dass Rechtsanwält*innen ein berechtigtes Interesse an der Datenverarbeitung zugesprochen werden muss. Denn es ist Teil ihres Berufs, die vertragliche Verpflichtung mit ihrer Mandantschaft zu erfüllen, die Prozessvertretung im zivilgerichtlichen Verfahren zu übernehmen und hierzu auch vorzutragen. Rechtsanwält*innen treten im Übrigen grundsätzlich nicht im eigenen Namen auf, sondern als Vertreter*innen und im Namen ihrer Partei. Bei den Äußerungen von Rechtsanwält*innen im Prozess handelt es sich also eigentlich um den Vortrag ihrer Mandant*innen.

Ein solcher Vortrag ist grundsätzlich auch erforderlich, um den Anforderungen des Zivilprozessrechts gerecht zu werden. Ein unvollständiger Vortrag kann nämlich zur Anwaltshaftung führen, etwa wenn Rechtsanwält*innen den Vortrag der gegnerischen Partei nicht bestreiten, obwohl dies notwendig wäre, oder den Sachverhalt aus der Perspektive der Mandantschaft unzureichend darstellen. Daher sind Rechtsanwält*innen

gehalten, im Interesse ihrer Mandantschaft umfassend Informationen vor Gericht einzubringen.

Schließlich: Die berechtigten Interessen an der Ausübung des Mandats überwiegen in der Regel auch das Interesse der betroffenen Personen an der Geheimhaltung ihrer Daten. Dies gilt jedenfalls dann, wenn der Vortrag auf die Sache bezogen und damit erforderlich ist. Datenschutzrechtliche Vorschriften stehen also in der Regel nicht entgegen, denn: Der Zweck der DS-GVO soll nicht so weit gehen, dass die legitime Durchsetzung von Rechten nicht mehr möglich ist.

Das heißt aber nicht, dass es nicht auch Fallkonstellationen gibt, in denen eine Datenverarbeitung unzulässig ist. Unzulässigkeit liegt etwa dann vor, wenn Informationen ohne sachlichen Zusammenhang zum konkreten Verfahren eingebracht werden. Das ist zum Beispiel bei privaten Verhältnissen ohne Bezug zum Streitgegenstand anzunehmen. Und noch etwas ist in diesem Zusammenhang wichtig: Der Unzulässigkeit der Datenverarbeitung steht in diesen Fällen nicht entgegen, dass die weitergegebenen personenbezogenen Daten später nicht im Urteil auftauchen. Selbst wenn die Einbringung dieser Daten in den Prozess später ohne Konsequenz bleibt oder die Daten im Urteil des Gerichts keine Erwähnung finden, bedeutet dies nicht, dass der Vorgang unzulässig war. Für die Zulässigkeit kommt es allein auf die prozessuale Relevanz zum Zeitpunkt der Verarbeitung an.

Weitere Fragen entstehen in diesem Zusammenhang durch besondere Konstellationen. Was etwa gilt, wenn Rechtsanwält*innen personenbezogene Daten nicht über die Mandantschaft, sondern von anderer Stelle erlangen und in das Verfahren einbringen? In einem solchen Fall hatte ein Anwalt eine Beschwerde, die der Klagegegner gegen ihn bei der Rechtsanwaltskammer eingereicht hatte, in ein gerichtliches Verfahren eingebracht. Der Klagegegner sah hierin eine unzulässige Verarbeitung seiner Daten als Beschwerdeführer.

Die Weitergabe der personenbezogenen Daten an das Gericht – und damit mittelbar auch an die Mandantin des Anwalts – stellt in diesem Fall aber keine Datenschutzverletzung dar. Der Vortrag des Anwalts war nicht sachfremd und diente der Verteidigung der Mandantin. Er war ein geeignetes Mittel, um bestimmte Aspekte der Rechtsverteidigung zu untermauern. Zwar wurden die Daten ursprünglich für ein anderes Verfahren erhoben – nämlich für das Beschwerdeverfahren bei der Rechtsanwaltskammer. Allerdings ist eine sog. Zweckänderung nach Art. 6 Abs. 4 DS-GVO in Verbindung mit § 24 Abs. 1 Nr. 2 BDSG zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Die betroffene Person musste nach Auffassung der LDI NRW angesichts des Zusammenhangs der beiden Verfahren und der engen zeitlichen Nähe mit einer solchen Nutzung ihrer Daten rechnen (vgl. EG 47 und EG 50 zur DS-GVO).

Die Weitergabe von Daten an das Gericht zur Rechtsverteidigung kann selbst dann zulässig sein, wenn Mandant*innen personenbezogene Daten rechtswidrig erlangt haben. Erforderlich ist insofern eine sorgfältige Prüfung des konkreten Einzelfalls. Dabei muss die Frage der Rechtswidrigkeit der Datenbeschaffung zwar in die Interessensabwägung miteinfließen. Sie schließt aber nicht zwingend die Verwertung der Information im Prozess aus. Wenn beispielsweise in einem Unterhaltsprozess eine Partei Unterlagen vorlegt, die ein deutlich höheres Einkommen der anderen Partei bestätigen, als von dieser selbst angegeben wurde, spielt die Rechtmäßigkeit der Beschaffung der Unterlagen eine eher geringe Rolle. Hier kann die Partei, die ihr wahres Einkommen verschleiern wollte, sich in der Regel nicht auf Zweifel an der rechtmäßigen Datenerhebung berufen. Ihr Interesse am Verschleiern des wahren Einkommens ist nicht schützenswert.

Fazit

Anwält*innen sollten sorgfältig prüfen, ob sie personenbezogene Daten Dritter in einen Zivilprozess einbringen – sowohl zum Schutz der betroffenen Personen als auch zur Vermeidung datenschutzrechtlicher Haftungsrisiken. Denn nicht jede Einbringung ist datenschutzrechtlich zulässig. Es kommt auf den Einzelfall an.

7.5. Ehrenamtskarte – Wer ist datenschutzrechtlich verantwortlich? Einigkeit der Datenschutzkonferenz beendet Rechtsunsicherheit

Das Onlinezugangsgesetz soll den digitalen Zugang zu staatlichen Leistungen herstellen. 2024 wurden seine Regeln zum Datenschutz überarbeitet. Das kann bei IT-Projekten, die länderübergreifend Anwendung finden sollen, zu Rechtsunsicherheiten führen. Am Fall der NRW-Anwendung „Ehrenamtskarte" zeigt sich, was zu tun ist.

Nur wenige Bürger*innen kennen das Onlinezugangsgesetz (OZG) – dabei existiert es seit 2017 und ist für sie gemacht. Ob Führerschein oder ein Antrag auf Elterngeld: Die Menschen in Deutschland sollen für staatliche Leistungen künftig nicht mehr zum Amt müssen, sondern alles vom heimischen Wohnzimmer aus beantragen können – online also. Um das umzusetzen, bedarf es entsprechender IT-Anwendungen, an denen seither gearbeitet wird. Und selbstverständlich muss dabei auch geklärt sein, wie mit den jeweils verarbeiteten Daten umzugehen und wer für den rechtskonformen Umgang zuständig ist.

Mitte 2024 nun reformierte der Bundesgesetzgeber die Regeln zum Datenschutz im OZG – und das führte zu Verunsicherung. Der neue § 8a OZG legt nämlich fest, dass die datenschutzrechtliche Verantwortlichkeit für einen Online-Dienst bei derjenigen Landesbehörde liegen soll, die den Dienst betreibt, und zwar auch dann, wenn die Behörde eines anderen Bundeslandes diesen Dienst später nutzt. Wie aber ist das gemeint? Und: Wie lassen sich Konflikte zwischen den Bundesländern über die datenschutzrechtliche Verantwortung lösen? Die Beratungen der LDI NRW im vergangenen Jahr zur sog. „Ehrenamtskarte" zeigen exemplarisch, dass und wie hier Rechtssicherheit hergestellt werden kann.

Bei der „Ehrenamtskarte" geht es um eine OZG-Anwendungssoftware, die die Staatskanzlei NRW seit 2021 federführend entwickelt hatte. Die Anwendung ist seit 2023 bei vielen Kommunen in NRW im Einsatz. Berechtigte können damit über eine App eine „Ehrenamtskarte" beantragen, um unter anderem gewisse Vergünstigungen bei lokalen Einrichtungen wie Schwimmbädern oder Theatern zu erhalten. Dies soll das ehrenamtliche Engagement honorieren. Die Anwendung soll zudem den für die Vergabe der „Ehrenamtskarte" zuständigen Stellen als Plattform dienen, damit diese mit den Antragsteller*innen und Karteninhaber*innen in Kontakt treten können. Die Bürger*innen können sich registrieren und wählen dann aus einem Menu die für sie zuständige Stelle aus. Anschließend werden sie zum „Antragsservice" weitergeleitet. Dieser besteht aus der Benutzeroberfläche, welche die Bürger*innen etwa für Eingaben und Abrufe nutzen. Hiermit verbunden ist zudem das Verwaltungsprogramm, das die zuständigen Stellen zur Mitgestaltung der Benutzeroberfläche und teilweisen Abwicklung des Bewilligungsverfahrens verwenden. Dementsprechend sah das Konzept der Staatskanzlei vor, die Verantwortlichkeit aufzuteilen zwischen dem Land NRW als Plattformbetreiber und den zuständigen Stellen für die Antragsbearbeitung.

Nun gilt beim OZG zwischen den Bundesländern das sog. „Einer-für-Alle"-Prinzip (kurz: „EfA"-Prinzip). Danach soll die von einem Land entwickelte Software auch von anderen Bundesländern nachgenutzt werden können. Deshalb gründete die Staatskanzlei NRW für die „Ehrenamtskarte" eine Nachnutzungsallianz mit Vertreter*innen interessierter Länder. Die Datenschutzaufsichtsbehörde eines anderen Bundeslandes äußerte dort jedoch Bedenken zum Datenschutzkonzept aus NRW, konkret zur Verteilung der datenschutzrechtlichen Verantwortlichkeit, weil diese nicht dem neu eingeführten § 8a OZG entspreche. Die Staatskanzlei bat die LDI NRW dazu um Beratung.

Zunächst: Sofern Rechtsunsicherheit besteht, ob der neu eingeführte § 8a OZG auch IT-Verfahren betrifft, die wie die „Ehrenamtskarte" vor seiner Einführung schon in der Entstehung waren, gilt: Das reformierte OZG enthält keine Übergangsregelung für ältere IT-Verfahren. Insoweit findet § 8a OZG eindeutig Anwendung.

Für die Lösung des „Länderkonflikts" war derweil Fingerspitzengefühl erforderlich. Das Datenschutzkonzept der Staatskanzlei NRW erkannte den länderübergreifenden Onlinedienst vor allem in den Plattformfunktionalitäten, also zum Beispiel bei der Registrierung in der mobilen Anwendung. Die Datenschutzaufsichtsbehörde des an der Nachnutzung interessierten Bundeslands war dagegen der Meinung, dass die gesamte Anwendung „Ehrenamtskarte" ein länderübergreifender Onlinedienst sei. Damit hätte § 8a OZG eine Verantwortung der Staatskanzlei NRW für das gesamte Verfahren verlangt. Entscheidend kam es also darauf an, in welchem konkreten Umfang es sich bei dem Verfahren „Ehrenamtskarte" um einen länderübergreifenden Onlinedienst handelt.

Um das zu klären, beteiligte die LDI NRW im März 2025 die entsprechenden Fachgremien aller Datenschutzaufsichtsbehörden über die Datenschutzkonferenz (DSK). Dort wurde nach Bewertung des Verfahrens übereinstimmend festgestellt, dass die Anwendung „Ehrenamtskarte" kein einheitliches Produkt ist, sondern technisch aus zwei Elementen besteht: zum einen der „App", die die Online-Benutzeroberfläche gegenüber den Bürger*innen bildet. Zum anderen gibt es ein „Verwaltungsprogramm", das der Behörde als Fachverfahren zur Verfügung steht, die den Antrag für die Ehrenamtskarte bearbeitet.

Auf der Basis dieser Bewertung nahm die Staatskanzlei NRW deshalb Mitte Juli 2025 eine Anpassung der Verteilung der datenschutzrechtlichen Verantwortlichkeiten vor. Dabei war sie bereit, nicht mehr nur die Plattformfunktionalitäten, sondern alle Aspekte der „App" als länderübergreifenden Onlinedienst gemäß § 8a OZG einzustufen, während das Verwaltungsprogramm dem Verantwortungsbereich der für die Antragsbearbeitung zuständigen Stelle zugeordnet wird. Diese Neubewertung wurde von der Staatskanzlei dokumentiert und steht den nachnutzenden Behörden seither zur Verfügung.

Die Rückmeldungen aus der Nachnutzungsallianz waren positiv. Die Ergebnisse der Diskussion in den DSK-Fachgremien flossen darüber hinaus in die „Orientierungshilfe zu ausgewählten Fragestellungen des Onlinezugangsgesetzes" aus Dezember 2025 ein. Außerdem stellt die DSK mittlerweile ein Dokument zur Verfügung, an dem sich diejenigen orientieren können, die einen zur Nachnutzung vorgesehenen Onlinedienst programmieren („Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz", Stand: Dezember 2025). Die dortigen Hinweise sollen erreichen, dass relevante Datenschutzaspekte bei der Konzeption von vorherein und laufend mitgedacht werden.

Fazit

Der von der LDI zum Verfahren „Ehrenamtskarte" angestoßene Beratungsprozess und die genannten Hilfestellungen der DSK zeigen, dass die Datenschutzaufsichten in Deutschland den Digitalisierungsprozess konstruktiv begleiten und in wichtigen Fragen Einigkeit herstellen.

7.6. Tonbandmitschnitte von Ratssitzungen – nicht jede Verwendung ist erlaubt

Eine „berüchtigte Sondersitzung" – so betitelte die Presse im vergangenen Jahr die Sitzung eines Stadtrats, bei der es offenbar hoch herging. Wer hätte da im Nachgang nicht gerne die Wortbeiträge der Teilnehmenden gelesen? Theoretisch wäre das möglich gewesen. Tatsächlich sprach in diesem Fall etwas Gewichtiges dagegen.

Eigentlich Routine: In vielen Kommunen ist es inzwischen üblich, Ratssitzungen auf Tonband aufzuzeichnen. Das hat einen so einfachen wie praktischen Grund. Die Mitschnitte werden genutzt, um gemäß § 52 der Gemeindeordnung NRW (GO NRW) die wesentlichen Inhalte der gefassten Beschlüsse in Niederschriften festzuhalten und diese dann der Öffentlichkeit zugänglich zu machen.

Grundsätzlich sind solche Mitschnitte zulässig. Allerdings muss sichergestellt werden, dass die Rechte der Ratsmitglieder und von anderen teilnehmenden Personen gewahrt werden. Die Ratsmitglieder, die in der Regel Politik nicht professionell betreiben, sollen ihre Aufgaben in den Sitzungen unbefangen wahrnehmen und offen sprechen können. Sie sollen ebenso wie andere Teilnehmende nicht befürchten müssen, dass im Nachhinein jedes Wort auf die Goldwaage gelegt wird. Durch Tonbandaufzeichnungen wird in diese Rechte eingegriffen; dieser Eingriff muss so gering wie möglich sein. Insbesondere müssen die Ratsmitglieder vor der Aufzeichnung wissen, wenn jedes einzelne Wort ihrer Redebeiträge im Detail protokolliert werden soll.

In einem Fall, der die LDI NRW 2025 beschäftigte, ging es um dieses Spanungsfeld von Sitzungspraxis und Teilnehmenden-Rechten. Die Angelegenheit wurde sogar öffentlich publik, als die Presse die Sitzung „hochemotional" nannte und als „berüchtigte Sondersitzung" bekannt machte.

Konkret erlaubte die Geschäftsordnung des betreffenden Stadtrates den Tonbandmitschnitt der Sitzung, um auf dieser Grundlage ein Ergebnisprotokoll zu erstellen. Festgehalten war in der Geschäftsordnung jedoch auch, den Mitschnitt zu löschen, falls in der auf die Zuleitung der Niederschrift folgenden Ratssitzung kein Wunsch zur Änderung des Protokolls geäußert wurde. Zur Löschung kam es jedoch zunächst nicht. Zwar wurden in der Folgesitzung im Rat keine Einwände gegen das vorgelegte Ergebnisprotokoll erhoben. Der Rat beschloss aber mehrheitlich, dass es – entgegen der Regelung in der Geschäftsordnung – ergänzend eine vollständige Abschrift der Tonbandaufnahme in Form eines Wortprotokolls geben sollte. Von der Löschung des Tonbands wurde bis auf Weiteres abgesehen.

Dieses Vorhaben führte zu mehreren Datenschutzbeschwerden, vor allem von Teilnehmenden der Sitzung, die sich darauf verlassen hatten,

in der Sitzung offen sprechen zu können und nicht mit einer Veröffentlichung ihrer Wortbeiträge rechnen zu müssen. Die LDI NRW gab den Beschwerdeführer*innen letztendlich Recht.

Zunächst: Tonbandaufzeichnungen von Ratssitzungen sind nur zulässig, soweit sie zur Aufgabenerfüllung des Rates erforderlich sind (§ 3 DSG NRW). Die genaue Ausgestaltung der Vorgaben obliegt dabei allerdings den Kommunen, weil die GO NRW nur Mindestanforderungen an die Protokolle von Ratssitzungen aufstellt. Ihre genaue Form (Ergebnis-, Verlaufs- oder Wortlautprotokoll) wird von einem Großteil der Kommunen in der jeweiligen Geschäftsordnung festgelegt, die der Rat beschließt. Die Geschäftsordnung regelt dann, ob Tonbandmitschnitte grundsätzlich erlaubt sind und wenn ja, für welche Art von Protokollen sie genutzt werden dürfen.

Durch diese Festlegung ist zugleich für alle Ratsmitglieder und sonstigen teilnehmenden Personen bereits im Vorhinein klar erkennbar, worauf sie sich einzustellen haben. Spätestens nach Erstellung der Niederschrift in der zuvor festgelegten Form und anschließender Genehmigung durch den Rat sind die Tonbandmitschnitte unverzüglich zu löschen, weil diese Daten sodann nicht mehr zur Aufgabenerfüllung des Rates erforderlich sind.

Im Fall der „berüchtigten Sondersitzung" reichte jedoch der nachträgliche Ratsbeschluss zur Erstellung eines Wortlautprotokolls nicht aus, um die Nutzung des Tonbandmitschnitts zu rechtfertigen. Der Beschluss stellte keine ausreichende Rechtsgrundlage für die hiermit verbundene Verarbeitung der personenbezogenen Daten dar. Er konnte auch nicht zu einer rückwirkenden Änderung der Geschäftsordnung führen.

Die Verarbeitung personenbezogener Daten zu anderen Zwecken als denjenigen, zu denen die Daten erhoben worden sind, ist nur unter bestimmten Voraussetzungen möglich. In NRW sind diese in § 9 Abs. 2 DSG NRW festgelegt. Die Anforderungen an eine solche Zweckänderung sind hoch, weil die betroffenen Personen grundsätzlich auf die jeweilige Rechtslage vertrauen dürfen und nicht davon ausgehen müssen, dass ihre Daten für einen anderen Zweck als den, der ihnen bekannt war, genutzt werden. Gründe, die eine solche Zweckänderung im Fall der konkreten Ratssitzung gerechtfertigt hätten, wurden weder vorgetragen noch waren sie ansonsten ersichtlich. Die angestrebte Zweckänderung war daher nicht zulässig, so dass der Tonbandmitschnitt nicht für die Erstellung eines Wortprotokolls genutzt werden durfte.

Die LDI NRW als Datenschutzaufsicht und die Bezirksregierung als Kommunalaufsicht waren hier einer Meinung. Die Stadt verzichtete schließlich auf die Erstellung eines Wortprotokolls und löschte die Tonbandaufnahme. Die einzelnen Äußerungen, die zu einer „hochemotionalen" Ratssitzung geführt haben sollen, blieben am Ende undokumentiert.

Fazit

Jede Verarbeitung personenbezogener Daten erfolgt zu einem bestimmten Zweck – und ist nur dann zulässig, wenn eine Rechtsgrundlage sie erlaubt. Ändert sich der Zweck, bedarf es auch einer eigenen Rechtsgrundlage für die Verarbeitung zu diesem neuen Zweck. Ein nachträglich gefasster Ratsbeschluss kann die Rechtslage nicht nachträglich zu Lasten der betroffenen Personen ändern.

7.7. Meldedaten-Abrufe nur aus dienstlichen Gründen zulässig – Das müssen die Kommunen veranlassen

Kommunale Beschäftigte müssen und dürfen für viele dienstliche Aufgaben die Meldedaten von Bürger*innen abrufen. Manchmal greifen Bedienstete aber auch aus rein privaten Interessen auf die Daten zu. Die Kommunen müssen dafür sorgen, dass so etwas nicht passiert. Die LDI NRW hat sie dazu beraten.

Mal eben schauen, wo die Exfreundin jetzt wohnt? Oder recherchieren, wann der Kollege Geburtstag hat? Solche Abfragen von Meldedaten sind den Beschäftigten in Behörden verboten. Erlaubt hingegen ist ihnen ein Abruf, wenn er zur Erfüllung ihrer eigenen dienstlichen Aufgaben erforderlich ist. Doch so klar die Regeln auch sind: immer wieder wird gegen sie verstoßen. Mal denken sich Beschäftigte nichts dabei, wenn sie auch ohne einen dienstlichen Grund auf Meldedaten zugreifen. Andere sind sich zwar bewusst, dass sie unzulässig handeln, gehen aber davon aus, dass sie schon nicht erwischt werden.

Kommunen dürfen solche unzulässigen Datenzugriffe nicht hinnehmen – und sie können sie auch durch einfach umzusetzende Maßnahmen weitgehend stoppen. In der Aufsichtspraxis der LDI NRW ist aufgefallen, dass es hier an manchen Stellen noch hakt. Die LDI NRW hat deshalb im vergangenen Jahr den Kommunen erläutert, wie die erforderlichen Maßnahmen aussehen sollten, die unberechtigte Zugriffe verhindern oder zumindest minimieren.

Schritt Nummer eins ist ein sog. Rollenkonzept. Das dient dazu festzuschreiben, wer in welchem Umfang überhaupt Meldedaten abrufen darf. In einer Dienstanweisung legt die Behörde dann für die Beschäftigten nachvollziehbar fest, unter welchen Umständen die Meldedaten abgerufen werden dürfen. Damit die Berechtigung des Abrufs nachgeprüft werden kann, soll die Dienstanweisung vorsehen, dass bei jedem Abruf das Aktenzeichen des Vorgangs anzugeben ist, für den der Abruf erfolgt ist. Wenn Beschäftigte einen elektronischen Zugang zum Melderegister erhalten, sind sie auf die Einhaltung dieser Regeln zu verpflichten. Außerdem muss an die Dienstanweisung regelmäßig erinnert werden, damit sie nicht in Vergessenheit gerät.

Diese Maßnahmen allein reichen aber noch nicht aus. Die Kommune muss die Abrufe auch kontrollieren. Dies ist ohne weiteres möglich, da jeder Abruf der Meldedaten protokolliert und für zwölf Monate aufbewahrt wird. Anhand dieser Protokolldaten ist mindestens einmal monatlich stichprobenhaft zu überprüfen, ob sich die Beschäftigten an die Regeln halten. Denn gänzlich unkontrolliert gäbe es keine Hemmschwelle für unberechtigte Zugriffe.

Fazit:

Mit behördeninternen Regelungen und regelmäßigen Datenschutzkontrollen lassen sich unzulässige Abrufe der Meldedaten durch kommunale Beschäftigte weitgehend vermeiden. Das hat die LDI NRW gegenüber den Meldebehörden aus gegebenem Anlass noch einmal in Erinnerung gerufen.

7.8. Die Dokumentation und Untersuchung von Antisemitismus in Deutschland sind datenschutzkonform möglich

Ein Netzwerk von Recherche- und Informationsstellen (RIAS) befasst sich in Deutschland mit der Dokumentation und Untersuchung von antisemitischen Vorfällen. Das ist auch datenschutzrechtlich eine Herausforderung. Die LDI NRW hat die Meldestelle dazu beraten – und ein Ergebnis erzielt, das Vorbild für andere Länder sein könnte.

Die Antisemitismusbekämpfung ist in Deutschland seit jeher ein zentrales Anliegen. Daher wurde vor Jahren damit begonnen, ein bundesweites Meldesystem zur Erfassung antisemitischer Vorfälle zu schaffen, insbesondere auch von Fällen unterhalb der Strafbarkeitsschwelle. 2018 entstand der Bundesverband Recherche- und Informationsstellen Antisemitismus, außerdem führten viele Bundesländer entsprechende Meldestellen ein. Auch in NRW existiert eine solche Einrichtung.

RIAS NRW hat seine Tätigkeit im April 2022 aufgenommen und wird durch das Ministerium für Kinder, Jugend, Familie, Gleichstellung, Flucht und Integration des Landes NRW gefördert. Der Trägerverein von RIAS NRW ist der Verein für Aufklärung und demokratische Bildung e. V., Düsseldorf. Da bei seiner Arbeit, insbesondere dem Umgang mit den entsprechenden Vorfallsmeldungen, auch Datenschutzfragen eine große Rolle spielen, hat die LDI NRW dazu beraten. Das Ergebnis: Die wichtige Tätigkeit der Meldestellen ist datenschutzkonform gestaltbar, sofern einige Regeln eingehalten werden.

Wesentliches Instrument der Informationsgewinnung der Meldestellen ist das Meldeportal **www.report-antisemitism.de**, in dem Hinweise zu antisemitischen Vorfällen gegeben werden können, die anschließend Eingang in eine Datenbank finden. Ziel ist, bundesweit eine einheitliche zivilgesellschaftliche Erfassung und Dokumentation zu gewährleisten. Hierzu gehören die Entgegennahme von Meldungen über antisemitische Vorfälle und die Unterstützung von Betroffenen. Die örtlichen Ansprechpartner*innen bieten Betroffenen zudem eine Erstberatung zum Umgang mit dem Erlebten an und verweisen diese bei Bedarf an zivilgesellschaftliche und staatliche fachspezifische Beratungs- und Beschwerdestellen sowie Anwält*innen. Weitere zentrale Aufgaben von RIAS sind die Aufklärungs- und Öffentlichkeitsarbeit sowie die Erstellung von Jahresberichten zu den jeweiligen Vorfällen in Deutschland. In die Datenbank, die auf den Meldungen aufbaut, werden nur Fälle übernommen, die anhand der Qualitätsmaßstäbe eindeutig als antisemitisch qualifiziert wurden.

Aus datenschutzrechtlicher Sicht ist dabei vor allem Folgendes wichtig:

Die Datenübernahme geschieht weitgehend anonymisiert. Eine vollständige Anonymisierung ist allenfalls in Ausnahmefällen nicht möglich. Meist betrifft das Fälle, über die auch die Presse schon berichtet hat. Meldungen können unter Angabe einer gültigen E-Mail-Adresse eingereicht werden. Weitere personenbezogene Daten sind nicht erforderlich.

Das Meldeformular enthält zudem gezielte Hinweise, die sicherstellen sollen, dass eine Identifizierung der Person nicht möglich ist, die den antisemitischen Vorfall initiiert hat. Erfolgen durch die meldende Person dennoch Hinweise, tragen die Meldestellen für eine weitergehende Anonymisierung der Person Sorge. Nach Übernahme der Meldungen in die Datenbank werden die initialen Meldedaten bei den örtlichen Meldestellen gelöscht.

Als Rechtsgrundlage für die Datenverarbeitung ist aus Sicht der LDI NRW Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO einschlägig. Derjenige, der erforderliche personenbezogene Daten für einen legitimen Zweck verarbeitet, muss ein berechtigtes Interesse daran haben. Außerdem darf dieses Interesse nicht von dem Interesse der betroffenen Person und deren Grundrechten und Grundfreiheiten überwogen werden.

Im Fall von RIAS stellt die abstrakte Lageberichterstattung über antisemitische Vorfälle auf einem wissenschaftlich abgesicherten Niveau ein berechtigtes Interesse der eingerichteten Meldestellen dar. Diesem stehen zwar die Interessen von meldenden Personen und gegebenenfalls identifizierbaren Personen, die den Vorfall angeblich oder tatsächlich verursacht haben, gegenüber. Diesen Interessen wird jedoch durch wesentliche Schritte für eine weitgehend anonyme Meldung im Hinblick auf die Verursacher*innen und einen interessensensiblen Umgang mit den

Daten der Meldenden Rechnung getragen. Soweit im Einzelfall Ereignisse personenbeziehbar sind, sind notwendige Schutzvorkehrungen getroffen, die diese Personenbeziehbarkeit wieder aufheben sollen.

Außerdem hat die LDI NRW auf eine deutlich kürzere Speicherung von Daten hingewirkt. RIAS NRW hat nunmehr ein differenziertes und am Maßstab der Erforderlichkeit bemessenes Prüf- und Löschkonzept geschaffen.

Die LDI NRW hat alle Datenschutzaufsichtsbehörden des Bundes und der Länder über das dargestellte Prüfergebnis unterrichtet. Ziel ist es, dass die Prüfungsergebnisse auch bundesweit Akzeptanz erhalten. Im kommenden Jahr werden dazu noch Gespräche mit den Kolleg*innen in anderen betroffenen Ländern und RIAS geführt.

Fazit

RIAS NRW leistet einen wichtigen Beitrag zum Vorgehen gegen Antisemitismus in NRW. Die Meldestelle macht Antisemitismus sichtbar, indem sie antisemitische Vorfälle veröffentlicht und Jahresberichte verfasst. Diese wichtige Tätigkeit ist datenschutzkonform gestaltbar.

8. Gesundheit und Soziales

8.1. BGH bestätigt LDI NRW im Streit mit Apotheken – Online-Verkauf geht nur mit strengem Schutz der Besteller*innen-Daten

Bei einer Überprüfung von Apotheken hatte die LDI NRW darauf gedrängt, dass auch beim Online-Verkauf von apothekenpflichtigen Medikamenten stets vorher die Einwilligung der Besteller*innen in die Nutzung ihrer Daten eingeholt wird. Der BGH hat diese Beratungspraxis der LDI NRW bestätigt.

Apotheken sind eine der größten Anlaufstellen für Personen mit gesundheitlichen Fragen und Problemen. Bei ihnen stehen tagtäglich sensibelste persönliche Informationen im Mittelpunkt. Bereits 2019 wollte die LDI NRW deshalb wissen, wie diese Branche mit den ihnen anvertrauten Gesundheitsdaten umgeht. Bei zwölf Apotheken in NRW wurde exemplarisch eine Initiativprüfung durchgeführt.

Dabei zeigte sich ein Problem ganz deutlich: Alle zwölf Apotheken holten offenbar bei den Arznei-Besteller*innen keine Einwilligungen für das Bewerben und den Vertrieb von apothekenpflichtigen Medikamenten über eine Online-Verkaufsplattform ein. Das ist aber erforderlich, weil auch beim Erwerb apothekenpflichtiger Arzneien Rückschlüsse auf Gesundheitsinformationen über die Kund*innen möglich sind. In einem länger währenden Rechtsstreit wurden nun 2025 sowohl die Apotheken als auch der Betreiber der Verkaufsplattform zur Einsicht gebracht. Sie haben ihre Systeme entsprechend umgestellt.

Grundsätzlich gilt, dass Art. 9 DS-GVO ein generelles Verbot der Verarbeitung von sensiblen Gesundheitsdaten festlegt. Dieses Verbot kennt

nur die in der Vorschrift selbst genannten engen Ausnahmen. Mit Blick auf die Apotheken sowie den Online-Vertrieb kommt danach nur eine mögliche Ausnahme in Betracht: und zwar die Einwilligung der Betroffenen nach Art. 9 Abs. 2 lit. a DS-GVO.

Zehn der von der LDI NRW überprüften Apotheken gingen dagegen davon aus, dass beim Verkauf nicht verschreibungspflichtiger Arzneimittel Gesundheitsdaten gar nicht verarbeitet würden und sie deshalb keine Einwilligungserklärungen der Besteller*innen einholen müssten. Teils äußerten sie die Auffassung, dass gar nicht klar sei, ob die bestellende Person das Medikament für sich oder eine andere Person kaufen möchte. Anders als bei verschreibungspflichtigen Medikamenten könne daher aus der Bestellung nicht auf den Gesundheitszustand der Person geschlossen werden, die ein Medikament bestellt. Zudem war der Betreiber der Online-Plattform, über die der Verkauf erfolgte, nicht bereit, eine Einwilligungserklärung in den Bestellprozess einzubauen.

Die geprüften Apotheken hatten wegen einer laufenden gerichtlichen Klärung ihren Verkauf über die Plattform immerhin zunächst eingestellt. Der BGH entschied schließlich (Urteil vom 27. März 2025, Az. ZR 222/19) auf der Grundlage der Vorabentscheidung des EuGH (Urteil vom 4. Oktober 2024, Az. C-21/23) so, wie die LDI NRW es zuvor auch schon bewertet hatte. Auch beim Vertrieb apothekenpflichtiger Arzneimittel über eine Online-Verkaufsplattform handelt es sich danach bei den Daten, die Kund*innen bei der Onlinebestellung von Arzneimitteln eingeben müssen (wie etwa Name und Lieferadresse) in Kombination mit den bestellten Arzneien um Gesundheitsdaten des Art. 9 DS-GVO. Dies gilt im Übrigen auch dann, wenn der Verkauf dieser Arzneimittel keiner ärztlichen Verschreibung bedarf. Auch nicht verschreibungspflichtige Arzneimittel dürfen also auf Online-Verkaufsplattformen nur mit Besteller*innen-Einwilligung verkauft werden.

Der EuGH hatte zuvor bereits den Einwand der Apotheken verworfen, dass die Bestellung nicht verschreibungspflichtiger Arzneien keinen unmittelbaren Rückschluss auf den Gesundheitszustand der bestellenden Person erlaube. Nach der Entscheidung des EuGH ist es wegen des hohen Schutzniveaus, das die DS-GVO gewährleistet, ausreichend, wenn aufgrund der Indikationen zu dem Medikament Rückschlüsse auf den Gesundheitszustand einer identifizierten oder identifizierbaren Person mittelbar möglich sind. Es sei unerheblich, ob es sich dabei um die das Medikament bestellende oder eine andere mittelbar identifizierbare Person handele. Der EuGH ließ die Möglichkeit solcher Rückschlüsse auf den Gesundheitszustand einzelner Personen ausreichen, um die Daten als Daten gemäß Art. 9 DS-GVO zu qualifizieren.

Die von der LDI NRW geprüften Apotheken konnten allerdings trotz der Gerichtsentscheidungen den Verkauf über die Online-Plattform wieder aufnehmen. Denn der Betreiber der Plattform hatte zwischenzeitlich die erforderlichen technischen Anpassungen vorgenommen, die nun das

Einholen einer ausdrücklichen Einwilligung ermöglichen. Der Verkauf über die Online-Verkaufsplattform ist deshalb datenschutzrechtlich nicht mehr zu beanstanden.

Fazit

Die Initiativprüfung der LDI NRW hat gezeigt, dass die datenschutzrechtlichen Anforderungen beim Online-Verkauf apothekenpflichtiger Arzneimittel nicht durchgängig beachtet wurden. Durch die Anpassungen wurde im digitalen Verkaufsprozess der Apotheken eine deutliche Verbesserung des Schutzes von Gesundheitsdaten erreicht. der an der Gesetzgebung beteiligten Organe, die in diesem Zusammenhang auf die Beratung der LDI NRW zurückgreifen können.

8.2. Wenn das Pflegepersonal Influencer spielt – Patient*innendaten haben im Netz nichts zu suchen

Mehrfach sind in NRW Pfleger*innen aufgefallen, die Pflegebedürftige durch Reels oder Livestreams im Internet zur Schau gestellt haben. Das ist nicht nur ein Vertrauensbruch, sondern regelmäßig auch ein Datenschutzverstoß. Und der kann finanzielle Folgen haben.

Bilder schrecklicher Krankheiten, schlecht gemachte Dokumentationen des Arbeitsalltags oder Livestreams am Patientenbett: Mitarbeitende von Pflegeeinrichtungen teilen immer häufiger Eindrücke und Erfahrungen aus ihrem Job auf Social-Media-Plattformen. Das Spektrum ist dabei ebenso breit gefächert wie die Motive, die dahinterstecken. Manche Pflegekräfte wollen schlicht Krankheitsbilder oder erkrankte Körperteile zur Schau stellen. Andere möchten Aufmerksamkeit für ihren Berufsalltag erzeugen, eine dritte Gruppe wiederum berichtet über genau solche Veröffentlichungen – und verstärkt damit das Problem. In den meisten Fällen begehen die Betreuungskräfte damit nicht nur arbeitsrechtliche Pflichtverletzungen. Sie verstoßen auch gegen den Datenschutz. Solche Veröffentlichungen von Patient*innendaten sind allenfalls dann zulässig, wenn die Betroffenen einwilligen. Das aber ist ihnen je nach Krankheitsbild gar nicht möglich, da viele Erkrankungen schon die Einwilligungsfähigkeit ausschließen.

Die LDI NRW hat 2025 mehrere solcher Vorgänge überprüft. Pflegekräfte hatten Videos während ihrer Arbeit erstellt und anschließend oder live auf Social-Media-Plattformen geteilt. In einem Fall wurden von Personen, die den Bundesfreiwilligendienst ableisteten, Patient*innenvideos und -fotos über die App Snapchat verbreitet. Daneben kam es immer wieder zu

Livestreams von Situationen des Pflegealltags durch Einzelpersonen, die ihre Arbeit und sich im Internet präsentierten. Oder mehrere Pflegekräfte einer Station posteten Filme und verbrachten so die Pause während ihrer Nachtschicht virtuell mit ihren Follower*innen. Eine weitere Pflegekraft teilte regelmäßig Videos, in denen schwer erkrankte Körper zu sehen waren, und präsentierte als Kontrast hierzu in anderen Videos ihr eigenes Leben.

Datenschutzrechtlich sind all diese Beispiele hoch problematisch. Werden Personen oder personenbezogene Daten in Videos oder Livestreams gezeigt, handelt es sich dabei um eine Datenverarbeitung. Diese bedarf grundsätzlich einer Rechtsgrundlage, wie aus Art. 6 Abs. 1 DS-GVO hervorgeht. Sind Gesundheitsdaten im Spiel, ist deren Verarbeitung in solchen Fällen sogar nur durch ausdrückliche Einwilligung der betroffenen Person zulässig. Denn grundsätzlich untersagt die DS-GVO die Verarbeitung von Gesundheitsdaten aufgrund ihrer Sensibilität.

Umso schwerer wiegt deshalb, wenn diese Daten von Personen veröffentlicht werden, denen sowohl Patient*innen als auch deren Angehörige grundsätzlich besonders vertrauen. Da wiegt es besonders schwer, wenn genau diese Pflegekräfte die besonders geschützten und sensiblen Gesundheitsdaten in Soziale Netzwerken einem unbegrenzten Kreis unbefugter Dritter offenbaren. Die Folgen für die Betroffenen können ganz erheblich sein.

Für die LDI NRW ist dies Grund, in der Pflege Tätige eindringlich zu warnen. In keinem der geprüften Fälle war das Vorgehen rechtlich zulässig. Die betroffenen Personen hatten keine Einwilligung gegeben, in einem Video oder gar einem Livestream zu erscheinen. Die Aufnahmen und Veröffentlichungen erfolgten ohne Wissen der Betroffenen. Patient*innendaten haben in solchen Fällen nichts im Netz zu suchen. Solche Rechtsverstöße können empfindliche Geldbußen nach sich ziehen. Die Betroffenen können darüber hinaus Schadensersatzansprüche geltend machen.

Fazit

Pflegebedürftige Personen sind besonders schutzbedürftig. Pflegekräften sollte daher bewusst sein, dass sie eine hohe Verantwortung tragen und ihnen großes Vertrauen entgegengebracht wird. Das sollte nicht durch unüberlegte Veröffentlichungen von Daten ihrer Patient*innen aufs Spiel gesetzt werden, um Reichweite in sozialen Netzwerken zu erzielen.

8.3. Brustvergrößerungssimulation: Schönheitschirurg zeigt Bilder von Patientin auf Instagram

Er wollte seine neue Technik bewerben: Also nutzte ein Operateur ohne Wissen seiner Patientin deren Bilder, um in den Sozialen Medien darzustellen, wie ihr entblößter Oberkörper nach einer Brustvergrößerung aussehen könnte. Besonders pikant: Versehentlich war sogar der Name der Frau lesbar. Der LDI NRW blieb deshalb datenschutzrechtlich keine Wahl.

Eine Instagram-Story mit Folgen: Im Rahmen einer Beschwerde musste sich die LDI NRW mit einem für die Betroffene besonders belastenden Datenschutzverstoß befassen. Die Frau hat sich in eine Arztpraxis begeben, um sich wegen der Möglichkeit einer Brustvergrößerung beraten zu lassen. Im Rahmen des ärztlichen Beratungsgesprächs fertigte die Praxis mit Einverständnis der Betroffenen Bilder ihres entblößten Brustbereichs an, um ihr mit neu in der Praxis verfügbarer Technik das künftige Erscheinungsbild der operierten Brust präsentieren zu können.

Was dann kam, war allerdings nicht abgesprochen. Ohne Wissen und Einwilligung der Frau veröffentlichte die Arztpraxis nur einen Tag später auf ihrem Instagram-Account eines der angefertigten Bilder, um für die neue Technik zu werben. Und nicht nur das: Das Bild zeigte neben dem auf dem abfotografierten Monitor der Praxis erkennbaren möglichen Operationsergebnis versehentlich auch noch den im Bildausschnitt lesbaren Klarnamen der Patientin.

Diese reagierte zwar schnell und machte die Praxis umgehend auf den Vorfall aufmerksam. Die „Story" auf Instagram wurde daraufhin entfernt. Bis dahin war sie jedoch bereits zehn Stunden über den Instagram-Account der Praxis mit ihren mehreren tausend Followern abrufbar gewesen. Für die LDI NRW war die Rechtslage damit eindeutig: Der Beauty-Praxis hatte einen erheblichen Datenschutzverstoß begangen.

Denn: Personenbezogene Daten sind von demjenigen, der sie verarbeitet, auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise zu behandeln. Auch dürfen sie nicht in einer mit dem Zweck der Erhebung nicht zu vereinbarenden Weise weiterverarbeitet werden. Mit der veröffentlichten Instagram-Story offenbarte die verantwortliche Praxis jedoch ohne erforderliche Einwilligung der Betroffenen und damit ohne datenschutzrechtliche Rechtsgrundlage zweckwidrig äußerst sensible Daten, die die Intimsphäre und damit den Kernbereich des Persönlichkeitsrechts der Betroffenen betreffen. Zwar leistete der Verantwortliche im konkreten Fall zivilrechtlich Schadenersatz an die Patientin und gab ihr gegenüber eine strafbewährte Unterlassungserklärung ab. Datenschutzrechtlich war der Fall für die LDI NRW damit aber noch nicht abgeschlossen. Dazu wog der Verstoß

auch angesichts des mit der Veröffentlichung verfolgten rein werblichen Ziels und der großen Zahl an Followern und der damit anzunehmenden Reichweite auf Instagram zu schwer. Die LDI NRW hat mittlerweile ein Bußgeldverfahren gegen die Praxis eingeleitet.

Fazit

Bei der Veröffentlichung von Patient*innendaten in Sozialen Medien ist datenschutzrechtlich äußerste Sorgfalt und Zurückhaltung geboten. Erfolgt sie zu Werbezwecken und ohne Einwilligung, ist sie datenschutzrechtlich unzulässig. Auch fahrlässige Datenschutzverstöße kann die LDI NRW mit Bußgeldern ahnden.

8.4. Therapeutin wirbt auf Social-Media – Daten von Patient*innen gehören dort nicht hin

Nutzen Gesundheitspraxen Instagram und Co., um über ihre ärztliche oder psychotherapeutische Arbeit zu informieren, ist besondere Vorsicht geboten. Das zeigt der Fall einer Psychotherapeutin, die auf Instagram die Bewilligung eines Therapieantrages veröffentlichte – und dabei etwas Wesentliches falsch machte.

Ärzt*innen und Therapeut*innen gehen mit der Zeit. Immer mehr Gesundheitspraxen setzen einen Social-Media-Account ein, um auf sich aufmerksam zu machen. Oft wird mit kleinen Textbeiträgen, Fotos und Videos aus dem Praxisalltag berichtet oder über allgemeine Gesundheitsthemen informiert. Doch neben berufsrechtlichen Vorschriften muss dabei auch der Datenschutz im Blick behalten werden. Das gilt besonders dann, wenn echte Behandlungsfälle im Internet landen. Exemplarisch dafür steht ein Fall, der die LDI NRW im vergangenen Jahr beschäftigte und der der betreffenden Psychotherapeutin am Ende eine Verwarnung einbrachte.

Die Psychotherapeutin hatte ihre Follower*innen über einen von der Krankenkasse genehmigten Therapieantrag informiert, um das mit ihrer Community zu feiern. Hierzu hatte sie ein Foto der Bewilligung für alle sichtbar auf ihrem Social-Media-Account hochgeladen. Was sie dabei offenbar übersah: Nicht nur die Bewilligung wurde öffentlich, auch der Name der Patientin war klar lesbar. Eine rechtliche Begründung für die Veröffentlichung des Namens konnte die Therapeutin in der von der LDI NRW angeforderten Stellungnahme nicht geben. Es handelte sich schlicht und einfach um ein Versehen.

Auch wenn die Psychotherapeutin die fehlende Absicht glaubhaft darlegen konnte – datenschutzrechtlich kann eine solche Aktion nicht fol-

genlos bleiben. Die Veröffentlichung besonders geschützter Gesundheitsdaten auf Social-Media stellt einen schwerwiegenden Eingriff für die Betroffenen dar. Eine Verarbeitung von sensiblen Gesundheitsdaten unterliegt noch strengeren datenschutzrechtlichen Vorgaben als die Verwendung anderer personenbezogener Daten. Selbst wenn keine Diagnosen oder Therapien erkennbar werden, ist allein die Tatsache, dass jemand bei einer Ärztin in psychotherapeutischer Behandlung ist, ein Gesundheitsdatum.

Bei der Entscheidung der LDI NRW, gegenüber der Psychotherapeutin eine Verwarnung auszusprechen, war aber nicht nur der besondere Schutzbedarf von Gesundheitsdaten ausschlaggebend. Zusätzlich schwer wog die Weitergabe von Daten der Patientin an einen unbestimmbaren Empfängerkreis. Denn durch eine Veröffentlichung auf einem Social-Media-Account gibt die verantwortliche Stelle die Kontrolle über die Daten vollständig aus der Hand. Auch wenn die Therapeutin den Beitrag nach Hinweisen von ihren Followern direkt gelöscht hatte und dieser letztendlich nicht mehr als eine Stunde sichtbar wurde, war er nicht mehr rückholbar. Da nicht mehr nachvollzogen werden kann, wer den Beitrag gesehen oder womöglich auch weitergeleitet hat, sind die möglichen sozialen Folgen für die betroffene Patientin nicht abzusehen. Auch Schadensersatzansprüche der Betroffenen sind denkbar, weil sie in solchen Fällen regelmäßig die Kontrolle über die eigenen Daten verlieren.

Ärzt*innen und Therapeut*innen sollten deshalb vor jeder Veröffentlichung auf Social-Media doppelt prüfen, ob Patient*innen womöglich identifizierbar sind. Dabei reicht es oft nicht aus, bloß auf den Klarnamen der Patient*innen zu verzichten. Allein die Summe weiterer veröffentlichter individueller Merkmale kann dazu führen, dass Außenstehende, die die Person kennen, sie dennoch identifizieren können. Die LDI NRW empfiehlt deshalb, einen Prüfprozess für die Veröffentlichung von Social-Media-Beiträgen zu definieren und zu dokumentieren. Im Zweifel muss vor einer Veröffentlichung eine Einwilligung der betroffenen Patient*innen eingeholt werden. Selbstverständlich ist diese nur wirksam, wenn die Patient*innen sie absolut freiwillig erteilen. Denn nur dann kann gegenüber der LDI NRW bei Beschwerden nachgewiesen werden, dass die im Umgang mit Gesundheitsdaten gebotene absolute Sorgfalt auch beachtet wurde.

Fazit

Für Ärzt*innen und Therapeut*innen, die über einen Social-Media Account einen Einblick in ihr Praxisleben geben wollen, sollten Daten von Patient*innen in der Regel tabu sein.

9. Wirtschaft

9.1. Dreiste Praktiken – LDI NRW verhängt Bußgeld von 300.000 Euro gegen Telekommunikationsunternehmen

Hunderte von Beschwerden, aktenweise Ermittlungs- und Erinnerungsschreiben der Aufsichtsbehörde: Ein Telekommunikationsunternehmen aus NRW ignoriert seit Jahren Betroffenenrechte und Transparenzpflichten. Das führte 2025 zu empfindlichen Konsequenzen.

Nicht immer zeigen sich Unternehmen sofort einsichtig, wenn es um Datenschutzverstöße geht. Nicht in jedem Fall werden Mitwirkungspflichten direkt umgesetzt, wenn die Aufsichtsbehörden darauf hinweisen. Ein Verhalten wie das eines Telekommunikationsunternehmens aus NRW ist der LDI NRW aber bisher noch nicht untergekommen. Trotz klarer Datenschutzverstöße und gesetzlicher Verpflichtungen gegenüber Betroffenen und Behörden ignorierte das Unternehmen die Maßnahmen der LDI NRW und änderte seine Geschäftspraktiken nicht. Bereits im letzten Datenschutzbericht für das Jahr 2024 hatte die LDI NRW den Fall um irreführende Werbeschreiben des Unternehmens und das damit verbundene datenschutzwidrige Verhalten aufgegriffen. Nun hat das illegale Geschäftsgebaren im vergangenen Jahr zu einem Bußgeld von 300.000 Euro geführt.

Die Anzahl der bei der LDI NRW eingegangenen Beschwerden geht in die Hunderte. Über einen Zeitraum von nahezu zwei Jahren versandte das Unternehmen personalisierte Werbeschreiben, die dem Anschein nach aus der Feder eines bekannten großen Telekommunikationsunternehmens

stammen und den Eindruck eines Angebots zum Tarifwechsel – nicht zum Anbieterwechsel – erwecken konnten. Wie das Unternehmen die personenbezogenen Daten der Adressat*innen erhalten haben könnte, war den Angeschriebenen schleierhaft. Sie gaben durchweg an, niemals zuvor Kontakt mit dem Unternehmen gehabt zu haben. Dafür waren die Werbeschreiben umso detaillierter. Sie enthielten sowohl die Adresse als auch die Festnetztelefonnummer der Angeschriebenen.

Die machten daraufhin ihre Betroffenenrechte nach der DS-GVO geltend. Das heißt, sie richteten einen Antrag auf Auskunft zu ihren personenbezogenen Daten – insbesondere auf Auskunft zur Herkunft der Daten – oder auch auf Löschung an das Telekommunikationsunternehmen. Darüber hinaus legten sie noch Werbewidersprüche ein. Das Unternehmen reagierte – entgegen seiner gesetzlichen Pflicht – aber auf keinen einzigen der Anträge.

Daraufhin wandten sich Adressat*innen der Werbeschreiben an die LDI NRW. Die Überprüfung zeigte, dass das Unternehmen sich nicht nur ignorant gegenüber den Betroffenenrechten verhielt, sondern es schon an der Erfüllung der Informationspflichten bei Verarbeitung personenbezogener Daten zu Werbezwecken mangelte. Weiter fehlte es im Unternehmen an jeglicher Dokumentation zur Datenverarbeitung. Damit wurde das Unternehmen der Rechenschaftspflicht aus Art. 5 Abs. 2 DS-GVO nicht gerecht, insbesondere mit Blick auf die Rechtmäßigkeit und die Transparenz der Datenverarbeitung.

Trotz Aufforderungen zur Stellungnahme in jedem einzelnen Fall – und auch vieler Erinnerungsschreiben, die bei der LDI NRW mehrere Aktenordner füllen – änderte das Unternehmen seine Geschäftspraktiken nicht. Es versandte weiter gleichlautende Werbeschreiben, antwortete der LDI NRW lediglich sporadisch und knapp – und den Beschwerdeführenden weiterhin gar nicht.

Die erste scharfe Reaktion erfolgte dann im Sommer 2025: Die LDI NRW erließ unter Androhung eines Zwangsgeldes eine Anweisung zu datenschutzkonformem Verhalten. Im Einzelnen wurde dem Unternehmen aufgegeben, ein Verarbeitungsverzeichnis nach Art. 30 Abs. 1 DS-GVO sowie Erläuterungen zur Rechtmäßigkeit der Verarbeitung vorzulegen. So soll sichergestellt werden, dass personenbezogene Daten zukünftig durch das Unternehmen ausschließlich unter Berücksichtigung einer einschlägigen Rechtsgrundlage verarbeitet und Betroffenenrechte geachtet werden. Das Unternehmen hat in seiner Antwort erklärt, schon seit Längerem keinerlei Werbeschreiben oder Werbeaktionen mehr durchzuführen und bei künftigen Werbeschreiben die datenschutzrechtlichen Vorgaben und Hinweise der LDI NRW umzusetzen.

Im November setzte die LDI NRW zudem Geldbußen in Höhe von 100.000 und 200.000 Euro gegen das Telekommunikationsunternehmen fest. Damit werden zum einen die Verstöße gegen die Informationspflichten

geahndet und zum anderen das Ignorieren der Anträge der Betroffenen, etwa auf Auskunft und Löschung. Inhaltlich hatte das Unternehmen den Vorwürfen im Ermittlungsverfahren wenig entgegenzusetzen. Es zweifelte an der Zuständigkeit der LDI NRW und verwies wegen nicht beantworteter Auskunftsbegehren auf vermeintliche Zustellprobleme der Post. Die Zuständigkeitsfrage ist gesetzlich klar umrissen. Während die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit für den Datenschutz dann zuständig ist, wenn es um Daten geht, die für die geschäftsmäßige Erbringung einer Telekommunikationsdienstleistung erforderlich sind, überwacht die LDI NRW die übrigen Datenverarbeitungstätigkeiten der Telekommunikationsunternehmen in NRW. In den von der LDI NRW bearbeiteten Fällen haben die Betroffenen keinen Telekommunikationsvertrag geschlossen, so dass die Daten zu keinem Zeitpunkt zur Erbringung von Telekommunikationsdiensten verarbeitet wurden. Auch das Vorbringen des Unternehmens zu angeblichen Zustellproblemen war wenig gehaltvoll, da die Betroffenen zu einem großen Teil Zustellnachweise vorweisen konnten.

Im Bußgeldverfahren fiel nicht zuletzt erschwerend ins Gewicht, dass sich das Telekommunikationsunternehmen der LDI NRW als Aufsichtsbehörde gegenüber nur sehr eingeschränkt kooperativ verhielt – trotz klarer gesetzlicher Vorschriften zur Mitwirkung und vieler Erinnerungen. Das Unternehmen hat mittlerweile gegen den Bußgeldbescheid Einspruch eingelegt.

Fazit

Systematische Verstöße gegen Auskunftsrechte von Verbraucher*innen sowie die hartnäckige Weigerung, Transparenz über die eigene Datenverarbeitung herzustellen, sind nicht hinnehmbar und haben zwangsläufig Konsequenzen. Die Folge können hohe Bußgelder sein.

9.2. EU-weite Prüfaktion: Wie läuft es mit dem Recht auf „Vergessenwerden”?

Wie gut setzen Unternehmen und Behörden in der EU das Recht auf Löschung personenbezogener Daten um? Das wollten die europäischen Datenschutzbehörden im Rahmen einer EU-weiten Prüfaktion herausfinden, an der auch die LDI NRW beteiligt war. In dem von ihr geprüften Bereich, der Versicherungsbranche, waren die Ergebnisse erfreulich.

Die europäischen Aufsichtsbehörden überprüfen regelmäßig in koordinierten Aktionen, wie es um die Umsetzung der DS-GVO steht.

Nachdem im Jahr 2024 das Recht der Bürger*innen auf Auskunft über sie betreffende Daten im Mittelpunkt stand, haben die Behörden 2025 den Umgang mit Löschanträgen unter die Lupe genommen. Insgesamt 32 Aufsichtsbehörden aus dem Europäischen Wirtschaftsraum haben mitgemacht – es war bereits die vierte gemeinsame Aktion dieser Art. Auch die LDI NRW hat sich beteiligt, ihr Fokus lag auf dem Sektor der Versicherungsunternehmen.

Die Prüfung ist Teil des Coordinated Enforcement Framework (CEF), einer EU-weiten Initiative des EDSA. Sie soll sicherstellen, dass das wichtigste Datenschutz-Regelwerk, die DS-GVO, nicht nur auf dem Papier existiert, sondern überall in der EU wirksam angewandt wird. Kern der Untersuchung war ein europaweit unter den beteiligten Behörden abgestimmter Fragebogen, der ausgewählten Unternehmen und Behörden zugeschickt wurde. Er sollte klären, wie diese mit Löschungsbegehren umgehen: Werden Daten tatsächlich entfernt, wenn sie nicht mehr benötigt werden? Wie transparent ist der Prozess für Betroffene? Und wo hakt es in der Praxis?

Dabei wurden die Untersuchungen auf nationaler Ebene entweder dazu durchgeführt, den Aufsichtsbehörden weitere Erkenntnisse zu liefern, oder um festzustellen, ob eine förmliche Untersuchung gerechtfertigt ist. Teilweise erfolgten sie auch im Rahmen eines förmlichen Durchsetzungsverfahrens.

Im Rahmen der Prüfung wurden Informationen von einer Vielzahl von Verantwortlichen aus verschiedenen Sektoren und Unternehmen unterschiedlicher Größe gesammelt. Insgesamt haben den Fragenbogen rund 700 Verantwortliche beantwortet, wodurch die teilnehmenden Aufsichtsbehörden praktische Einblicke in viele Aspekte der Umsetzung des Rechts auf Löschung im gesamten Europäischen Wirtschaftraum gewinnen konnten.

Das Recht auf Löschung gilt nicht absolut, sondern ist nur anwendbar, wenn kein legitimer Grund zur weiteren Speicherung der personenbezogenen Daten durch die verantwortliche Stelle besteht. So können beispielsweise gesetzliche Pflichten, öffentliche Interessen oder die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen das Recht einschränken. Dies macht den Umgang mit Anträgen auf Löschung für die Verantwortlichen besonders herausfordernd.

Erfreulicherweise hat die Untersuchung bei den von der LDI NRW befragten Versicherungsunternehmen ein hohes Niveau an Regeltreue gezeigt. Die Untersuchung liefert wertvolle Hinweise für den weiteren Dialog zur Verkürzung der Aufbewahrungsdauer von Gesundheitsdaten durch die Versicherungsunternehmen. Die gewonnenen Erkenntnisse bilden einen Baustein für die weiteren Schritte der LDI NRW zur Verkürzung dieser derzeit teils mehrere Jahrzehnte langen Fristen.

Aus den Ergebnissen der europaweiten Prüfung sollen ebenfalls konkrete Maßnahmen abgeleitet werden. Es könnten etwa neue Leitlinien entstehen oder Empfehlungen zu bestehenden Vorgaben abgegeben werden, um die Rechte der Bürger*innen in der digitalen Welt besser zu schützen. Zugleich soll die Aktion den Austausch und die Zusammenarbeit der Datenschutzbehörden stärken.

Der EDSA wird im ersten Halbjahr 2026 einen umfassenden Bericht vorlegen. Dann werden auch die nationalen Berichte der jeweils beteiligten Aufsichtsbehörden veröffentlicht. Der europäische Bericht wird die am häufigsten identifizierten Fallstricke bei der Bearbeitung des Rechts auf Löschung durch die Verantwortlichen enthalten. Zu diesen Aspekten wird der EDSA Empfehlungen abgeben, um Fehler bei der Gewährung dieses Betroffenenrechts zu vermeiden. Außerdem wird der Bericht Hinweise auf bereits vorhandene Vorgaben, Muster und Hilfestellungen der Aufsichtsbehörden enthalten.

Im Jahr 2026 wird es erneut eine koordinierte Aktion geben – diese befasst sich dann mit der Einhaltung der Transparenz- und Informationspflichten gemäß der DS-GVO.

Fazit

Das Recht auf Löschung ist ein zentraler Pfeiler des Datenschutzes. Immer wieder erreichen die LDI NRW Beschwerden, wonach verantwortliche Stellen entsprechende Anträge schlicht ignorieren oder nur unzureichend erfüllen. Auch bei anderen europäischen Behörden hat das Recht auf Löschung zu zahlreichen Beschwerden und Entscheidungen geführt. In einer Welt, die ständig nach mehr Datennutzung verlangt, ist es entscheidend, das Recht auf Vergessenwerden zu verteidigen. Falsche oder überholte Informationen dürfen Betroffenen nicht dauerhaft zum Nachteil gereichen.

9.3. LDI NRW unterbindet Austausch sensibler Daten

Ein geschlossener E-Mail-Verteiler, sensible Gesundheitsdaten und gleich mehrere Versicherer: 2024 erhielt die LDI NRW Hinweise auf einen rechtswidrigen Datenaustausch – und leitete unmittelbar eine Prüfung gemeinsam mit anderen Aufsichtsbehörden in Deutschland und in Liechtenstein ein. Nun geht es um die Konsequenzen.

Der Fall machte Schlagzeilen: Unter dem Begriff „Datenkartell" berichteten verschiedene Medien über Ermittlungen der LDI NRW gemeinsam mit anderen Aufsichtsbehörden gegen Versicherungsunternehmen. Knapp 40 Versicherer aus Deutschland und auch aus Liechtenstein hatten zur Betrugserkennung in der Auslandsreisekrankenversicherung Kund*innendaten über einen gemeinsamen E-Mail-Verteiler ausgetauscht – darunter auch Gesundheitsdaten und Daten Minderjähriger (siehe hierzu 30. Bericht unter 10.7).

Da elf der beteiligten Unternehmen in NRW ansässig sind, leitete die LDI NRW 2024 eine Überprüfung ein. Zwar ist Betrugsprävention ein berechtigtes Interesse von Unternehmen, das eine Datenverarbeitung legitimieren kann. Die konkrete Ausgestaltung war jedoch nicht zulässig. Für einen derart umfangreichen Datenaustausch fehlte es erkennbar an einer Rechtsgrundlage. 2025 ging die Beschäftigung mit dem Fall weiter. Die Unternehmen müssen mit Konsequenzen rechnen.

Bei der Bewertung spielt vor allem eine Rolle, dass die Versicherungsunternehmen an einem eigens zur Bekämpfung von Versicherungsbetrug eingerichteten System vorbei operierten. Das sog. Hinweis- und

Informationssystem der deutschen Versicherungswirtschaft (HIS) wurde konkret dafür errichtet, dass sich Versicherungen datenschutzkonform über mögliche Betrugsversuche austauschen können. Entscheidend ist hier, dass es sich beim „HIS" um eine reine Hinweisdatei handelt. Der Austausch über konkrete Informationen zu den verdachtsbegründenden Tatsachen erfolgt nur zwischen den Versicherungen, die jeweils die zu versichernde Person betreuen oder betreuten. Daher werden über das „HIS" auch keine Gesundheitsdaten geteilt – und dies mit gutem Grund. Denn die Verarbeitung von Gesundheitsdaten ist wegen derer besonderen Sensibilität nur unter sehr eng umgrenzten Voraussetzungen zulässig.

Im aktuellen Fall nutzten die beteiligten Versicherungsunternehmen hingegen einen E-Mail-Verteiler, in dem Inhaltsdaten einschließlich Gesundheitsdaten mit allen am Verteiler angeschlossenen Unternehmen geteilt wurden, selbst wenn diese zu der versicherten oder zu versichernden Person niemals Kontakt hatten. Es fehlten jegliche Maßnahmen für einen datenschutzkonformen Austausch, die die Übermittlung der Daten auf das erforderliche und gesetzlich zulässige Maß beschränkten. Die Praxis war außerdem auch deswegen datenschutzrechtlich unzulässig, weil die betroffenen Personen nicht über den Datenaustausch informiert wurden.

Die Datenschutzaufsichtsbehörden haben deshalb zunächst unter Koordinierung durch die LDI NRW die Unternehmen erfolgreich aufgefordert, den Austausch unverzüglich abzustellen. Außerdem sollten die von der LDI NRW beaufsichtigten Versicherungen die betroffenen Personen über den Datenaustausch nachträglich informieren.

Doch damit ist der Fall noch nicht erledigt. Die LDI NRW prüft derzeit die Einleitung von Bußgeldverfahren gegen die in NRW ansässigen Versicherungsunternehmen Zudem führen die Datenschutzaufsichtsbehörden zusätzlich Gespräche mit den beteiligten Unternehmen, wie der Austausch über Betrugsverdacht in der Auslandsreisekrankenversicherung datenschutzkonform gestaltet werden kann.

Fazit

Die Bekämpfung von Versicherungsbetrug kommt grundsätzlich allen Versicherten zugute, da sie verhindert, dass betrugsbedingte Mehrkosten auf die Gemeinschaft umgelegt werden. Dabei dürfen jedoch keine Methoden eingesetzt werden, die gegen den Datenschutz verstoßen. Um künftige Rechtsverletzungen zu verhindern, sind die Datenschutzaufsichtsbehörden mit der Versicherungsbranche in einen Dialog eingetreten.

9.4. Versicherungen erhalten neue Verhaltensregeln für den Umgang mit Kund*innendaten

Die Versicherungswirtschaft hat sich mit den Datenschutzaufsichtsbehörden auf neue Verhaltensregeln für ihre Branche verständigt. Dieser sog. Code of Conduct beschreibt insbesondere, unter welchen Bedingungen Versicherungsunternehmen die besonders sensiblen Gesundheitsdaten verarbeiten dürfen.

Codes of Conduct (CoC) sind geeignete Instrumente, um im Datenschutz Rechtssicherheit und Transparenz herzustellen. Sie sind Selbstverpflichtungserklärungen innerhalb einer Branche, bestimmte datenschutzrechtliche Standards einzuhalten. Die Datenschutzaufsichtsbehörden beraten bei der Entwicklung, um potentielle Streitpunkte bereits im Vorhinein auszuräumen.

Einem solchen CoC für die Versicherungsbranche haben die Datenschutzaufsichtsbehörden des Bundes und der Länder im Dezember 2025 grünes Licht erteilt. Der Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV) hatte die neuen Verhaltensregeln vorgelegt. Nun steht, zusammen mit der Akkreditierung der entsprechenden Überwachungsstelle, die Genehmigung des Regelwerks durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit an. Die LDI NRW hat sich maßgeblich an der Entstehung des CoC beteiligt. Sie beaufsichtigt in NRW einige große Versicherungsunternehmen und verfügt deshalb über viel Aufsichtserfahrung. Zugleich hat sie ein großes Interesse daran, ihre Aufsichtsstandards der Versicherungswirtschaft in Deutschland zu vermitteln.

Bereits unter der alten Fassung des Bundesdatenschutzgesetzes existierte in Deutschland ein Datenschutzkodex des GDV. Dieser wurde rechtzeitig vor Anwendung der DS-GVO ab Mai 2018 an die neuen gesetzlichen Regelungen angepasst. Bereits damals waren die Datenschutzaufsichtsbehörden beratend tätig. Allerdings wurde dieser CoC nicht durch die zuständige Aufsichtsbehörde nach Art. 40 DS-GVO genehmigt, da die erforderliche Überwachungsstelle für den Code nicht benannt war.

Für die Versicherungsnehmer*innen schafft der neue CoC Transparenz, wie das Datenschutzrecht bei spezifischen Fragen im Rahmen ihres Versicherungsverhältnisses angewendet wird. Für die Versicherungswirtschaft wiederum bedeutet er Rechtssicherheit im Verhältnis zu den Aufsichtsbehörden, weil ein einheitliches Verständnis über die im CoC berücksichtigten Fragen erreicht wurde. Die aktuelle Rechtsprechung sowie die Veröffentlichungen der europäischen und deutschen Datenschutzaufsichtsbehörden finden im CoC ihre branchenspezifische Konkretisierung.

Klarheit schafft der CoC insbesondere in folgenden Punkten:

- Häufig verwendete Begriffe in der Versicherungswirtschaft wie etwa „wissenschaftliche Forschung" werden konkret definiert, um dasselbe Verständnis über diese Begriffe sicherzustellen.

- Der Ablauf, wie Betroffene ihr Auskunftsrecht gegenüber einer Versicherung ausüben können, wurde besser strukturiert. So sind Versicherungsunternehmen grundsätzlich berechtigt, gestuft Auskünfte zu erteilen, da sie regelmäßig große Mengen an Daten verarbeiten. Zunächst erfolgt die Auskunft über die allgemeinen Daten der betroffenen Person sowie zusammenfassende Informationen nach Art. 15 Abs. 1 und Abs. 2 DS-GVO, die von der jeweiligen Versicherung in der laufenden Vertragsbeziehung aktuell verarbeitet werden. Damit die betroffene Person einschätzen kann, welche weiteren Datenverarbeitungen stattfinden, erläutert die verantwortliche Stelle sodann im Überblick, welche Datenverarbeitungen und Aktivitäten für die betroffene Person darüber hinaus von Bedeutung sein können. Die verantwortliche Stelle weist die betroffene Person auf dieser Stufe ergänzend darauf hin, dass zum Beispiel durch Benennung des Zeitraums und des konkreten Geschäftsvorgangs die Möglichkeit besteht, gezielt nach weitergehenden Daten zu suchen und diese zu benennen. Nimmt die betroffene Person keine Konkretisierung vor, ist die verantwortliche Stelle jedoch grundsätzlich verpflichtet, umfassend Auskunft zu erteilen. Art. 23 Abs. 2 des CoC überträgt diese Vorgehensweise auf die Versicherungswirtschaft unter Verwendung des Wortlauts der einschlägigen EDSA-Leitlinien zu Art. 15 DS-GVO.

- Werden Auskünfte der Betroffenen in deren Namen durch Anwält*innen geltend gemacht, erfolgt eine Auskunft unmittelbar an die Anwält*innen nur dann, wenn sie eine entsprechende Empfangsbevollmächtigung nachweisen. Dies dient vor allem dem wirksamen Schutz sensibler Daten der Betroffenen, die die Versicherungen verarbeiten.

- Versicherungsunternehmen müssen die von der Datenverarbeitung Betroffenen transparent gemäß Art. 13, 14 DS-GVO unter anderem über Dienstleister informieren, die bei der Datenverarbeitung unterstützen. Da dies oft sehr viele Dienstleister sind, beschreibt der CoC, wie dies über Listen überschaubar und aussagekräftig sowie im Einklang mit den EDSA-Leitlinien zur Transparenz gelingt.

- Geht es um die Verarbeitung von Gesundheitsdaten in sog. Regressfällen, also Fällen, in denen die Versicherung nach Leistung eines Schadens ihr Geld vom eigentlichen Verursacher zurückfordert, bedarf es keiner datenschutzrechtlichen Einwilligung der Versicherungsnehmer*innen. Die Datenverarbeitung kann vielmehr

auf die gesetzliche Grundlage nach Art. 9 Abs. 2 lit. f DS-GVO gestützt werden, wenn die Verarbeitung für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Eine Einwilligung der geschädigten Person könnte zwar auch in diesen Fallkonstellationen eine Grundlage für die Datenübermittlung sein. Sie ist allerdings praktisch häufig nicht geeignet. Denn die Betroffenen haben regelmäßig kein Interesse, die Einwilligung zu erteilen, da sie ihre Gesundheitskosten bereits vom eigenen Versicherer erstattet erhalten haben.

- Soweit die Versicherungen Einwilligungen in die Datenverarbeitung einholen, stellt der CoC klar, dass man bereits bei Jugendlichen ab Vollendung des 16. Lebensjahres davon ausgeht, dass diese die für eine Einwilligung notwendige Einsichtsfähigkeit haben. Die Versicherer holen daher deren datenschutzrechtliche Einwilligung neben der zivilrechtlich erforderlichen Beteiligung der geschäftlich vertretungsberechtigten Eltern ein.

Der CoC trifft zudem Aussagen zur künftigen Überwachungsstelle, also jener Einrichtung, die die Einhaltung des CoC kontrolliert. So orientieren sich die Regeln für diese Stelle (Art. 29a ff. des CoC) an den von der LDI NRW entwickelten zentralen Pflichten für eine solche Einrichtung, niedergelegt in dem DSK-Papier „Kernelemente der Überwachungsaufgaben von Überwachungsstellen für Verhaltensregeln nach Art. 40 DS-GVO" vom 23.11.2023. Die LDI NRW konnte außerdem erreichen, dass der jährliche Bericht der Überwachungsstelle auch den zuständigen Aufsichtsbehörden zur Verfügung gestellt wird (Art. 29h Abs. 2 Satz 2 des CoC). So ist sichergestellt, dass auch die LDI NRW über die korrekte Anwendung der Verhaltensregeln durch die Versicherungsunternehmen, die sie beaufsichtigt, informiert bleibt.

Die Versicherungsunternehmen, die dem CoC beigetreten sind oder künftig beitreten, sind verpflichtet, ihre Datenverarbeitungsprozesse an den branchenspezifischen Standards auszurichten. Spätestens alle fünf Jahre erfolgt eine Evaluation der Regelungen.

Fazit

Der neue CoC für die Versicherungsbranche, an dessen Abstimmung unter den Datenschutzaufsichtsbehörden die LDI NRW maßgeblich mitgewirkt hat, beschreibt, unter welchen Bedingungen Versicherungsunternehmen personenbezogene Daten verarbeiten dürfen. Davon profitieren Versicherungsunternehmen, Versicherungsnehmer*innen und sonstige Personen, deren Schäden von Versicherungen ausgeglichen werden. Der CoC erleichtert zudem eine einheitliche Datenschutzaufsicht.

9.5. Schulden bezahlt, aber trotzdem noch bei der Auskunftei gespeichert? BGH äußert sich zu den Löschfristen der Branche

Dürfen Wirtschaftsauskunfteien Informationen zur Kreditwürdigkeit auch dann noch speichern, wenn die Forderung beglichen wurde? Der Branchenverband hat dazu eigene Regeln aufgestellt – und damit die LDI NRW wie auch den BGH überzeugt.

Verbände, die Daten verarbeitende Unternehmen repräsentieren, haben die Möglichkeit, die Anwendung des Datenschutzrechts spezifisch für ihre Branche in einem sog. Code of Conduct (CoC) festzulegen. Dies hat erhebliche Vorteile für Unternehmen, die sich diesen Verhaltensregeln unterwerfen. Genehmigt die zuständige Datenschutzaufsicht den CoC, bestätigt dies den Firmen, die sich dem CoC unterwerfen, dass ihre Datenverarbeitung als grundsätzlich rechtskonform anzusehen ist.

Auch der Verband der Wirtschaftsauskunfteien, also jener Unternehmen, die Informationen über Personen und Firmen sammeln, um deren Kreditwürdigkeit einzustufen, hat einen solchen CoC auf die Beine gestellt. Doch in einem besonderen Punkt war dessen Rechtmäßigkeit bislang umstritten. Der BGH hat in einem Urteil aus Dezember 2025 (Az. ZR 97/25) hier nun Klarheit geschaffen. Wirtschaftsauskunfteien müssen danach von Vertragspartnerunternehmen übermittelte Daten über Zahlungsstörungen nicht sofort löschen, wenn die Forderung beglichen wird. So hat es auch die LDI NRW bisher vertreten.

Zum Hintergrund: Der betreffende CoC war vor Jahren von der LDI NRW genehmigt worden. Allerdings hatte der EuGH eine darin enthaltene Regelung zur Speicherfrist von Informationen über Restschuldbefreiungen für nicht vereinbar mit dem Datenschutzrecht angesehen. Der Verband der Wirschaftsauskunfteien hatte daraufhin seinen CoC grundlegend überarbeitet und bei der hessischen Datenschutzaufsicht zur Genehmigung vorgelegt. Wegen eines Sitzwechsels des Verbandes war nämlich nicht mehr die LDI NRW, sondern nunmehr die hessische Aufsicht für die Genehmigung zuständig.

Nach intensiven Beratungen des Verbandes mit den Aufsichtsbehörden aus Hessen, Baden-Württemberg, Bayern und NRW wurde das Ergebnis schließlich von allen deutschen Aufsichtsbehörden in der Datenschutzkonferenz (DSK) gebilligt und der CoC im Mai 2024 von der Datenschutzaufsicht in Hessen genehmigt. Auf diese Weise sollten die Wirtschaftsauskunfteien, die ihre Datenverarbeitung an dem CoC ausrichten wollten, die notwendige Rechtssicherheit erhalten.

Allerdings kam es Monate danach zu einem Rechtsstreit, der bis zum BGH ging – und in dem auch der neue CoC eine Rolle spielte. Eigentlich wurde um einen Schadensersatzanspruch wegen unrechtmäßiger Datenverarbeitung gestritten. Dabei musste aber auch die Frage geklärt werden, ob Wirtschaftsauskunfteien Informationen, die sie von Partner-

unternehmen über nicht bezahlte Forderungen erhalten, auch nach dem Begleichen der Forderung weiterhin speichern dürfen. Hierzu enthält der neue CoC eine entsprechende Regelung.

Zunächst korrigierte der BGH die Auffassung des Berufungsgerichts, dass eine weitere Speicherung unzulässig sei. Anders als vom Berufungsgericht angenommen, seien Daten über Zahlungsstörungen, die Wirtschaftsakteure an Auskunfteien für die Bonitätsbewertungen übermittelten, nicht mit Daten zu vergleichen, die aus einem öffentlichen Register über die Restschuldbefreiung stammten. Lediglich die Informationen zur Restschuldbefreiung seien zügig zu löschen; sie dürften nur so lang von den Auskunfteien gespeichert werden, wie sie in dem öffentlichen Register enthalten sind. Der im Schuldnerverzeichnis veröffentlichten Restschuldbefreiung komme nämlich eine Warnfunktion zu, die nur so lange andauern dürfe, wie es für das Register vorgesehen sei. Die Bonitätsbewertung durch Auskunfteien dagegen ziele auf eine Prognose über zukünftige Zahlungsausfälle, die nicht funktioniere, sollten Informationen sofort nach Forderungsbegleichung gelöscht werden.

In einem zweiten Schritt klärte der BGH sodann, in welchem Umfang und wie lang säumige Zahlungen auch nach deren Ausgleich noch bei einer Bonitätsbewertung berücksichtigt werden dürfen. Dies sei im Einzelfall im Rahmen der Interessenabwägung gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO zu prüfen. Danach muss derjenige, der personenbezogene Daten verarbeitet, ein berechtigtes Interesse daran haben. Außerdem darf dieses Interesse nicht von dem Interesse der betroffenen Person und deren Grundrechten und Grundfreiheiten überwogen werden.

Hier stellte der BGH fest, dass die Regelung im CoC der Auskunfteien geeignet sei, den Anforderungen an die Rechtmäßigkeit der Datenverarbeitung grundsätzlich Rechnung zu tragen. Dort beträgt die regelmäßige Speicherfrist von säumigen Forderungen drei Jahre nach dem Begleichen der Forderung. Eine kürzere Speicherfrist von 18 Monaten ist dann vorgesehen, wenn der Auskunftei bis zu diesem Zeitpunkt keine weiteren Negativdaten gemeldet worden sind und keine Informationen aus dem Schuldnerverzeichnis oder aus Insolvenzbekanntmachungen vorliegen. Außerdem muss die Forderung innerhalb von 100 Tagen, nachdem sie bei der Auskunftei gemeldet worden ist, bezahlt worden sein. Schließlich lässt der CoC daneben auch noch Einzelfallprüfungen zu. So können Betroffene aus Gründen, die sich aus ihrer besonderen Situation ergeben, der Datenverarbeitung auch unabhängig von den zuvor genannten Voraussetzungen widersprechen.

Fazit

Das Urteil bestätigt, dass ein CoC mit gut abgewogenen Verhaltensregeln ein gutes Instrument ist, um der Wirtschaft Rechtssicherheit über die branchenspezifische Auslegung des Datenschutzrechts zu geben. Eine einheitliche Sicht aller deutschen Aufsichtsbehörden auf die Rechtsfragen wird durch die Verfahren der DSK sichergestellt.

9.6. Aufsichtsbehörden verlangen Gastzugang im Online-Handel

Die deutschen Datenschutzaufsichtsbehörden fordern seit Anfang 2022, dass bei der Online-Bestellung auch ein Gastzugang möglich sein muss, also Bestellungen auch ohne dauerhaftes Kund*innenkonto funktionieren. Die LDI NRW setzt sich auch auf europäischer Ebene dafür ein. Nun hat der EDSA entsprechende Empfehlungen veröffentlicht.

Online-Shopping ist aus dem Leben vieler Käufer*innen nicht mehr wegzudenken. Nach Zahlen aus den USA kauft mittlerweile über ein Drittel der Weltbevölkerung online ein, der Umsatz geht in die Billionen, fast 30 Millionen E-Commerce-Shops bieten weltweit ihre Waren an. Nicht alle, die online einkaufen, sind jedoch bereit, dabei eine Vielzahl ihrer persönlichen Daten preiszugeben. Viele Unternehmen bieten deshalb neben dem Anlegen von Kund*innenkonten zusätzlich an, dass Einkäufe auch über sog. Gastzugänge erfolgen können. Sie erlauben das Shopping, ohne sich vorher zu registrieren oder dauerhaft anzumelden.

Bereits 2022 haben sich die deutschen Aufsichtsbehörden in der DSK dahingehend positioniert, dass im Onlinehandel grundsätzlich auch ein Gastzugang möglich sein muss. Siehe hierzu die „Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang" vom 24. März 2022, abrufbar unter **www.datenschutzkonferenz-online.de/beschluesse-dsk.html** sowie 28. Bericht unter 9.7. Der EDSA ist für ganz Europa nachgezogen und hat Empfehlungen zur Verarbeitung personenbezogener Daten im Onlinehandel erarbeitet, die 2025 bekannt gemacht wurden – „Recommendations 2/2025 on the legal basis for requiring the creation of user accounts on e-commerce websites", abrufbar unter **www.edpb.europa.eu**. Diese Empfehlungen richten sich ausdrücklich auch

an die großen Onlinehandelsplattformen und nehmen lediglich Onlineshops für den Verkauf spezifischer regulierter Produkte und Dienstleistungen sowie Verbraucher-zu-Verbraucher-Plattformen aus.

Wie auch die DSK empfiehlt der EDSA Onlineshops, ihren Kund*innen Gastbestellungen zu ermöglichen. Begründung: Ein fortlaufendes Kund*innenkonto kann grundsätzlich nur auf Basis einer freiwilligen Einwilligung der Kund*innen eingerichtet werden. Mit den Empfehlungen soll den Onlineshops zugleich eine Leitlinie zur Verarbeitung der Kund*innen-Daten an die Hand gegeben werden, in welchen Fällen ausnahmsweise eine verpflichtende Einrichtung von laufenden Kund*innenkonten zur Anwendung kommen kann. Der EDSA definiert dies anhand von konkreten Fallbeispielen.

Wie der EDSA ausführt, ist eine etwaige Bereitschaft der betroffenen Person, weitere Einkäufe über die betreffende Website oder Anwendung zu tätigen, für sich allein nicht hinreichend, um die verpflichtende Einrichtung eines fortlaufenden Kund*innenkontos zu rechtfertigen. Kommt es hingegen zum Abschluss eines Dauerschuldverhältnisses (Abonnements), kann die Einrichtung eines verpflichtenden Kund*innenkontos auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO (Abschluss eines Vertrages) zulässig sein. Denn ein Abonnement ist auf eine gewisse Dauer angelegt, und deshalb kann es für die Erfüllung des Vertrags erforderlich sein, dass Kund*innen sich während der gesamten Laufzeit des Vertrags wiederkehrend authentifizieren, um die Leistungen in Anspruch nehmen zu können. Allerdings ist hierbei sehr genau zu prüfen, inwieweit die bei der Einrichtung des Kontos erhobenen Kund*innendaten tatsächlich für die Abwicklung des Verkaufs erforderlich sind. Kund*innen dürfen etwa nicht dazu gedrängt werden, optionale personenbezogene Daten anzugeben. Bei den Käufer*innen darf nicht der Eindruck entstehen, diese Daten seien für die Bearbeitung der Bestellung erforderlich.

Darüber hinaus ist ein laufendes Kund*innenkonto weder erforderlich, um im Falle einer Onlineplattform (Marktplatz) transparent darzustellen, welches Produkt von welchem Unternehmen oder Anbietenden gekauft wurde. Noch ist ein solches Konto notwendig, um Kund*innen die direkte Interaktion mit dem Anbietenden zu ermöglichen, um zum Beispiel Rücksendeetiketten zu erhalten oder Gewährleistungsansprüche geltend zu machen. Dies kann auch auf anderen Wegen erreicht werden. Es gilt hier der Grundsatz der Datensparsamkeit, da unnötige Daten unnötige Risiken für die Betroffenen erzeugen. Dies zeigt sich nicht zuletzt bei den sog. „verwaisten Kund*innen-Konten", die nur für einen einmaligen Einkauf eingerichtet worden sind und in denen Kreditkartendaten hinterlegt wurden. An diese können sich die Kund*innen unter Umständen gar nicht mehr erinnern. Solche verwaisten Konten können dann unter Umständen ein Angriffsziel für Identitätsdiebstahl bleiben, obwohl sie gar nicht mehr benötigt werden.

Der EDSA hat die Empfehlungen für eine öffentliche Konsultation bis zum 12. Februar 2026 veröffentlicht. Mit einer Verabschiedung im ersten Halbjahr 2026 ist zu rechnen.

Fazit

Der Grundsatz der Datensparsamkeit sollte gerade auch im Online-Handel zur Geltung kommen. Kund*innenkonten enthalten zahlreiche personenbezogene Daten, die Rückschlüsse auf persönliche Vorlieben und Interessen ermöglichen. Im Online-Handel müssen deshalb in der Regel Bestellungen ohne Kund*innenkonten möglich sein, um den Schutz der Privatsphäre beim Onlineshopping zu gewährleisten.

9.7. Dürfen die das? Wenn Online-Händler*innen an den Warenkorb erinnern

Die einen finden es bequem, wenn sie noch einmal an einen nicht abgeschlossenen Online-Einkauf erinnert werden. Die anderen fühlen sich bedrängt und verweisen auf den Datenschutz. Die LDI NRW hat sich mit der Rechtslage beschäftigt – und nennt neben den Regeln eine wichtige Ausnahme.

Da gehen die Meinungen auseinander: Sind E-Mails von Versandhäusern und anderen Online-Verkäufer*innen ein lästiges Zumüllen des eigenen Accounts? Oder sind sie hilfreiche Tools, um wichtige Einkäufe nicht zu vergessen? Und was ist eigentlich mit dem Datenschutz? Die LDI NRW hat sich im vergangenen Jahr mit dieser modernen Form der Kund*innenbindung beschäftigt, die einige Fragen aufwirft. Und nicht nur für Kund*innen, gerade auch für die Online-Händler*innen ist es wichtig, die Antworten zu kennen. Dabei gilt generell: Händler*innen ersparen sich Probleme, wenn sie bei der Erhebung von Mailadressen transparent darüber informieren, wofür sie diese nutzen wollen und Einwilligungen für die Nutzung zur Erinnerung einholen. Bei Bestandskund*innen sind in einem engen Rahmen Ausnahmen möglich.

Anlass für die LDI NRW, dieses Thema aufzugreifen, war die Beschwerde eines Kunden, der von einem Online-Händler nacheinander drei E-Mails erhielt, nachdem er Produkte in den Warenkorb des Online-Shops gelegt, die Bestellung aber nicht abgeschlossen hatte. Der Online-Händler sah solche Erinnerungen nicht als Werbung, sondern als „Servicekommunikation” im Interesse des Kunden und damit als zulässig an.

Beim Blick auf die Rechtslage ist zunächst festzuhalten, dass Warenkorberinnerungen nach Abbruch des Bestellvorgangs weder vorvertragliche noch vertragliche Maßnahmen sind. Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO lässt zwar unter gewissen Umständen eine Datenverarbeitung bei vorvertraglichen und vertraglichen Beziehungen zu. Da Kund*innen beim Verlassen einer Webseite ohne Einkauf aber deutlich zeigen, dass sie einen Vertrag nicht mehr eingehen wollen, können sich Online-Händler*in-

nen bei der Warenkorberinnerung nicht darauf berufen. Vielmehr ist das vorvertragliche Verhältnis damit beendet. Selbst wenn man das Ablegen von Produkten im Warenkorb und das Eingeben der personenbezogenen Daten, die für die Bestellung erforderlich sind, als Anfragen der Kund*innen zur Durchführung eines Kaufvertrags wertet, ist durch den Abbruch des Bestellvorgangs keine Geschäftsbeziehung zum Warenanbieter zustande gekommen. Die betroffene Person stellt auch nicht den Antrag, an den Warenkorb erinnert zu werden. Bei einer Erinnerung per E-Mail handelt es sich folglich um eine Datenverarbeitung, die ausschließlich auf Initiative der Online-Händler*innen erfolgt. Kund*innen ist bei Eingabe ihrer E-Mail-Adresse gar nicht bewusst, dass diese von den Anbieter*innen genutzt wird, um an das Kaufverhalten (Befüllen des Warenkorbs) per E-Mail zu erinnern.

Eine andere denkbare Rechtsgrundlage für Erinnerungsmails kann das sog. berechtigte Interesse nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO sein. Danach ist eine Datenverarbeitung zulässig, sofern sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" ist und „nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Mit Blick darauf muss die rechtliche Einschätzung differenziert werden und zwar danach, ob es sich um neue Kund*innen oder Bestandskund*innen handelt. Diese Differenzierung ergibt sich aus den Wertungen des Gesetzes gegen den unlauteren Wettbewerb (UWG), das auch Regeln für Werbung enthält.

Bei Erinnerungsmails handelt es sich nämlich um Werbung und nicht – wie der Händler im konkreten Fall bei der LDI NRW annahm – um Servicekommunikation. Wie aus einer EU-Richtlinie sowie Wertungen der Datenschutzaufsichtsbehörden hervorgeht, ist Wirtschaftswerbung „jede Äußerung bei der Ausübung eines Handels, Gewerbes, Handwerks oder freien Berufs mit dem Ziel, den Absatz von Waren oder die Erbringung von Dienstleistungen, einschließlich unbeweglicher Sachen, Rechte und Verpflichtungen, zu fördern" (Art. 2 lit. a der EU-Richtlinie 2006/114/EG vom 12. Dezember 2006; Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der DS-GVO). Direktwerbung ist dabei durch die unmittelbare Ansprache der Zielperson gekennzeichnet und kann in unterschiedlicher Form erfolgen, zum Beispiel postalisch, per E-Mail, Telefon, Fax oder SMS. Kaufabbruch- oder Erinnerungsmails verfolgen den Zweck der Umsatzsteigerung mit Bezug auf ein zuvor beobachtetes Kaufverhalten und sind daher als Online-Werbung („Retargeting") anzusehen.

Und damit kommt das UWG ins Spiel – denn werbliche Maßnahmen sind durch das UWG besonders reglementiert. Und im Interesse der Einheitlichkeit der Rechtsordnung können die Wertungen des UWG bei

der Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO nicht außer Acht gelassen werden. Kurz gesagt: Soweit das UWG Werbung nicht zulässt, kann dies auch nicht über die DS-GVO erlaubt werden. Umgekehrt ist nach dem UWG explizit zulässige E-Mail-Werbung auch nach der DS-GVO grundsätzlich zulässig.

Laut UWG (§ 7 Abs. 2 Nr. 1) ist E-Mail-Werbung, also auch die Warenkorberinnerungsmail, grundsätzlich nur mit ausdrücklicher Einwilligung zulässig. Dementsprechend ergibt die Interessenabwägung nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO: die Interessen der Kund*innen am Unterlassen der unverlangten Werbung überwiegen grundsätzlich das Werbeinteresse der Händler*innen. Sofern aber eine Einwilligung der Kund*innen vorliegt, können die Händler*innen die Mailadresse datenschutzkonform für Erinnerungsmails nutzen. Dabei könnte eine datenschutzkonforme Einwilligung – wie bei der Anmeldung zu einem Newsletter – mit einer aktiv anzuklickenden Checkbox und einem sog. Double-Opt-in-Prozess eingeholt werden.

Allerdings gilt eine Ausnahme für Bestandskund*innen. So erlaubt das UWG bei solchen Kund*innen Warenkorberinnerungen auch ohne Einwilligung, sofern die dafür festgelegten Bedingungen im Gesetz eingehalten werden. Diese sind nach § 7 Abs. 3 Nrn. 1 bis 4 UWG:

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

Unter den genannten Voraussetzungen ist dann auch die Datenverarbeitung auf der Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO möglich.

Im konkreten Fall, der bei der LDI NRW gelandet war, griff diese Ausnahmeregelung jedoch nicht ein. Der Beschwerdeführer war noch kein Kunde des Online-Händlers geworden, da er die Erstbestellung abgebrochen hatte und somit noch kein vorheriger Kaufvertrag zustande gekommen war. Die Datenverarbeitung war damit unzulässig.

Fazit

Online-Händler*innen sollten transparent damit umgehen, zu welchem Zweck sie erhobene E-Mail-Adressen verarbeiten, und müssen das Wettbewerbsrecht beachten. Das vermeidet Rechtsverstöße und ist gut für die Kundenzufriedenheit.

10. Finanzwirtschaft

10.1. Europäischer Gerichtshof sorgt für mehr Transparenz beim Kreditwürdigkeits-Check

Wer das sog. Scoring einsetzt, muss betroffene Personen nachvollziehbar darüber informieren, wie die automatisierte Einschätzung ihrer Kreditwürdigkeit zustande kommt. Es ist nicht das erste Mal, dass der EuGH in das Geschäft mit dem Scoring eingreift. Die Datenschutzbeauftragten erarbeiten dazu Hinweise für die Praxis.

Beantragen Verbraucher*innen ein Darlehn oder wollen sie eine Wohnung mieten oder auf Kredit einkaufen, sehen sie sich häufig mit der Überprüfung ihrer Kreditwürdigkeit konfrontiert. Dabei kommen oft auch Scorewerte zum Einsatz, die anhand von bestimmten Kriterien automatisiert eine Bewertung der Kreditwürdigkeit ausdrücken. Solche Scores werden oft durch Dienstleistungsunternehmen erstellt. Eines der bekanntesten Unternehmen in diesem Bereich ist die Schufa.

Umstritten sind dabei aber immer wieder die Grenzen, etwa in welchem Maß betroffene Personen über das Scoring zu informieren sind. Der EuGH hat hier im vergangenen Jahr zum zweiten Mal eingegriffen. Die Datenschutzbeauftragten von Bund und Ländern werden die Entscheidung in die Praxishinweise einfließen lassen, an deren Erarbeitung die LDI NRW beteiligt ist.

Konkret hat der EuGH am 27. Februar 2025 in der Rechtssache C-203/22 (Dun & Bradstreet Austria GmbH) das Auskunftsrecht nach Art. 15 Abs. 1 lit. h DS-GVO gestärkt. Das Auskunftsrecht besagt, dass betroffene

Personen eine Bestätigung und detaillierte Informationen darüber verlangen können, welche ihrer personenbezogenen Daten verarbeitet werden. Dies umfasst unter anderem den Verarbeitungszweck, die Art der Daten und die Speicherdauer. Zudem hat der EuGH noch einmal die auch von der DSK geforderte Transparenz für von Scoringverfahren betroffene Personen bestätigt.

Betroffene Personen haben nach der EuGH-Entscheidung einen Anspruch auf einzelfallbezogene Erläuterung zur involvierten Logik einer sie betreffenden automatisierten Entscheidung. Durch das Auskunftsrecht sollen Betroffene in die Lage versetzt werden, die Rechtmäßigkeit sowie die Richtigkeit der konkret verarbeiteten personenbezogenen Daten überprüfen zu können. Dementsprechend müssen sie auch alle notwendigen Informationen erhalten, um die automatisierte Entscheidung über den Score nachvollziehen zu können, der mit den eigenen Daten erstellt wurde. Um die widerstreitenden Interessen zwischen der Transparenz von Algorithmen und dem Geschäftsgeheimnisschutz in einen angemessenen Ausgleich zu bringen, verlangt der EuGH eine Interessensabwägung im Einzelfall und weist die Überprüfung der Ergebnisse solcher Abwägungen neben den Gerichten auch explizit den Datenschutzaufsichtsbehörden zu.

Der EuGH urteilt damit bereits zum zweiten Mal innerhalb von wenigen Jahren zum Scoring. Im Jahr 2023 hatte die DSK Vorschläge für ein datenschutzgerechtes Scoringverfahren gemacht und der damaligen Bundesregierung entsprechende Handlungsempfehlungen zugeleitet. Die „Vorschläge für Handlungsempfehlungen an die Bundesregierung zur Verbesserung des Datenschutzes bei Scoringverfahren" vom 11. Mai 2023 sind abrufbar unter **www.datenschutzkonferenz-online.de/stellungnahmen.html**. Sie beinhalten auch Vorschläge zu Umfang und Detailtiefe sowie Verständlichkeit von Informationen und Auskunftsrechten. Diese Forderungen der DSK bestätigte der EuGH 2023 in der Rechtssache C-634/21. Einige der von der DSK seinerzeit formulierten Anforderungen dürften sich also bereits jetzt als nach den Ausführungen des Gerichts zulässiges Ergebnis einer betroffenengerechten Auslegung der DS-GVO darstellen. So ist im Sinne der Transparenz zu gewährleisten, dass betroffene Personen Informationen zur Aussagekraft des konkreten Score-Wertes und zur Prognosegenauigkeit und damit zur Güte des Score-Wertes erhalten.

Die jüngste Entscheidung des Gerichts aus 2025 fließt nun ein in die laufenden Arbeiten der deutschen Aufsichtsbehörden, Kriterien für eine ordnungsgemäße Auskunft über Scoringverfahren festzulegen. Dabei sollen diese Arbeiten auch dazu führen, ein gemeinsames Verständnis dafür zu entwickeln, wie in der aufsichtsbehördlichen Praxis mit der Überprüfung von Geschäftsgeheimnissen umzugehen ist. Das Arbeitspapier soll zum einen eine einheitliche Prüfpraxis der Aufsichtsbehörden sicherstellen und zugleich auch eine Handreichung für verantwortliche Stellen darstellen. Die LDI NRW leitet einen der Arbeitskreise, die dieses Arbeitspapier erstellen.

Fazit

Betroffene können von Auskunfteien und anderen Unternehmen, die Scoreverfahren nutzen, eine nachvollziehbare Erklärung über ihren Score-Wert erwarten. Die DSK wird die Verantwortlichen dazu mit praxisgerechten Hinweisen unterstützen, an deren Erarbeitung die LDI NRW beteiligt ist.

10.2. Betrugsbekämpfung im Zahlungsverkehr: LDI NRW arbeitet mit Finanzaufsichtsbehörden und Wirtschaftsvertreter*innen an Strategien

Immer schneller, immer digitaler: Der moderne digitale Zahlungsverkehr hat viele Vorteile, er zieht aber auch neue Betrugsformen nach sich. Die Deutsche Bundesbank hat deshalb wichtige Vertreter*innen aus allen Bereichen an einen Tisch geholt. Ihr Ziel: der vereinte Kampf gegen die neuen Kriminalitätsformen. Mit dabei: die LDI NRW, stellvertretend für die deutschen Datenschutzbehörden.

Noch vor wenigen Jahren war der Begriff „Social Engineering" nur Fachleuten bekannt. Heute wird diese Form des Betrugs mittels „Identitätsdiebstahls" nahezu täglich versucht. Kriminelle verleiten dabei etwa ihre Opfer, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät oder einem Computer im Firmennetzwerk zu installieren.

Wie ernst diese neue Form des Betrugs im Zahlungsverkehr zu nehmen ist, zeigt auch eine Aktion der Deutschen Bundesbank. Sie hat 2025 Vertreter*innen der wichtigsten Akteur*innen in diesem Bereich an einen Tisch gebracht, um wirksame Strategien zu diskutieren und zu entwickeln – darunter auch die LDI NRW, stellvertretend für die deutschen Aufsichtsbehörden. Mit von der Partie waren zudem hochrangige Vertreter*innen des Finanzsektors, von Handel, Verbraucherschutz, von Telekommunikations- und Internetdienstleistern, Ministerien sowie Aufsichts- und Strafverfolgungsbehörden.

Die Teilnehmenden sind sich darüber einig, dass es sich bei der Betrugsbekämpfung um eine gesamtgesellschaftliche Aufgabe handelt, die den vollen Einsatz und die Zusammenarbeit aller Beteiligten erfordert. Dabei wirkt sich die Betrugsbekämpfung allerdings teilweise auch auf den Datenschutz aus, den die LDI NRW innerhalb der Gruppe besonders im Blick hat. So kann man zwar davon ausgehen, dass alle Rechtschaffenen, die am Zahlungsverkehr teilnehmen, ein Interesse an der Betrugsbekämpfung haben. Zugleich möchte aber niemand selbst zu Unrecht in den Fokus der Ermittlungen geraten.

Um das zu vermeiden oder schnell zu bereinigen, müssen deshalb die entsprechenden Verfahren transparent gestaltet sein – etwa der Einsatz von KI-Verfahren und deren Ergebnisse – sowie zügige Korrekturen möglich werden, sollten fehlerhafte Ergebnisse erzeugt worden sein. Ein zentraler Punkt ist deshalb in allen Bereichen die Transparenz über die Verarbeitung der Daten.

Die Teilnehmenden des Roundtable Betrugsbekämpfung haben drei Handlungsfelder identifiziert, die in Form gemeinschaftlicher Arbeiten auf Expertenebene weiterverfolgt werden sollen. Dies sind: die gemeinsame Kommunikation gegenüber Verbraucher*innen, der sektorübergreifende Informationsaustausch zu konkreten Betrugsfällen und die Bewertung der (datenschutz-)rechtlichen Grundlagen für die Betrugsbekämpfung. Hierzu sollen konkrete Maßnahmen erarbeitet werden, mit denen Betrug im Zahlungsverkehr branchenübergreifend wirksam bekämpft werden kann.

Die LDI NRW wird an den weiteren Treffen des Roundtable teilnehmen. Insbesondere wird sie mitwirken an der Bewertung der (datenschutz-) rechtlichen Grundlagen für die Betrugsbekämpfung. In dieser Gruppe werden bei Bedarf auch Vorschläge zur Verbesserung des Informationsaustauschs sowie des Schutzes unter anderem vor sog. Phishing-, Smishing- oder Spoofing-Attacken erarbeitet.

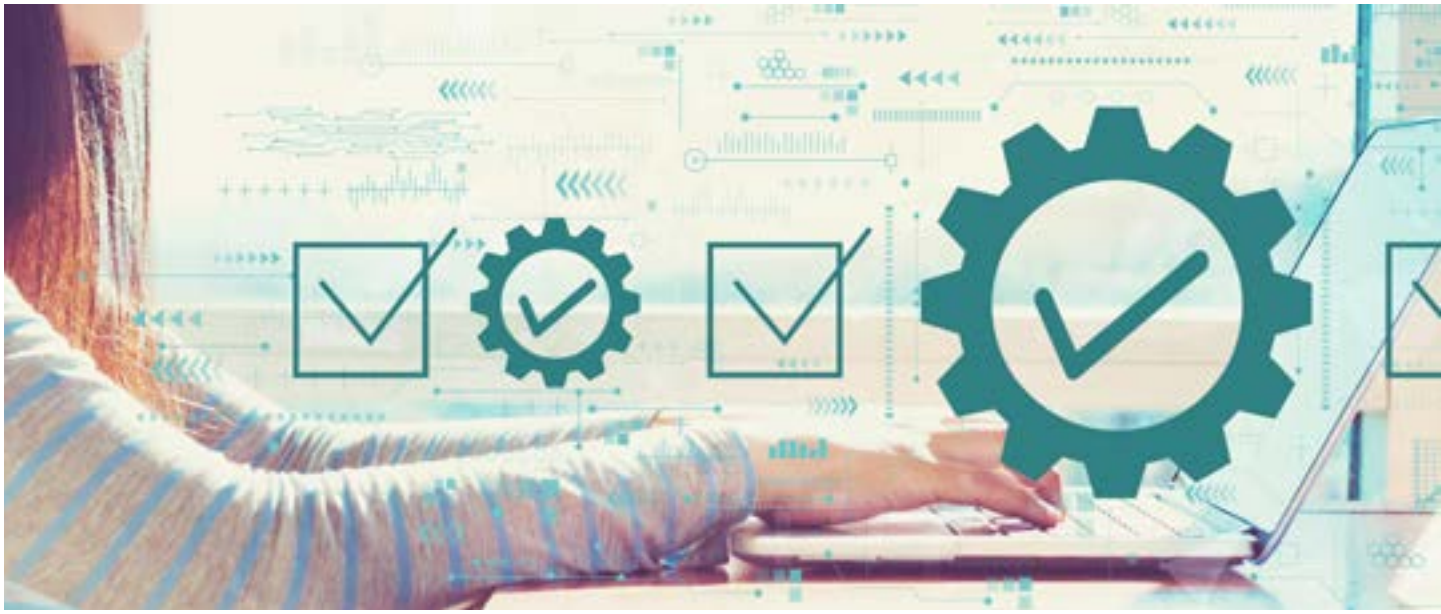
Phishing, Smishing und Spoofing sind Begriffe für Betrugsmaschen. Beim Phishing fordern als seriöse Bank, Internetanbieter oder andere Dienstleister getarnte Spam-E-Mail-Absender die Empfänger*innen zum Beispiel zu einer vorgeblich notwendigen Aktualisierung ihrer persönlichen Daten auf. Hinter Smishing steckt das Phishing per SMS. Das vorrangige Ziel ist es, Zugangsdaten abzugreifen und diese für weitere Betrügereien zu missbrauchen. Spoofing beschreibt die Technik, bei der sich Angreifer als jemand anderes ausgeben, oft als Teil eines Phishing-Angriffs.

Die LDI NRW nahm als Vorsitzende des zuständigen DSK-Arbeitskreises Kreditwirtschaft an dem Treffen der Expert*innen teil. Sie vertritt zudem die Bundesländer auch in der zuständigen Arbeitsgruppe des Europäischen Datenschutzausschusses (EDSA) auf europäischer Ebene. So hat sie bereits Vorgaben für den Datenaustausch unter Zahlungsdienstleistern formuliert, die dazu geführt haben, dass der EDSA 2024 gemeinsam mit dem Europäischen Datenschutzbeauftragten (EDSB) eine Stellungnahme zu den EU-Gesetzesvorschlägen veröffentlicht hat. Das „Statement 2/2024 on the financial data access and payments package" ist abrufbar unter **www.edpb.europa.eu**.

Fazit

Die LDI NRW engagiert sich intensiv in der Bekämpfung von Betrug im Zahlungsverkehr. Dazu berät sie regelmäßig Vertreter*innen aus Bankenaufsicht, Verbraucherschutz, Kreditwirtschaft und weitere Interessengruppen zu datenschutzkonformen Maßnahmen und nimmt an entsprechenden Treffen teil.

11. Zertifizierungen



11.1. Zertifizierung: LDI NRW veröffentlicht neuen Frage-Antwort-Katalog plus Flyer

Eine Zertifizierung nach der DS-GVO bietet Unternehmen einen erheblichen Wettbewerbsvorteil. Sie belegen damit die Einhaltung der Datenschutzregeln und stärken so das Vertrauen von Kund*innen und Geschäftspartner*innen in ihre Datensicherheit. Auf dem Weg dahin helfen jetzt neue Hinweise der LDI NRW.

Tue Gutes und sprich darüber. Nach diesem alten Sprichwort funktioniert in etwa auch die Qualitätssicherung über eine datenschutzrechtliche Zertifizierung. Unternehmen, die personenbezogene Daten verarbeiten, lassen ihre Prozesse daraufhin überprüfen, ob sie Datenschutz-Standards entsprechen – und können im Erfolgsfall durch ein Zertifikat damit werben. Um Interessierten auf diesem sinnvollen Weg Hilfestellung zu leisten, hat die LDI NRW im vergangenen Jahr entsprechende Unterlagen erstellt, und zwar eine Aufstellung von häufig gestellten Fragen (FAQ – Frequently Asked Questions) und einen Kurzüberblick in Form eines Flyers.

Die FAQ richten sich dabei insbesondere auch an Verantwortliche und Auftragsverarbeiter, die sich erstmals mit der Möglichkeit einer DS-GVO-Zertifizierung befassen, aber auch an Antragsteller*innen von Zertifizierungsprogrammen. In leicht verständlicher Form werden zentrale Fragen beantwortet, unter anderem dazu, was eine Zertifizierung nach der DS-GVO bedeutet, welche Vorteile sie bietet, welche Stellen zertifizieren dürfen und wie ein solches Verfahren abläuft.

Ergänzend zu den FAQ fasst ein neu erstellter Flyer die wichtigsten Informationen zur DS-GVO-Zertifizierung kompakt und übersichtlich

zusammen. Der Flyer bietet einen schnellen Einstieg in das Thema und eignet sich besonders als erste Orientierung oder zur Weitergabe innerhalb von Organisationen. Er zeigt auf, für wen eine Zertifizierung sinnvoll sein kann und welche Schritte typischerweise auf dem Weg zur Zertifizierung erforderlich sind.

Mit den beiden Informationsangeboten soll das komplexe Thema der DS-GVO-Zertifizierung verständlich und praxisnah aufbereitet werden. Verantwortliche können so leichter einschätzen, ob und in welcher Form eine Zertifizierung für ihre Organisation in Betracht kommt. Eine Zertifizierung hilft ihnen, sie schafft Transparenz und Datenschutzkonformität bezüglich der eigenen Datenverarbeitung. Sie kann auch bei Kund*innen Vertrauen in die Datenverarbeitung schaffen.

Die FAQ sowie der Flyer sind unter www.ldi.nrw.de/zertifizierung abrufbar und können für Informations- und Schulungszwecke genutzt werden.

Fazit

Die neuen FAQ und der begleitende Flyer leisten einen wichtigen Beitrag zur Information rund um die DS-GVO-Zertifizierung. Sie bieten eine fundierte Orientierungshilfe für Organisationen, die sich mit dem Thema Datenschutz und Qualitätssicherung befassen. So können Verantwortliche informierte Entscheidungen treffen, ob eine Zertifizierung im Datenschutz für die eigene Organisation in Betracht kommt.

11.2. Datenschutz-Zertifizierung: Erfahrungen der LDI NRW sind europaweit gefragt

Wie schafft man verbindliche Datenschutz-Standards in Europa? Zertifizierungen spielen hier eine wichtige Rolle; die LDI NRW zählt auf diesem Gebiet europaweit zu den erfahrensten Datenschutzbehörden. Von ihrem Wissen profitieren nicht nur andere Aufsichtsbehörden – auch die Wirtschaft sucht den Austausch.

Zertifizierungen im Datenschutz setzen Maßstäbe. Sie haben zum Ziel, das Datenschutzniveau in einem Unternehmen transparent zu machen – sowohl für Vertragspartner*innen des Unternehmens als auch für die von der Datenverarbeitung betroffenen Personen. Zertifizierungen sind damit ein Gewinn für alle: Sie minimieren datenschutzrechtliche Risiken und verschaffen den beteiligten Unternehmen Wettbewerbsvorteile, da sie sich auf die Einhaltung von Standards berufen können.

Bei der Etablierung solcher Standards in Europa spielt die LDI NRW als besonders erfahrene Behörde auf diesem Gebiet eine wichtige Rolle.

Das hat sie auch im Jahr 2025 wieder bewiesen. Gemeinsam mit den Aufsichtsbehörden aus Schleswig-Holstein und dem Bund sowie dem EDSA hat die LDI NRW im Juni zu einem Workshop nach Berlin eingeladen, um die Datenschutz-Standards in Europa weiterzuentwickeln. Im Mittelpunkt stand dabei ein offener Dialog zwischen Datenschutzaufsicht und Wirtschaft. Vertreter*innen von Datenschutzaufsichtsbehörden aus 18 Mitgliedsstaaten und verschiedene Stakeholder*innen, insbesondere von Akkreditierungsstellen, Systembetreiber*innen und Zertifizierungsstellen, beteiligten sich daran.

Durch die Zertifizierung wird die Einhaltung der Datenschutzbestimmungen für bestimmte Verarbeitungsvorgänge bestätigt. Sie dient als Nachweis für die Konformität mit der DS-GVO und kann sowohl für Verantwortliche als auch für Auftragsverarbeiter relevant sein. Der Zertifizierungsprozess umfasst in der Regel eine detaillierte Prüfung der Verarbeitungsvorgänge durch die Zertifizierungsstelle. Dabei werden die technischen und organisatorischen Maßnahmen sowie die Einhaltung der DS-GVO-Prinzipien überprüft. Nach erfolgreicher Prüfung wird das Zertifikat erteilt, das in der Regel eine Gültigkeitsdauer von drei Jahren hat.

Ein wichtiges Ziel des Workshops war, die beteiligten Akteure am Markt, die Akkreditierungsstellen sowie die europäischen Aufsichtsbehörden besser zu vernetzen. Dabei wurde zugleich herausgearbeitet, wo genau die noch bestehenden neuralgischen Punkte im Bereich von Zertifizierung und Akkreditierung liegen. So ist etwa der Bekanntheitsgrad von DS-GVO-Datenschutzsiegeln bei betroffenen Personen noch erheblich verbesserungsbedürftig. Erkennbar wurde zudem, dass europaweit das Interesse von Unternehmen an einer datenschutzrechtlichen Zertifizierung durch ein Datenschutzsiegel gefördert werden muss. Neben eigenen Maßnahmen der Datenschutzaufsichten für mehr Bekanntheit von Datenschutzsiegeln hielten es die Teilnehmer*innen des Workshops deshalb für wichtig, dass europaweit ein optisch einheitliches Datenschutzsiegel nach DS-GVO zügig eingeführt wird. Dieses Anliegen soll deshalb erneut an die hierfür zuständige Europäische Kommission herangetragen werden, damit sie diese wichtige Maßnahme für die Erkennbarkeit eines DS-GVO-Datenschutzsiegels mit Nachdruck verfolgt.

Aus Sicht der LDI NRW wäre es zudem eine wichtige gesetzliche Weiterentwicklung, wenn ein europäisches Datenschutzsiegel auch für Produkte normiert würde, mit denen Daten verarbeitet werden. Bisher können nur Verfahren zertifiziert werden, in denen Daten konkret verarbeitet werden. Vielfach sind aber Probleme bereits in den Produkten angelegt, die für die Verarbeitung personenbezogener Daten auf dem Markt angeboten werden. Es wäre für die datenverarbeitenden Stellen ein enormer Vorteil, wenn sie für ihre Datenverarbeitung auf Produkte zurückgreifen könnten, deren Eignung für eine datenschutzgerechte Nutzung durch eine europäische Zertifizierung bestätigt ist. Teils entstehen für Unternehmen nämlich

deswegen Datenschutzprobleme, weil die Konfiguration der eingesetzten Produkte keine datenschutzkonforme Verarbeitung ermöglicht. Hier wäre es ein wichtiger Schritt für mehr Datenschutz in der Praxis, mit einem Siegel bereits auf Produktebene anzusetzen.

Fazit

Die LDI NRW hat ein Interesse daran, dass Unternehmen breite Möglichkeiten erhalten, ihre Datenverarbeitungsverfahren zertifizieren zu lassen. Das verbessert den Datenschutz in den Unternehmen und mindert dort das Risiko von Datenschutzverletzungen. Die LDI NRW setzt sich deshalb in Deutschland und Europa dafür ein, dass das Angebot an Zertifizierungsverfahren zunimmt. Weitere Informationen zur Zertifizierung nach DS-GVO sind abrufbar unter **www.ldi.nrw.de/datenschutz/wirtschaft/akkreditierungzertifizierung**.

11.3. Zertifizierung 3.0: Datenschutzkonferenz verbessert Rechtssicherheit für Unternehmen mit neuem Prüfkriterienpapier

Unternehmen, die Datenschutz-Zertifikate vergeben wollen, müssen bestimmte Voraussetzungen erfüllen. Dazu gehört auch die Vorlage eines Programms, in dem festgelegt wird, welche Kriterien für die Zertifizierung eine Rolle spielen. Die DSK hat nun die entsprechenden Vorgaben dafür überarbeitet und in einer Version 3.0 vorgelegt. Nicht nur künftige Zertifizierungsstellen sollten es kennen.

Unternehmen, die dokumentieren wollen, dass sie datenschutzrechtliche Standards einhalten, können dies durch eine Zertifizierung erreichen. Das entsprechende Zertifikat ist nicht nur deshalb von Vorteil, weil der Prozess zum Erwerb des Siegels dazu beiträgt, dass die internen Unternehmensabläufe auf einem rechtskonformen Niveau sind. Es kann darüber hinaus auch als Marketinginstrument gegenüber Verbraucher*innen oder Geschäftskund*innen ausgesprochen hilfreich sein.

Das Zertifikat wird dabei von bestimmten Stellen verliehen, die zuvor selbst eine Prüfung durchlaufen müssen (Akkreditierung). Zur Vorbereitung ihrer Akkreditierung müssen diese Unternehmen unter anderem ein Zertifizierungsprogramm erstellen und durch die Deutsche Akkreditierungsstelle GmbH (DAkkS) auf Eignung prüfen lassen. Wesentlicher Teil dieses Zertifizierungsprogramms sind die Kriterien, wie Unternehmen, die eine Zertifizierung anstreben, datenschutzrechtliche Anforderungen

umzusetzen haben. Diese Kriterien werden entweder von der zuständigen Datenschutzaufsichtsbehörde genehmigt oder dem EDSA zur Genehmigung übermittelt.

Bereits seit 2021 gibt die DSK, in der auch die LDI NRW vertreten ist, dazu ein Prüfkriterienpapier mit Anwendungshinweisen heraus. Im Dezember 2025 hat die DSK dieses Papier mit dem Titel „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme" nun überarbeitet und in der Version 3.0 verabschiedet. Es soll vor allem die Rechtssicherheit und Transparenz für interessierte Unternehmen weiter verbessern.

Bei der Zertifizierung nach Art. 42 der DS-GVO wird die Einhaltung der Datenschutzbestimmungen für bestimmte Verarbeitungsvorgänge bestätigt. Die deutschen Aufsichtsbehörden, die sich in der DSK abstimmen, haben schon früh damit begonnen, einheitliche Anforderungen an die Zertifizierungskriterien zu formulieren, so dass sich die zu akkreditierenden Zertifizierungsstellen schon bei der Erstellung ihrer Dokumente hierauf stützen können. Aber nicht nur für die Zertifizierungsstellen ist die Arbeit der DSK hilfreich. Auch den Unternehmen, die eine Zertifizierung anstreben, gibt das DSK-Papier im Vorfeld wichtige Hinweise.

Seit der ersten Version erlebt diese Hilfestellung der DSK zudem eine stetige Weiterentwicklung. Dabei stützt sich die DSK auf Erfahrungswerte, um die Umsetzung noch praktikabler zu machen, und nimmt zugleich auch eine vertiefte Auseinandersetzung mit den gesetzlichen Grundlagen auf europäischer Ebene vor. So finden sich in der neuen Version 3.0 nicht nur breitere, transparentere Anforderungen zum Thema Auftragsverarbeitung. Die neue Version bietet auch einen noch tieferen Einstieg in Fragen der Erforderlichkeit von technischen und organisatorischen Maßnahmen in Zertifizierungsprogrammen. Das neue Prüfkriterienpapier kann auf der Website der DSK heruntergeladen werden www.datenschutzkonferenz-online.de/anwendungshinweise.

Fazit

Das Prüfkriterienpapier 3.0 ist eine verbesserte Praxishilfe, nicht nur für die Erstellung eines Zertifizierungsprogramms, sondern für alle Unternehmen, die sich mit datenschutzrechtlichen Anforderungen auseinandersetzen. Das Papier zeigt, worauf es bei einer Prüfung ankommt, und kann somit – auch unabhängig von einem Zertifikat – eine wertvolle Hilfestellung bei der Ausgestaltung der eigenen datenschutzrelevanten Prozesse sein.

12. Wohnen

12.1. Codes of Conduct: So schaffen Wirtschaft und Aufsichtsbehörden Rechtssicherheit – am Beispiel der Messgeräteindustrie

Selbstverpflichtungen der Wirtschaft, sog. Codes of Conduct (CoC), bieten die Möglichkeit, die Anwendung von Datenschutzrecht passgenau für bestimmte Branchen festzulegen – sofern die zuständige Aufsichtsbehörde die Rechtskonformität bestätigt. Im vergangenen Jahr hat die LDI NRW einem Verband der Messgeräteindustrie eine solche Genehmigung erteilt.

Wenn es um „Smart Meter" – also intelligente Messgeräte zur Ermittlung des Gas- oder Wasserverbrauchs – geht, wird es datenschutzrechtlich sensibel. Denn bei Messungen individueller Verbräuche in Einzelhaushalten dringt die digitale Technik zunehmend in das private Umfeld ein. Auf der einen Seite ist das hilfreich, weil sich der Verbrauch so besser kontrollieren und steuern lässt. Auf der anderen Seite geht dies stets mit der Verarbeitung personenbezogener Daten einher, was möglicherweise nicht allen Verbraucher*innen gefällt.

Vor diesem Hintergrund hat die LDI NRW im vergangenen Jahr die selbst erarbeiteten Verhaltensregeln genehmigt – den sog. CoC – des Verbandes der Deutschen Wasser- und Wärmezählerindustrie (VDDW), der für Verbrauer*innen und Verband Sicherheit über eine datenschutzgerechte Datenverarbeitung herstellt. Er ist auf der Website des VDDW abrufbar unter **www.vddw.de/code-of-conduct**.

In diesem CoC stellt der Verband Verhaltensregeln auf, wie die eigene Branche mit personenbezogenen Daten bei der Entwicklung und dem Einsatz von Messgeräten für Kalt-/Warmwasser und thermische Energie umzugehen hat. Vorausgegangen war eine Abstimmung über den CoC innerhalb der DSK, dem Zusammenschluss der Aufsichtsbehörden von Bund und Ländern. So konnten noch Anpassungen vorgenommen werden, die aus Sicht anderer Datenschutzbehörden zur Klarstellung der richtigen Rechtsanwendung dienten.

Wie aber schützt dieser neue CoC nun die Verbraucher*innen? Zunächst: Er gilt für alle Mitgliedsunternehmen des VDDW, die nicht nur Gerätehersteller sind, sondern auch im Auftrag von Versorgungsunternehmen für diese Daten verarbeiten, also die Messgeräte betreiben. Reine Gerätehersteller können die im CoC aufgeführten technischen Maßgaben aber bei der Herstellung berücksichtigen. Dies liefert einen großen Beitrag dazu, datenschutzkonforme Geräte auf den Markt und zum Einsatz zu bringen.

Bei der Prüfung des CoC lag der Fokus der LDI NRW zudem darauf, die komplexe Datenverarbeitung mit Hilfe von Smart Metern transparent zu machen. So ist zu Beginn der „Technischen Maßgaben" – im Anhang des CoC – der Verarbeitungsprozess in einem Schaubild genau aufgeschlüsselt. Zu jedem Verarbeitungsschritt werden dann nach einem einheitlichen Schema weitere Erläuterungen gegeben. Hierzu gehören die Aufzählung der Rechtsgrundlagen, die Begrenzung der verarbeiteten Daten auf den für den jeweiligen Zweck maßgeblichen Umfang, Speicherzeiträume sowie Gerätesicherheit und Zugriffsschutz. Vereinfacht gesagt geht es darum, wie oft, von wem und zu welchem Zweck die Daten über Smart Meter ausgelesen werden, wann sie gelöscht werden und wie sie vor unbefugtem Auslesen geschützt werden. Das gibt auch Verbraucher*innen Sicherheit, was mit ihren Daten passiert.

Wenn sich ein Wirtschaftsverband Verhaltensregeln gibt, muss er auch eine Stelle vorsehen, die die Einhaltung der Regeln durch die Mitgliedsunternehmen überwacht. Außerdem muss diese Überwachungsstelle auch ein Beschwerdeverfahren für betroffene Verbraucher*innen einrichten. Der Verband VDDW hat sich dazu entschieden, eine externe Überwachungsstelle mit dieser Aufgabe zu betrauen. Diese Stelle wird noch von der zuständigen Datenschutzaufsicht zu akkreditieren sein. Die LDI NRW hat hierzu bereits erste Beratungsgespräche geführt. Die betroffenen Unternehmen können die Regelungen des CoC aber auch schon einhalten, wenn die Überwachungsstelle noch nicht arbeitet.

Was die Verbraucher*innen-Rechte anbelangt, so wenden sich Bürger*innen, die etwas über ihre Daten erfahren wollen, an das datenschutzrechtlich verantwortliche Versorgungsunternehmen, von dem sie ihr Wasser oder die thermische Energie beziehen. Das Unternehmen muss den Anfragenden zur Funktionalität und zum Datenverarbeitungsprozess nachvollziehbare Informationen vermitteln. Im CoC ist nun geregelt, dass die Hersteller der Smart Meter den Versorgungsunternehmen die

notwendigen Informationen für die anfragenden Verbraucher*innen geben müssen. Geschieht dies nicht, können sich Verbraucher*innen an die spezielle Überwachungsstelle wenden. Zwar bleibt die LDI NRW auch weiterhin als Datenschutzaufsicht Ansprechpartnerin für betroffene Verbraucher*innen. Oft werden die betrieblichen Datenschutzbeauftragten der Versorger oder die Überwachungsstelle aber schneller helfen können.

Niemand sollte im Übrigen Sorge haben, dass der Staat über Smart Meter den Energieverbrauch von Einzelpersonen kontrollieren und steuern will. Im staatlichen Interesse ist es, die Versorgungssicherheit zu gewährleisten. Dazu können Smart Meter beitragen. Dabei geht es aber nicht um die Kontrolle der Verbraucher*innen. Vielmehr sollen diese mit einem intelligenten Messsystem ihren Verbrauch selbst besser im Blick halten können, um ihr eigenes Einsparpotenzial zu erkennen und nutzen zu können.

Der CoC kompensiert auch ein gesetzliches Vakuum. Anders als beim Energieverbrauch gibt es für den Kaltwasserbereich keine spezifischen gesetzlichen Vorgaben zum Umgang mit personenbeziehbaren Daten. Die Datenschutzaufsichtsbehörden fordern seit einiger Zeit bereits ein spezielles Gesetz auch für diesen Bereich. Nach Angaben des VDDW ist dieser darauf vorbereitet und würde entsprechende Anpassungen am CoC vornehmen.

Fazit

Der CoC ist ein wichtiger Schritt für mehr Rechtssicherheit bei fernauslesbaren Smart Meter. Das Instrument des CoC sollte von Branchenverbänden, die Sicherheit über die richtige Anwendung der DSGVO durch ihre Mitglieder herstellen wollen, intensiv genutzt werden.

12.2. Weitergabe von Mieter*innendaten an Sozialbehörden? In bestimmten Notsituationen ist das erlaubt.

Sind Mieter*innen länger mit der Miete im Rückstand, stehen Wohnungskündigung und Räumung bevor. Im schlimmsten Fall droht die Obdachlosigkeit, wenn der Staat nicht finanziell einspringt. Dürfen Vermieter*innen in dieser Situation die Daten der Mieter*innen an die Sozialbehörden übermitteln, um die kritische Lage abzufedern? Eine schwierige Frage, auf die die LDI NRW eine Antwort hat.

Der Wohnungsmarkt in Deutschland gestaltet sich für Bürger*innen zunehmend schwierig. Nicht nur, dass es viel zu wenig bezahlbaren Wohnraum gibt. Die persönliche und insbesondere finanzielle Lebenssituation

vieler Bürger*innen gestaltet sich auch zunehmend prekär. Mieter*innen sind dann mitunter nicht mehr in der Lage, ihre Miete zu bezahlen. Die Folge: ihnen droht mit der Kündigung wegen anhaltender Mietrückstände eine Räumungsklage, an deren Ende die Obdachlosigkeit stehen kann. Zwar ist es den Ordnungsbehörden möglich – wenn ihnen keine andere Mittel zur Verfügung stehen –, die Wiedereinweisung in die bisherige Wohnung anzuordnen. Allerdings gelingt das nicht immer, insbesondere dann nicht, wenn die Behörden erst zu einem späten Zeitpunkt von der konkreten Gefahrenlage erfahren. Damit stellt sich die Frage, ob die Vermieter*innen in solchen Situationen vorzeitig eingreifen dürfen. Konkret: ob sie bereits frühzeitig die Sozialbehörden über die kritische Lage informieren dürfen.

Die LDI NRW hat sich anlässlich mehrerer Fälle und Anfragen ausgiebig mit dem Thema beschäftigt. Und sie hat Kriterien aufgestellt, die erfüllt sein müssen, damit die Datenweitergabe legal möglich ist.

Zu Beurteilung der Rechtslage ist zunächst wichtig, die Phasen eines Räumungsverfahrens zu kennen. Das besteht in der Regel aus: dem Androhen einer Kündigung, dem Aussprechen der Kündigung, dem Durchführen der Räumungsklage, die eine Mitteilungspflicht des Gerichts an das Sozialamt/Jobcenter auslöst, der zweimonatigen Heilungsfrist, der Güteverhandlung vor Gericht, dem Räumungsurteil, der Räumungsfrist, der Einschaltung der*des Gerichtsvollziehers*in und dem ersten und ggfs. weiteren Räumungstermin/en. Die Mitteilung durch die Gerichte an die Sozialbehörden erfolgt dabei in einer sehr späten Phase, in der eine erfolgversprechende Prävention vor Obdachlosigkeit im Wege der Wohnungssicherung häufig nicht mehr möglich ist. Zumeist ist das Mietverhältnis zu diesem Zeitpunkt auch bereits so zerrüttet, dass bei Vermieter*innen keine Bereitschaft mehr zur Fortsetzung des Vertragsverhältnisses besteht.

In vielen Kommunen gibt es schon jetzt Projekte, die von den Sozialbehörden oder -einrichtungen betrieben werden, um in Kooperation mit großen Wohnungsbauunternehmen Obdachlosigkeit rechtzeitig zu verhindern. In diesen Projekten geht es unter anderem darum, sog. passive Mieter*innen vor Wohnungsnot zu schützen, die aufgrund von psychischen oder körperlichen Erkrankungen oder aus Scham nicht in der Lage sind, ihre eigenen Angelegenheiten zu bewältigen. Der Gedanke dahinter: Die Sozialbehörden oder -einrichtungen sollen durch Vermieter*innen, die – trotz ausbleibender Miete und des Vorliegens eines Kündigungsgrundes – an der Fortsetzung des Mietverhältnisses interessiert sind, bereits vor einer Kündigungsklage von der drohenden Obdachlosigkeit erfahren, damit sie auf die Mieter*innen mit Angeboten zugehen zu können. Sofern die Mieter*innen dann im Antragsverfahren mitwirken kann eine staatliche Unterstützung zur Mietzahlung und zu Mietrückständen geprüft und in vielen Fällen so die Fortsetzung der Mietverhältnisse erreicht werden.

Solche Projekte berühren allerdings datenschutzrechtliche Fragen, vor allem, weil die Vermieter*innen dabei personenbezogene Informationen weiterleiten. Insofern interessiert sowohl die Mieter*innen und Vermieter*innen als auch die Sozialbehörden, ob dieser Austausch von Daten überhaupt zulässig ist.

Was gilt für Datenverarbeitung durch die Sozialbehörden?

Für eine zulässige Datenübermittlung durch Vermieter*innen an Sozialbehörden bedarf es zunächst einer Befugnis der Behörde, Daten überhaupt erheben zu dürfen. Diese leitet sich aus dem sog. „Kenntnisgrundsatz" im Sozialrecht ab. Die Sozialbehörden werden nach § 15 Abs. 1 Sozialgesetzbuch (SGB) XII nicht erst auf Antrag, sondern bereits bei Kenntnisnahme von einer drohenden Notlage tätig – unabhängig davon, von wem diese Kenntnis kommt. Die Information, die die Sozialbehörde über einen drohenden Wohnungsverlust erhält, öffnet ihr damit die Tür für das Beratungsangebot an die betroffene Person („Türöffnerfunktion") und für anschließende Maßnahmen zur Abwendung der Obdachlosigkeit, etwa durch das Anstoßen eines Sozialhilfeantrags. Wird bei der Beratung festgestellt, dass es sich um eine Person handelt, die Anspruch auf Bürgergeld hat, kann die Sozialbehörde ebenfalls notwendige Anträge anregen und – sofern sie die Aufgabe nicht selbst wahrnimmt – der zuständigen Stelle zuleiten. Die Sozialbehörden haben also nach §§ 15 und 18 SGB XII auch außerhalb von Antragsverfahren die Berechtigung zur Erhebung von personenbezogenen Daten, um drohende Notfälle abzuwenden. Eine Datenerhebungsbefugnis besteht somit.

Was gilt für die Datenverarbeitung durch Vermieter*innen?

Vermieter*innen dürfen Daten säumiger Mieter*innen allerdings nicht ohne Weiteres an die Sozialbehörden übermitteln. Die Information, dass eine bestimmte Person ihre Miete nicht mehr zahlt und kurz vor der Wohnungsräumung und damit möglicherweise vor einer Obdachlosigkeit steht, ist sehr sensibel. Vermieter*innen können Daten nur dann übermitteln, wenn dies im berechtigten eigenen Interesse oder dem berechtigten Interesse eines Dritten liegt und nicht Interessen der betroffenen Person am Schutz ihrer Grundrechte und ihrer Daten überwiegen (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO).

Berechtigte Interessen der Vermieter*innen bestehen – und zwar an einer ungestörten Zahlung der Miete ohne Konflikt, an einem Hausfrieden ohne Räumungsunruhe, an einer geringen Mieter*innen-Fluktuation sowie an der Einsparung von Verfahrenskosten infolge Kündigung. Diesen Interessen kann durch ein mögliches Eintreten der Sozialbehörden in

Mietzahlungen und die Übernahme von Mietrückständen Rechnung getragen werden. Im Verhältnis dazu sind die Interessen der betroffenen Person zu gewichten, dass keine sensiblen Daten – Mietzahlungsverzug, drohende Wohnungskündigung – an eine staatliche Stelle übermittelt werden. Schließlich könnten auch Fehlmeldungen passieren, die dem Ansehen der betroffenen Person schaden. Allerdings kann auch das zu vermutende eigene Interesse der Mieter*innen daran, nicht obdachlos zu werden, im Rahmen der Interessenabwägung betrachtet und gewichtet werden.

Es muss jedenfalls geprüft werden, ob die Datenübermittlung an das Sozialamt auch erforderlich ist, um das damit verbundene Ziel zu erreichen – nämlich die Übernahme der Mietzahlung durch das Sozialamt und damit das Behalten der Wohnung durch den*die Mieter*in.

Nicht erforderlich ist etwa eine Kontaktaufnahme der Vermieter*innen mit den Sozialbehörden, wenn die Vermieter*innen bereits Kenntnis darüber haben, dass die Mieter*innen selbst in Kontakt zur Sozialbehörde wegen der säumigen Mietzahlungen stehen. Sofern die Mieter*innen bereits selbst den Mietvertrag gekündigt haben, kommt eine Mitteilung an die Sozialbehörde durch die Vermieter*innen ebenfalls nicht in Betracht. Gleiches gilt, wenn die Zahlungsrückstände erkennbar nicht auf einer sozialen Notlage der Mieter*innen beruhen, sondern es sich beispielsweise um eine zwischen den Parteien umstrittene Mietminderung handelt. Bei diesen Sachlagen ist eine Unterstützung der Sozialbehörden zur Fortsetzung des Mietverhältnisses nicht möglich bzw. nicht erforderlich. Etwaige ausstehende Mietzahlungen können in diesen beiden Fällen nur zivilrechtlich durchgesetzt werden. Sollten Vermieter*innen feststellen, dass örtliche Sozialbehörden aufgrund von Hinweisen von Vermieter*innen nicht tätig werden, sind schließlich weitere Datenübermittlungen an die Behörden zu unterlassen.

Diese Sachlage zeigt, dass die Datenweitergabe durch Vermieter*innen an enge Grenzen stößt. Mit Blick auf das übergeordnete Ziel – die Vermeidung einer drohenden Obdachlosigkeit – erscheint der LDI NRW eine Datenübermittlung an die Sozialbehörden unter bestimmten Voraussetzungen vertretbar. Andere Datenschutzaufsichtsbehörden sehen das anders. Sie sprechen sich für eine explizite Regelung durch den Gesetzgeber aus. Auch die LDI NRW spricht sich für eine Regelung durch den Gesetzgeber aus, um Rechtsunsicherheiten zu klären. Diesbezüglich stehen die Aufsichtsbehörden weiter im Austausch.

In der Zuständigkeit der LDI NRW gelten die folgenden Überlegungen, zur Zulässigkeit einer Datenübermittlung nach Art. 6 Abs. 1 UAbs 1 lit. f DS-GVO.

Diese Voraussetzungen müssen zwingend erfüllt sein

Vermieter*innen dürfen sich wegen des Ausbleibens der Mietzahlung an die zuständige Sozialbehörde wenden und

- Name und Anschrift der Mieter*innen und
- Informationen zur bevorstehenden Kündigung übermitteln,

wenn die folgenden Bedingungen erfüllt sind:

- Die Voraussetzungen zur außerordentlichen Kündigung wegen Nichtzahlung der Miete liegen vor.
- Die Vermieter*innen haben die Mieter*innen zuvor darauf hingewiesen, dass sie sich an die Sozialbehörde wenden werden, wenn die Mietzahlungen weiter ausbleiben. Dabei haben die Vermieter*innen darauf hingewiesen, dass die Mieter*innen dem innerhalb einer angemessenen Frist (mindestens zwei Wochen) widersprechen können. Dies kann etwa in einem Mahnschreiben geschehen.
- Die Mieter*innen haben dem nicht innerhalb der gesetzten Frist widersprochen.
- Die Vermieter*innen haben die Mieter*innen konkret aus Anlass des Zahlungsverzugs über staatliche Hilfsangebote mindestens einmal informiert und dies dokumentiert. Die Information kann etwa mit einem Flyer und auch mit einem Mahnschreiben geschehen.
- Die Vermieter*innen dürfen aufgrund ihnen bekannter Tatsachen annehmen, dass eine Information der zuständigen Sozialbehörde geeignet sein kann, die Mieter*innen vor einer drohenden Obdachlosigkeit infolge der aufgelaufenen Mietrückstände zu bewahren.
- Die Vermieter*innen wissen nicht, dass die ausbleibenden Zahlungen nicht mit einer sozialen Notlage in Zusammenhang stehen.
- Die Vermieter*innen wissen nicht, dass es zu einer eigenständigen Kontaktaufnahme der Mieter*innen mit dem Sozialamt gekommen ist.
- Die Vermieter*innen wissen nicht, dass den Mieter*innen bereits eine andere Wohnung zur Verfügung oder in Aussicht steht.
- Sollten die Vermieter*innen feststellen, dass örtliche Sozialbehörden aufgrund von Hinweisen von Vermieter*innen nicht tätig werden, sind weitere Datenübermittlungen an diese zu unterlassen.

Fazit

Im Interesse von guten Lösungen für beide Mietparteien ist es unter engen Voraussetzungen zulässig, wenn Vermieter*innen Daten über säumige Mieter*innen an die Sozialbehörden weiterleiten. Angesichts von verbleibenden Rechtsunsicherheiten wäre aber eine gesetzgeberische Lösung zu begrüßen. Die LDI NRW hat deshalb dem Ministerium für Arbeit, Gesundheit und Soziales NRW empfohlen, die Bundesregierung auf den Bedarf für eine entsprechende Regelung hinzuweisen. Die LDI NRW würde eine Bundesratsinitiative aus NRW begrüßen.

13. Videotechnik

13.1. Spielhallen überprüft – LDI NRW gibt Hinweise zur Videoüberwachung im Außenbereich

Betreiber*innen von Spielhallen haben ein berechtigtes Interesse daran, im Inneren der Spielhallen Videoüberwachung zu ihrem eigenen Schutz und dem ihrer Mitarbeiter*innen einzusetzen. Aber wie weit darf die Überwachung draußen vor der Tür gehen? Die LDI NRW hat 38 solcher Hallen überprüft – und klare Regeln aufgestellt.

Ein Blick in die Lokalnachrichten genügt, um zu erkennen: Spielhallen sind ein häufiges Ziel von Raubüberfällen. Die oftmals hohen Bargeldbestände locken Kriminelle an, die auf schnelles Geld aus sind. Um den Anreiz für Überfälle zu verringern, sehen die Unfallverhütungsvorschriften „Überfallprävention" der Deutschen Gesetzlichen Unfallversicherung deshalb den Einsatz von Kameras in gewissen Bereichen einer Spielhalle vor.

Was manch ein*e Betreiber*in allerdings nicht weiß: Ob eine Videoüberwachung zulässig ist und wie weit sie gehen darf, ergibt sich nicht aus Unfallverhütungsvorschriften, sondern aus dem Datenschutzrecht, der DS-GVO. Und wenn es um den Außenbereich der Hallen geht, gelten besonders strenge Regeln. Um zu überprüfen, wie weit die Erkenntnisse auf diesem Gebiet und ihre Umsetzung in der Branche fortgeschritten sind, hat die LDI NRW deshalb im vergangenen Jahr insgesamt 38 Spielhallen in ganz NRW angeschrieben und gebeten, Auskunft über die Überwachung ihres Außenbereichs zu geben. Das Ergebnis: es gibt Verbesserungsbedarf.

Rechtsgrundlage für eine Videoüberwachung in einer Spielhalle ist Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO. Danach ist die Verarbeitung von personenbezogenen Daten zulässig, wenn sie „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" ist und „sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen". Den Interessen von Kindern ist dabei besonders Rechnung zu tragen. Dies ist bei Spielhallen ein wichtiger Aspekt. Denn von einer Videoüberwachung im Außenbereich sind auch Passant*innen und Kinder betroffen, die jeweils keinerlei Bezug zum Spielhallenbetrieb haben. Deren Interessen kommt daher besonderes Gewicht zu. Sie haben das Recht, sich im öffentlichen Raum grundsätzlich frei und unbeobachtet zu bewegen. Hier muss durch die Spielhallenbetreiber*innen genau geprüft werden, inwiefern die Überwachung wirklich erforderlich ist und ob die Interessen der Betroffenen am Ausschluss einer Videoüberwachung nicht überwiegen.

Die Prüfung der LDI NRW unter den Betreiber*innen ergab dazu folgendes Bild: Neun Spielhallen setzten eine Außenbereichsüberwachung ein. Diese betraf die öffentliche Straße und Bürgersteige sowie Bereiche vor dem Eingang zur Spielhalle und den Parkplatz. Bei acht von neun Spielhallen gab es Verbesserungsbedarf, und zwar bei der Begrenzung des Erfassungsbereiches und/oder der Hinweisbeschilderung. Bei drei Spielhallen wurde sogar die Abschaltung einzelner Kameras verlangt und durchgesetzt.

Dabei ist die Aufnahme des Eingangsbereichs als Zutrittskontrolle wegen der abstrakten Gefahr, der Spielhallen unterliegen, in der Regel datenschutzrechtlich nicht zu beanstanden. Gleichwohl reicht es hierfür aus, wenn lediglich der Eingang sowie ein kleiner Bereich davor gefilmt wird (maximal ein Meter). Die Aufnahme weiter Teile der öffentlichen Straße sowie des Bürgersteigs ist ebenfalls nicht erforderlich und damit unzulässig. Auf dem Parkplatz einer Spielhalle kann nicht automatisch von einer erhöhten Gefahr ausgegangen werden. Diese erhöhte Gefahr ist aber Voraussetzung für eine zulässige Überwachung. Sie muss gegebenenfalls durch die Spielhallenbetreiber*innen nachgewiesen werden.

Wie so oft mangelte es schließlich an einer rechtmäßigen Hinweisbeschilderung. Ein Piktogramm mit einem Kamerasymbol ist nicht ausreichend. Vielmehr sind die in Art. 13 DS-GVO genannten Informationen wie etwa die verantwortliche Stelle, die Rechtsgrundlage, die Zwecke und die Speicherdauer der Datenverarbeitung den Betroffenen mitzuteilen, bevor sie den Erfassungsbereich der Kamera betreten. Weitergehende Informationen und ein Muster für Hinweisschilder sind abrufbar unter **www.ldi.nrw.de/datenschutz/videoueberwachung**.

Fazit

Trotz erhöhter Gefahren wegen hoher Bargeldbestände: Betreiber*innen von Spielhallen müssen bei einer Videoüberwachung genau darauf achten, dass sie im Außenbereich ihrer Spielhalle nicht mehr aufnehmen, als es für ihre Zwecke erforderlich ist. Darüber hinaus ist eine aussagekräftige Hinweisbeschilderung unerlässlich.

13.2. Keine private Videoüberwachung gegen allgemeine Kriminalität

Das Bedürfnis, Bürger*innen vor kriminellen Übergriffen zu schützen, ist verständlich. Wer dazu Videoüberwachung einrichten will, darf den gesetzlich erlaubten Rahmen aber nicht überschreiten. Eine privatrechtliche Gesellschaft, an der eine Stadt beteiligt ist, musste deshalb die Videoüberwachung eines öffentlichen Platzes stoppen.

Gerade in Großstädten entstehen immer wieder Probleme an öffentlichen Plätzen. Schlechte Beleuchtung, uneinsehbare Ecken und die Anonymität durch eine Vielzahl von Passant*innen erzeugen schnell ein Gefühl von Unsicherheit. Hinzu kommen tatsächliche kriminelle Vorgänge wie Drogendelikte, Vandalismus oder Diebstähle. Manche kommunale Verantwortliche wünschen sich deshalb die dauerhafte Überwachung solcher Bereiche. Allerdings kann die konkrete Ausgestaltung der Videoüberwachung schnell zu einem Fall für die Datenschutzaufsicht werden – wie ein Vorgang zeigt, mit dem sich die LDI NRW 2025 auseinanderzusetzen hatte.

Dabei ging es um einen öffentlich zugänglichen, stark frequentierten Platz in einer Großstadt. An dem Platz liegen unter anderem ein Wohn- und Geschäftszentrum sowie zwei Kindergärten. Um hier mehr Sicherheit zu gewährleisten, ließ eine privatrechtliche Gesellschaft, die Eigentümerin des Platzes ist, den Bereich durch einen Dienstleister, einen sog. Auftragsverarbeiter, videoüberwachen. Dazu hatte sie zwei Videotürme, die mit je vier Kameras ausgestattet waren, sowie eine weitere Einzelkamera installieren lassen. Damit wurden drei Schwerpunktbereiche rund um die Uhr überwacht. Zwecke der Videoüberwachung waren Abschreckung, die Gewährleistung der erhöhten Sicherheit aufgrund von Drogenkriminalität, der Schutz vor Einbruch, Diebstahl und Vandalismus sowie die Erfassung von strafrechtlich relevantem Verhalten. Solche Aufnahmen sollten an die Polizei weitergeleitet werden. Die Videodaten wurden durch den Auftragsverarbeiter stündlich gesichtet, 48 Stunden lang gespeichert und anschließend gelöscht. Eine Audioaufzeichnung, Weiterleitung an Dritte oder Verbreitung im Internet erfolgte nicht. An allen Zugangsbereichen des Platzes wiesen Schilder auf die Videoüberwachung hin. Die Videoüberwachung war zunächst testweise für drei bis sechs Monate geplant.

Zur Begründung trug die Gesellschaft gegenüber der LDI NRW Folgendes vor: auf dem Platz gebe es seit mehreren Jahren kriminelle Aktivitäten, die Polizei und das Ordnungsamt der Stadt seien personell nicht in der Lage, eine ständige Bestreifung des Platzes zu gewährleisten. Alternativen zur Videoüberwachung seien geprüft und aus wirtschaftlichen Gründen verworfen worden. Durch die Videoüberwachung des Platzes sei es im Übrigen zu einem Rückgang der Drogenkriminalität gekommen. Nach eigenen Angaben wollte die für die Videoüberwachung verantwortliche Gesellschaft anstelle der Polizei für Sicherheit sorgen.

Gerade darin liegt jedoch eine grundsätzliche Fehlvorstellung, wenn es um die Überwachung öffentlicher Orte geht. Kurz gesagt: Öffentlich zugänglicher Raum kann überwacht werden – aber in der Regel nur durch Polizei und Ordnungsbehörden.

Darüber klärte die LDI NRW die Stadt auf und hörte die verantwortliche Gesellschaft zu einer von der LDI NRW beabsichtigten Anordnung an, die Videoüberwachung des Platzes unverzüglich einzustellen und gespeicherte Aufnahmen irreversibel zu löschen. Auch beabsichtigte die LDI NRW, die Anordnung für sofort vollziehbar zu erklären, da ansonsten bis zur Rechtskraft der Entscheidung ein nicht länger hinzunehmender rechtswidriger Zustand mit Auswirkungen auf die Rechte aller dort tagtäglich passierenden Personen fortbestehen würde.

Grundsätzlich gilt: Auch wenn – wie in diesem Fall – die für die Videoüberwachung verantwortliche Gesellschaft Eigentümerin des Platzes ist, kann sie ihre Videoüberwachung nicht auf die Rechtsgrundlage eines berechtigten Interesses gemäß Art. 6 Abs. 1 UAbs 1 lit. f DS-GVO stützen. Danach ist eine Datenverarbeitung zulässig, sofern die Verarbeitung „zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich" ist und nicht „die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt."

Zwar ist durchaus ein berechtigtes Interesse darin zu sehen, Eigentum und andere Rechtsgüter gegen kriminelle Übergriffe zu schützen. Da ein öffentlicher Platz aber von einer Vielzahl von Personen ständig genutzt und betreten wird, ist das Interesse der Eigentümerin gegen die Interessen dieser Personen abzuwägen. Dabei ist zusätzlich zu bedenken, dass die Mehrzahl dieser Personen überhaupt keinen Anlass für eine Aufzeichnung ihres Verhaltens gegeben hat. In diesem Fall überwiegen deren Rechte, sich in der Öffentlichkeit unbeobachtet bewegen zu können. Dies gilt umso mehr, wenn es sich um Kinder handelt. In dem konkreten Fall liegen gleich zwei Kindergärten an dem Platz. Überdies ist es keine Aufgabe von privaten Stellen, die allgemeine Sicherheit für eine unbestimmte Vielzahl von Personen auf einem für jeden zugänglichen Platz in exponierter Lage zu gewährleisten. Es handelt sich um ein Interesse der Allgemeinheit, nicht um das Interesse bestimmter Dritter. Die Abwägung zwischen

den Interessen der Verantwortlichen und den Interessen der von der Videoüberwachung Betroffenen führte folglich zu dem Ergebnis, dass deren Interessen überwiegen, nicht von der Videoüberwachung erfasst zu werden.

Der Fall zeigt damit ein grundsätzliches Missverständnis auf: Videoüberwachung durch Private verlangt eine sorgfältige Abwägung von Interessen – und der Schutz der Öffentlichkeit im öffentlichen Raum (Gefahrenabwehr und Strafverfolgung) und die dafür erforderliche Datenverarbeitung sind keine Privatsache, sondern per Gesetz den Strafverfolgungsbehörden, namentlich der Polizei und den Staatsanwaltschaften, sowie den Ordnungsbehörden zugewiesen. Private Stellen sind nicht dazu legitimiert, allgemeine Aufgaben der Gefahrenabwehr oder Strafverfolgung wahrzunehmen. Da in dem konkreten Fall das kriminelle Potenzial auf dem Platz nicht derartig gewichtig ist, dass die für eine polizeiliche Videoüberwachung erforderlichen Voraussetzungen eines sogenannten Kriminalitätsschwerpunkts gegeben wären, kann erst recht nicht eine private Stelle im öffentlichen Raum die Gefahrenabwehraufgaben übernehmen.

Nach Abschluss der Testphase hat die Verantwortliche die Videoinstallation bereits freiwillig beendet. Außerdem hat die LDI NRW auf Einladung der Stadt eine Ortsbegehung vorgenommen. Diese hat ergeben, dass zwar keine personenscharfe Überwachung der für den allgemeinen Verkehr geöffneten Flächen zulässig ist. In bestimmten Randbereichen sind allerdings Sachverhalte denkbar, die zum Schutz der berechtigten Interessen der Gesellschaft als Eigentümerin des Platzes und von Bewohner*innen und Nutzer*innen der Gebäude in einem engen Rahmen eine Videoüberwachung als zulässig erscheinen lassen. Die Gesellschaft, in deren Eigentum der Platz steht, wird den Sachverhalt aufgrund der Hinweise der LDI NRW noch einmal prüfen und gegebenenfalls ein neues Konzept erstellen.

Fazit

Private Stellen dürfen öffentlichen Raum nicht videoüberwachen, um Passant*innen vor allgemeiner Kriminalität zu schützen. Das ist Aufgabe von Polizei und Ordnungsbehörden.

13.3. Türkontrolle per Smartphone: Ohne Einwilligung der Mieter*innen geht es nicht

Die Digitalisierung hält Einzug – auch beim Wohnen. Immer häufiger setzen Vermieter*innen auf digitale Klingelanlagen und Zutrittskontrollsysteme, die etwa mit den Smartphones von Mieter*innen verbunden werden. Dabei werden allerdings meist personenbezogene Daten der Mieter*innen verarbeitet – und das kann rechtliche Probleme mit sich bringen.

Die Welt wird smarter. Neben der digitalen Steuerung von Strom- und Gasverbrauch sowie diverser Haushaltsgeräte gehören mittlerweile auch Türklingeln zum „schlauen" Wohnen, bei denen Klingeln und Türkameras mit Smartphones oder anderen Geräten verbunden werden. Doch deren Einsatz ist nicht nur eine Frage der Technik, sondern wird auch zur datenschutzrechtlichen Herausforderung, wenn Vermieter*innen von Wohngebäuden solche Systeme einführen wollen.

Fürsprecher*innen führen gern innovative und fortschrittliche Verbesserungen für die Nutzer*innen an. Smarte Türöffnungslösungen versprächen mehr Sicherheit und höheren Wohnkomfort. Dem gegenüber stehen allerdings grundlegende Fragen des Datenschutzes. Welche personenbezogenen Daten der Bewohner*innen werden für die smarte Türklingel verarbeitet, und wo werden diese von wem gespeichert? Werden Mieter*innen über überraschende Datenwege vorab informiert und haben diese zuvor in die Datenverarbeitung eingewilligt?

Die LDI NRW hat sich 2025 intensiv mit diesen Themen beschäftigt. Besonders kritisch wird es, wenn durch derartige Systeme die Besuchshäufigkeit bei den Mieter*innen erfasst werden kann.

In einem konkreten Fall hatte sich der Mieter einer Wohnanlage bei der LDI NRW über die neue Klingelanlage beschwert. Er sorgte sich um den Schutz seiner personenbezogenen Daten, zumal er vorher keine Einwilligung zur Nutzung der Daten erteilt hatte. Diese Sorge war begründet, entschied die LDI NRW.

Bei dem eingesetzten Zutrittskontrollsystem wurde das Signal nicht mehr über einen herkömmlichen gebäudeinternen Klingeldraht geleitet. Vielmehr wurde nach dem Klingeln eine Verbindung zum örtlichen Mobilfunknetz aufgebaut und die Smartphones oder Festnetzgeräte der Bewohner*innen wurden angewählt. Anschließend konnte die Haustür per Tastendruck über das Endgerät der Bewohner*innen geöffnet werden. Optional konnte dazu auch eine entsprechende App verwendet werden.

In Zuge dieses Datenverarbeitungsvorgangs wurden Namen und Telefonnummern der Mieter*innen in das System der Anlage eingepflegt. Die hinterlegten Daten, die mit der jeweiligen Klingel verknüpft waren, mussten bei jedem Klingelvorgang mit den personenbezogenen Daten und dem zugehörigen Endgerät der Bewohner*innen abgeglichen werden. Die Ermittlungen der LDI NRW ergaben zudem, dass die personenbezogenen Daten temporär auf Servern der Produktanbieterin gespeichert wurden. Darüber hinaus wurden – im Falle der Nutzung der zugehörigen App – zusätzlich Mobilfunknummern, Ereignishistorien, Standorte, Nutzer*innenaktionen, IP-Adressen und technische Informationen des Telefons für sieben Tage gespeichert. Dass aus diesen Daten mögliche Besuchsprofile der Mieter*innen hätten erstellt werden können, stufte die LDI NRW als besonders problematisch ein.

Durch die umfangreiche Datenspeicherung sollte unter anderem ein erweiterter Service für die App-Nutzer*innen realisiert werden. Eine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten war allerdings nicht ersichtlich. Hinzu kam: die Vermieterin hatte die Bewohner*innen weder rechtzeitig und transparent über diese komplexen Datenverarbeitungsprozesse informiert, noch bei ihnen die entsprechenden Einwilligungen für die Datenverarbeitung eingeholt.

Die LDI NRW entschied daher, dass die aufgezeigte Datenverarbeitung gegen das Datenschutzrecht verstößt. Allerdings dürfen nicht alle digitalen Klingelanlagen gleich beurteilt werden. Sofern etwa nur Bilder der Klingelnden kurzzeitig über eine lokale Anlage in die Wohnung übertragen werden, ist das als grundsätzlich unproblematisch anzusehen.

Im konkreten Fall wurde die Vermieterin angewiesen, entsprechende Einwilligungen bei ihren Bestandsmieter*innen nachzuholen bzw. für zukünftige Mietverhältnisse vorab einzuholen. Für Mieter*innen, die nicht in die Datenverarbeitung eingewilligt hatten, waren sämtliche personenbezogene Daten zu löschen. Die Vermieterin stellte den betroffenen Personen schließlich eine alternative Lösung zur Türöffnung zur Verfügung.

Fazit

Neue Techniken bieten oft auch zusätzlichen Komfort. Wenn sie mit der Verarbeitung von personenbezogenen Daten einhergehen, muss es dafür eine Rechtsgrundlage geben. Vermieter*innen sollten sich daher immer vorab mit den Datenverarbeitungsvorgängen von Zutrittskontrollsystemen auseinandersetzen und nicht blind auf die von Dienstleister*innen angebotenen Lösungen vertrauen. Eine Einwilligung der Mieter*innen ist nur dann freiwillig und kann die Verarbeitung ihrer Daten zum Betrieb der Klingel legitimieren, wenn Mieter*innen eine Möglichkeit zum Türöffnen erhalten, die ohne die Verarbeitung ihrer Daten auskommt.

13.4. Gericht gibt LDI NRW Recht im Streit um Überwachungsanlage für Lkw

Sind Frontfotos von Fahrzeugen mit bestimmten Abmessungen erlaubt, um ein Durchfahrtverbot für Lkw zu kontrollieren? Laut dem VG Düsseldorf fehlt es dafür im konkreten Fall an einer Rechtsgrundlage. Die betroffene Stadt. Die betroffene Stadt will in Berufung gehen.

Hierum ging es: Eine Stadt hatte auf einer Straße eine stationäre Überwachungsanlage eingesetzt, um ein Durchfahrtsverbot für Lkw über 7,5 Tonnen durchzusetzen. Bis dahin waren die Anwohner*innen aufgrund des hohen Lkw-Aufkommens erheblichen Lärm- und Abgasbelastungen ausgesetzt. Die Messanlage fertigte Fotos von Fahrzeugen an, deren Abmessungen auf ein zulässiges Gesamtgewicht von über 7,5 Tonnen schließen ließen. Dabei wurden jedoch auch Fahrzeuge erfasst, die tatsächlich leichter oder deren Fahrer*innen als Anlieger*innen vom Verbot ausgenommen waren. Die Fotos zeigten die Kennzeichen und die fahrenden Personen. Die Stadt wertete die Fotos regelmäßig aus, um Verstöße festzustellen und zu verfolgen.

Die LDI NRW hatte deshalb beanstandet, dass bei diesem Vorgehen viele Personen erfasst würden, die keinen Verstoß begangen hatten, und ordnete die Einstellung des Betriebs der Überwachungsanlage an. Hiergegen klagte die Stadt mit dem Argument, dass bereits das Überschreiten bestimmter Fahrzeugabmessungen den Anfangsverdacht für eine Ordnungswidrigkeit wegen des Verstoßes gegen das Durchfahrtsverbot begründe.

Das VG Düsseldorf hat der LDI NRW Recht gegeben und die Klage abgewiesen (Urteil vom 16. Januar 2025, Az. 29 K 3891/23). Es hat klargestellt, dass die Datenverarbeitung durch die Überwachungsanlage schwerpunktmäßig der Gefahrenabwehr dient. Sie ziele auf die Einhaltung des

Durchfahrtsverbots und den Schutz der Anwohner*innen. Die Annahme, dass die Anlage hauptsächlich die Verfolgung von Ordnungswidrigkeiten bezwecke, teilte das Gericht nicht. Zu viele der über die Abmessungen erfassten Fahrzeuge verstießen nicht gegen das Verbot oder seien als Anlieger*innen zur Durchfahrt berechtigt.

Damit sei der Betrieb der Anlage an den allgemeinen Regeln der DS-GVO zu messen, so die Schlussfolgerung des Gerichts. Diese Regeln verlangten für die Erhebung und Speicherung der Fotografien von Fahrer*innen und Kennzeichen eine gesetzliche Grundlage. Hieran fehle es jedoch. Eine Rechtsgrundlage ergebe sich nicht aus der Generalklausel zur behördlichen Datenverarbeitung im DSG NRW. Diese rechtfertige nämlich nur Datenverarbeitungen mit geringer Eingriffsintensität. Frontfotos von Kennzeichen und fahrenden Personen stellten jedoch einen Grundrechtseingriff von erheblichem Gewicht dar.

Fazit

Das Urteil macht deutlich: Für die Überwachung eines Durchfahrtsverbots für Lkw mittels Frontfotos, die beim Überschreiten bestimmter Fahrzeugabmessungen aufgenommen werden, besteht keine Rechtsgrundlage. Ohne diese ist der Betrieb entsprechender Überwachungsanlagen datenschutzwidrig, auch wenn an sich legitime Ziele wie der Schutz der Anwohner*innen verfolgt werden. Die Stadt hat beim OVG NRW einen Antrag auf Zulassung der Berufung gegen die Entscheidung des VG gestellt, über den noch nicht entschieden ist.

14. Arbeit

14.1. Gesundheitsdaten von Beschäftigten: Das dürfen Arbeitgeber*innen zur Entgeltfortzahlung tun und wissen

Wenn Beschäftigte länger krank sind, benötigen Arbeitgeber*innen bestimmte Informationen, um die weitere Zahlung des Arbeitsentgelts zu prüfen. Aber wie weit darf der Einblick in den Gesundheitszustand gehen? Wann ist die Verarbeitung von Gesundheitsdaten erlaubt, und welche Grenzen setzt das Datenschutzrecht? Die LDI NRW gibt den Beteiligten eine Hilfestellung an die Hand.

Immer dann, wenn Beschäftigte länger erkranken, stellt sich für Arbeitgeber*innen die Frage, ob die jeweiligen Beschäftigten weiterhin einen Anspruch auf Entgeltfortzahlung haben. Das ist insbesondere relevant, wenn eine Erkrankung über sechs Wochen hinaus andauert oder es zu mehreren Erkrankungen innerhalb kurzer Zeit kommt. Arbeitgeber*innen möchten dann wissen, ob es sich um sog. Fortsetzungserkrankungen handelt. Denn der Anspruch auf Entgeltfortzahlung gilt in der Regel nur für die ersten sechs Wochen einer Erkrankung. Danach gibt es Krankengeld durch die Krankenkasse. Handelt es sich nun hintereinander um dieselbe Krankheit, beginnt nicht bei jeder Erkrankung wieder eine neue Sechs-Wochen-Frist für die Entgeltfortzahlung. Vielmehr werden die Zeiten der „fortgesetzten" Erkrankungen addiert.

Für die Beurteilung, ob eine solche „Fortsetzungserkrankung" vorliegt, sind unter Umständen Gesundheitsdaten erforderlich. Da diese Informationen jedoch besonders sensibel sind, sehen die DS-GVO und das

BDSG strenge Regelungen vor. Wie diese anzuwenden sind, damit hat sich die LDI NRW 2025 ausführlich beschäftigt.

Grundsätzlich dürfen Arbeitgeber*innen Gesundheitsdaten nur dann verarbeiten, wenn sie zur Erfüllung arbeitsrechtlicher Pflichten erforderlich sind. Das Entgeltfortzahlungsgesetz (EFZG) begründet in § 3 Abs. 1 konkrete arbeitsrechtliche Pflichten und ermöglicht damit gemäß Art. 6 Abs. 1 UAbs. 1 lit. c DS-GVO die zur Ausübung dieser Pflichten erforderliche Datenverarbeitung. Darüber hinaus bedarf es für die Verarbeitung der Gesundheitsdaten als besondere Kategorie personenbezogener Daten einer zusätzlichen gesetzlichen Grundlage, die das grundsätzliche Verbot der Verarbeitung solcher Daten gemäß Art. 9 Abs. 1 DS-GVO durchbricht. Diese ergibt sich aus Art. 9 Abs. 2 lit. b in Verbindung mit § 26 Abs. 3 BDSG, soweit die Verarbeitung zur Ausübung von Rechten und zur Erfüllung rechtlicher Pflichten aus dem Arbeitsverhältnis erforderlich ist.

Arbeitgeber*innen unterliegen in diesem Zusammenhang allerdings häufiger einem Irrtum über die Reichweite der Datenerhebungsbefugnis. Die Verarbeitung ist nämlich nur insoweit zulässig, als sie tatsächlich erforderlich ist. Der bloße Verdacht, dass es sich um eine Fortsetzungserkrankung handeln könnte, reicht nicht aus. Es muss vielmehr eine konkrete Vermutung im Einzelfall vorliegen, etwa aufgrund zeitlicher Nähe oder inhaltlicher Hinweise, dass die Erkrankungen zusammenhängen. Arbeitgeber*innen sind zudem angehalten, gegenüber einer eigenen Erhebung von Gesundheitsdaten mildere Mittel zu prüfen. So kann es in bestimmten Fällen ausreichend sein, bei der Krankenkasse eine Einschätzung einzuholen, ob aus ihrer Sicht eine Fortsetzungserkrankung vorliegt. Eine weitere schonendere Alternative kann die Einschaltung des Betriebsarztes sein, der eine medizinische Einschätzung abgibt, ohne dass sensible Gesundheitsdaten direkt an den*die Arbeitgeber*in gelangen. Während das Bundesarbeitsgericht die Anfrage bei der Krankenkasse im gerichtlichen Verfahren zur Entgeltfortzahlung nicht für ausreichend hält (Urteil vom 18. Januar 2023, Az. 5 AZR 93/22), sind solche Maßnahmen im Rahmen der vorprozessualen Datenverarbeitung vorrangig zu ergreifen. Erst wenn dies nicht ausreichende Sicherheit für die Beurteilung gibt, kann eine eigene Datenerhebung durch den Arbeitgeber in Betracht kommen.

Ebenfalls unklar ist manchen Arbeitgeber*innen, dass ausdrückliche Einwilligungen von Beschäftigten in die Offenlegung von Diagnosedaten – etwa, um einem möglichen Streit über die Fortsetzungserkrankung zuvorzukommen – die Datenverarbeitung in der Regel nicht rechtfertigen. Denn eine Einwilligung ist nur wirksam, wenn sie freiwillig erfolgt. In einem Beschäftigungsverhältnis kann davon aber selten die Rede sein. Gerade im Fall einer Erkrankung stehen Beschäftigte häufig unter Druck, weil sie befürchten, ohne Offenlegung ihrer Daten keine weiteren Lohnzahlungen zu erhalten. Insofern scheitert die Wirksamkeit ihrer Einwilligung an der fehlenden Freiwilligkeit der Einwilligungserklärung.

Zu beachten ist außerdem, dass der Umgang mit Gesundheitsdaten bei Entgeltfortzahlungsansprüchen besonders hohe Anforderungen an Sicherheit und Vertraulichkeit verlangt. Arbeitgeber*innen müssen angemessene technische und organisatorische Maßnahmen treffen, um die betroffenen Beschäftigten zu schützen. Dazu gehört insbesondere, dass die betreffenden Daten getrennt von der eigentlichen Personalakte aufbewahrt werden. Auch eine gemeinsame Ablage mit den üblichen ärztlichen Arbeitsunfähigkeitsbescheinigungen, wie sie nach § 5 Abs. 1 Satz 2 EFZG vorzulegen sind, ist datenschutzrechtlich unzulässig. Denn diese Bescheinigungen enthalten lediglich Informationen über Beginn und Dauer der Arbeitsunfähigkeit, nicht jedoch über Diagnosen oder chronische Leiden. Sobald Gesundheitsdaten verarbeitet werden, etwa im Rahmen ärztlicher Gutachten oder durch eigene Erhebung der Arbeitgeber*innen, sind diese getrennt und besonders geschützt zu speichern – vgl. mit den Regelungen zum betrieblichen Eingliederungsmanagement.

Die Daten dürfen zudem nur so lange aufbewahrt werden, wie sie für die Prüfung des Entgeltfortzahlungsanspruchs erforderlich sind. Die Dauer der Speicherung richtet sich nach den Fristen, die das EFZG vorsieht. Darüber hinaus kann sich die Speicherfrist etwa aus tarifvertraglichen oder gesetzlichen Verjährungs- und Ausschlussfristen ergeben. Auf einen Verdacht, dass Beschäftigte rechtliche Schritte einleiten, kommt es nicht an. Auch wenn Arbeitgeber*innen glauben, in Krankheitsmustern bestimmte Auffälligkeiten zu erkennen, berechtigt sie das nicht zur längeren Speicherung.

Die Weitergabe von Gesundheitsdaten an Dritte ist im Regelfall ausgeschlossen. Auch innerhalb des Unternehmens ist eine Weitergabe an Vorgesetzte oder andere Stellen nur dann zulässig, wenn sie zur Zweckerfüllung erforderlich ist – was bei Fragen der Entgeltfortzahlung in der Regel nicht der Fall ist. Anders sieht es aus, wenn sich Arbeitgeber*innen gegen geltend gemachte Ansprüche verteidigen müssen. In einem solchen Fall ist die Weitergabe an interne Jurist*innen, an externe Rechtsanwält*innen oder den Arbeitgeberverband – wenn dieser die rechtliche Vertretung übernimmt – zulässig. Dies ergibt sich aus Art. 6 Abs. 1 UAbs. 1 lit. f und Art. 9 Abs. 2 lit. f DS-GVO, da die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen ein berechtigtes Interesse darstellt, das eine Weitergabe erlaubt. Auch hier gilt jedoch: Die Weitergabe darf sich nur auf die Daten erstrecken, die tatsächlich erforderlich sind.

Fazit

Arbeitgeber*innen sind im Zusammenhang mit der Entgeltfortzahlung durchaus berechtigt, bestimmte Gesundheitsdaten zu verarbeiten – allerdings nur dann, wenn dies wirklich erforderlich ist und keine milderen Alternativen bestehen. Eine pauschale Erhebung von Diagnosen oder die Abfrage von chronischen Vorerkrankungen außerhalb des Entgeltfortzahlungszeitraums ist aber unzulässig. Besonders sensible Gesundheitsdaten müssen zudem sicher verwahrt und frühzeitig gelöscht werden und dürfen nicht beliebig weitergegeben werden.

14.2. Bei Dienstunfällen müssen Behörden auf den korrekten Umgang mit Gesundheitsdaten achten

Beamt*innen müssen Dienstunfälle ihren Vorgesetzten melden. Dabei brauchen die Vorgesetzten aber keine Gesundheitsdaten. Behörden müssen ihre Verfahren so organisieren, dass nur die Stellen Gesundheitsdaten erhalten, die sie benötigen.

Das Stichwort lautet Unfallfürsorge. Werden etwa Polizist*innen bei einem Einsatz im Fußballstadion verletzt, erleiden Justizvollzugsbedienstete bei einem Angriff Körperverletzungen oder Berufsfeuerwehrleute Rauchvergiftungen, dann übernimmt der Dienstherr zum Beispiel Behandlungs- und Krankenhauskosten oder zahlt die Reha. Damit dieses System funktioniert, ist es allerdings unerlässlich, dass der Vorgang als Dienstunfall anerkannt wird, und dazu muss er dem oder der Vorgesetzten mitgeteilt werden. Die zuständige Behörde gibt dabei in der Regel vor, welche Unterlagen der Anzeige beizufügen sind. Die Anzeigen werden jeweils auf dem hierfür vorgegebenen Weg an die zuständige Dienstunfallfürsorgestelle weitergeleitet.

Doch ganz so unproblematisch, wie das klingt, ist es in der Praxis oft nicht. Bei der Unfallanzeige werden teilweise auch sensible Gesundheitsinformationen weitergeben. Und das kann falsch laufen, wie die LDI NRW 2025 wiederholt aufgrund von Beschwerden festgestellt hat.

Zunächst: Ein Dienstunfall ist ein auf äußerer Einwirkung beruhendes, plötzliches, örtlich und zeitlich bestimmbares Ereignis, das einen Körperschaden verursacht hat und das in Ausübung des Dienstes oder infolge des Dienstes eingetreten ist (§ 36 Landesbeamtenversorgungsgesetz). Haben Beamt*innen einen Dienstunfall, müssen sie diesen den jeweiligen Vorgesetzten anzeigen, um Unfallfürsorge zu erhalten. Das ist gesetzlich so geregelt.

Nach Erkenntnissen der LDI NRW kommt es in diesem Zusammenhang immer wieder vor, dass die von Behörden geforderten Unterlagen auch ärztliche Bescheinigungen umfassen. Dies ist zwar insofern unproblematisch, als diese Unterlagen für die Bearbeitung durch die Dienstunfallfürsorgestelle grundsätzlich erforderlich sind. Für die Anzeige des Dienstunfalls auf dem Dienstweg sind sie das aber nicht. Die zuständigen Behörden haben deshalb darauf zu achten und sicherzustellen, dass die durch Art. 9 Abs. 1 DS-GVO besonders geschützten Gesundheitsdaten nur für die zuständige Dienstunfallfürsorgestelle einsehbar sind.

Dies lässt sich im Übrigen auch leicht bewerkstelligen. So können die entsprechenden ärztlichen Bescheinigungen zum Beispiel in einem verschlossenen, besonders gekennzeichneten Umschlag der Dienstunfallanzeige beigefügt werden. Oder die Beamt*innen übermitteln sie selbst direkt an die Dienstunfallfürsorgestelle. Die Behörden sollten auf diese Möglichkeiten in den Hinweisen und Merkblättern zur Anzeige von Dienstunfällen hinweisen.

Fazit

Gesundheitsdaten sind besonders geschützt. Da die Preisgabe von Diagnose- und Behandlungsdaten für die bloße Anzeige eines Dienstunfalls nicht erforderlich ist und diese Informationen damit auch nicht den jeweiligen Vorgesetzten auf dem Dienstweg zur Kenntnis gelangen dürfen, müssen die Behörden organisatorisch dafür Sorge tragen, dass diese Daten nur den Sachbearbeiter*innen zur Kenntnis gegeben werden, die sie für die Unfallbearbeitung benötigen.

14.3. GPS-Ortung von Dienstwagen: Firma darf Beschäftigte nicht dauerüberwachen

Unternehmen mögen es: Über die GPS-Ortung ihrer Firmenfahr-zeuge können sie die Kfz-Flotte effizient koordinieren und Aufgaben leichter organisieren. Allerdings dürfen sie dabei nicht die Persönlichkeitsrechte ihrer Beschäftigten außer Acht lassen. Die Ortung darf nicht in einen ständigen Überwachungsdruck ausarten. Arbeitgeber*innen sollten die Grenzen kennen.

Je nach Größe und Branche können bei einem Unternehmen schon mal 50 oder mehr Firmenwagen zusammenkommen, die koordiniert werden müssen. Die moderne Technik bietet dabei gerade für die Steuerung der Einsätze der Fahrzeuge mittlerweile ein hilfreiches Mittel an: die Ortung des Autos mittels GPS, dem Global Positioning System.

Durch die Verbindung von satellitengestützter Ortung der Fahrzeuge mit den Beschäftigten, die sie fahren, entstehen jedoch Daten, die personenbezogen sind. So erlauben die Standortdaten eines Fahrzeugs etwa, den Aufenthaltsort der jeweiligen Fahrer*innen zu einem bestimmten Zeitpunkt nachzuvollziehen. Die LDI NRW hat sich in einigen Fällen mit der Frage befasst, ob die jeweilige GPS-Ortung die Datenschutzrechte der Beschäftigten verletzt hat.

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke verarbeitet werden. Unternehmen müssen die Gründe für die Erhebung von GPS-Daten klar dokumentieren und die Beschäftigten transparent darüber informieren. Nur wenn ein nachvollziehbarer Zweck besteht und für die Verarbeitung eine Rechtsgrundlage vorliegt, kann eine GPS-Ortung zulässig sein.

Als Rechtsgrundlage kommen vor allem drei Varianten von Art. 6 DS-GVO in Betracht. Dieser Artikel regelt, wann die Verarbeitung von personenbezogenen Daten rechtmäßig ist. Einmal kommt Art. 6 Abs. 1 UAbs. 1 lit. b DS-GVO in Betracht, sofern die Verarbeitung zur Durchführung eines Arbeitsverhältnisses erfolgt, dann die Variante nach lit. c, bei der es um die Erfüllung einer rechtlichen Verpflichtung geht, oder schließlich lit. f, der die Verarbeitung zur Wahrung eines berechtigten Interesses zulässt (zu den Rechtsgrundlagen im Beschäftigungskontext eingehend siehe 29. Bericht unter 12.1).

Eine Einwilligung der Beschäftigten in die Datenverarbeitung (Art. 6 Abs. 1 UAbs. 1 Satz 1 lit. a DS-GVO in Verbindung mit § 26 Abs. 2 BDSG) bildet hingegen meist keine hinreichende Rechtsgrundlage. Denn eine Einwilligung ist nur dann wirksam, wenn sie freiwillig erteilt wird. Aufgrund des Über-/Unterordnungsverhältnisses zwischen Arbeitgeber*innen und ihren Beschäftigten wird eine Einwilligung in der betrieblichen Praxis aber nur selten freiwillig sein. Für die GPS-Ortung während der privaten Nutzung durch Beschäftige, kommt die Einwilligung aber unter Umständen in Betracht: Die Beschäftigten erhalten mit der Möglichkeit zur privaten Nutzung einen klaren Vorteil und das Über-/Unterordnungsverhältnis spielt insoweit keine Rolle. Das GPS-System sollte die Option bieten, die Ortung während der Privatfahrten selbstständig auszuschalten (Datenschutz durch Technikgestaltung). Eine Auswertung der Privatnutzung außerhalb der Arbeitszeit bleibt allerdings jedenfalls grundsätzlich unzulässig.

Auch wenn ein Dienstfahrzeug privat genutzt werden darf und Beschäftigte die steuerliche Wahl haben, den privaten Nutzungsanteil über ein Fahrtenbuch nachzuweisen, kann die GPS-Ortung auf Grundlage einer wirksamen Einwilligung für diesen Zweck erfolgen. Sofern allerdings die sog. „1-Prozent-Regelung” angewendet wird, wonach Beschäftigte das überlassene Fahrzeug privat nutzen dürfen, dafür aber pauschal monatlich (in der Regel) ein Prozent des Bruttolistenpreises versteuert wird, wird ein Nachweis durch ein Fahrtenbuch nicht erforderlich sein. In diesem Fall bietet die GPS-Ortung keinen Vorteil für die betroffenen

Beschäftigten mehr. Eine Einwilligung kann die Ortung dann grundsätzlich nicht mehr legitimieren.

Insofern bleibt die Frage, ob die GPS-Ortung auch ohne gültige Einwilligung zulässig ist, etwa zur Verfolgung von berechtigten Interessen der Arbeitgeber*innen (Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO). Dann müsste die Verarbeitung zur Wahrung dieser Interessen erforderlich sein und dürfte das schutzwürdige Interesse der Beschäftigten am Ausschluss der Verarbeitung nicht überwiegen. Hier ist stets eine sorgfältige Abwägung wichtig. Die GPS-Ortung darf nur in den Grenzen des absolut Notwendigen erfolgen. So ist etwa eine dauerhafte Überwachung des Fahrzeugs in den meisten Fällen nicht gerechtfertigt, da sie erheblichen psychischen Anpassungsdruck auf die Beschäftigten ausübt und ihre Freiheit einschränkt. In der Praxis reicht oft eine punktuelle Ortung, beispielsweise zur Koordination von Folgeaufträgen, zur effizienten Einsatzplanung oder zur Disposition. Eine Speicherung der Daten über die punktuelle Standortermittlung hinaus ist meist nicht erforderlich.

Für Zwecke wie die Arbeitszeiterfassung ist die GPS-Ortung zudem in der Regel ungeeignet – insbesondere, wenn bereits andere Systeme zur Zeiterfassung bestehen. Ebenso ist die GPS-Ortung zur Kontrolle der Tätigkeiten am Einsatzort nur in Ausnahmefällen zulässig, da die Erfassung des Standorts zum Nachweis von geleisteten Tätigkeiten regelmäßig ungeeignet ist und mildere Mittel, etwa eine Empfangsbestätigung durch Kund*innen, vorzugswürdig sind. Auch zur Vorbeugung unerlaubter Privatnutzung ist die permanente Erfassung meist nicht erforderlich, da alternative Methoden wie der Abgleich von Kilometerständen ausreichend sein können. Bei besonders wertvollem Eigentum oder hochsensiblen Frachtgütern kann hingegen ausnahmsweise eine dauerhafte Ortung gerechtfertigt sein, da sie sowohl den Schutz des Eigentums als auch die Sicherheit der Beschäftigten unterstützt.

Fazit

Die GPS-Ortung von Dienstfahrzeugen kann ein nützliches Instrument für Unternehmen sein. Ihr Einsatz muss gleichwohl stets einen konkreten Zweck verfolgen und auf einer Rechtsgrundlage fußen. Bevor GPS-Systeme eingesetzt werden, sollten Unternehmen zudem prüfen, ob alternative Möglichkeiten bestehen, und jedenfalls sicherstellen, dass die Datenverarbeitung auf das unbedingt notwendige Maß beschränkt bleibt.

15. Datensicherheit

15.1. Bürokratie Ade? Das einheitliche Meldeformular für Datenpannen soll kommen

Wer Datenpannen in mehreren Bundesländern oder Mitgliedsstaaten melden will, muss sich bisher mit unterschiedlichen Formularen befassen. Das soll sich bald ändern. Sowohl national als auch in der EU gibt es Bestrebungen, ein einheitliches Meldeformular bereitzustellen.

Ein Unternehmen wird Opfer eines Cyberangriffs. In einer Kita wird eingebrochen und es werden Speicherkarten mit Fotos gestohlen. Ein Krankenhaus gibt einen medizinischen Bericht an die falsche Patientin heraus. Das sind nur einige Beispiele für sog. Datenpannen, die häufig vorkommen und oft an die zuständige Datenschutzaufsichtsbehörde zu melden sind. Doch was wie ein Standardverfahren klingt, kann dann aufwendiger sein, wenn Datenpannen bei mehreren Aufsichtsbehörden gemeldet werden müssen. Denn derzeit stellt jede Aufsichtsbehörde ein eigenes Meldeformular bereit. Und nicht nur das: Datenpannen müssen unverzüglich und möglichst innerhalb von 72 Stunden gemeldet werden. Unterschiedliche Formulare verschärfen den Zeitdruck, unter dem die Verantwortlichen stehen.

Bei der DSK, dem EDSA und den einzelnen Aufsichtsbehörden ist das Problem angekommen. Auch die LDI NRW begleitet Pläne, die Meldeformulare zu vereinheitlichen. Bürokratiearme Aufgabenerledigung ist eines ihrer Ziele.

Betroffen sind vor allem Unternehmen aus Drittstaaten ohne Niederlassung in der EU sowie zentrale Datenschutzabteilungen in Unternehmensgruppen und externe Dienstleistungsunternehmen. Aber auch Datenschutzberater*innen, die Meldungen für Verantwortliche in verschiedenen Bundesländern oder Mitgliedsstaaten übernehmen, kennen den Aufwand durch unterschiedliche Formulare. Gerade bei Cyberangriffen auf IT-Dienstleister, die für verschiedene Unternehmen und andere Stellen tätig sind, muss der gleiche Sachverhalt meist an mehrere Aufsichtsbehörden gemeldet werden.

Den Aufwand dafür zu verringern, ist sowohl der DSK als auch dem EDSA ein wichtiges Anliegen. Dabei soll künftig ein gemeinsames Meldeformular für Datenpannen helfen. Die DSK hatte das Thema mit einer Arbeitsgruppe bereits aufgegriffen, als der EDSA es in seiner Helsinki-Erklärung im Juli 2025 ebenfalls propagierte. Er plant nun die Umsetzung für sein Arbeitsprogramm 2026-2027.

Bei der LDI NRW gehen jährlich über 2000 Datenpannenmeldungen ein. Im Jahr 2025 waren es sogar 2.844. Entsprechend ist es für die LDI NRW wichtig, dass diese Meldungen für eine zielgerichtete Bearbeitung aufbereitet sind und die Informationen enthalten, die für die Bearbeitung benötigt werden. Das schont nicht nur personellen Ressourcen bei der LDI NRW, sondern auch Kapazitäten bei den meldenden Stellen. Die LDI NRW wird daher die geplanten Aktivitäten für ein einheitliches Meldeformular begleiten, um sicherzustellen, dass die mit der Vereinheitlichung angestrebten Ziele erreicht werden und auf Seiten der Aufsichtsbehörden und der meldenden Stellen keine Mehraufwände bei der Bearbeitung von Meldungen entstehen.

Die Europäische Kommission schlägt sogar eine zentrale Meldestelle („Single Entry Point") für Meldungen von Datenpannen bzw. Sicherheitsvorfällen bei der Agentur für Cybersicherheit der Europäischen Union (ENISA) vor. Darüber sollen mit einer Meldung verschiedene Meldepflichten erfüllt werden können. Dies betrifft insbesondere die Meldepflichten nach den europäischen Verordnungen und Richtlinien DS-GVO, NIS-2, DORA, CER und eIDAS. Von einer solchen zentralen Meldestelle würden beispielsweise große Finanzunternehmen profitieren, die bei einem IT-Sicherheitsvorfall Meldepflichten nach verschiedenen Regeln unterliegen können.

Fazit

Die LDI NRW wird die Vereinheitlichung von Meldeformularen für Datenpannen im Interesse bürokratiearmer Aufgabenerledigung begleiten. Eine Vereinfachung wirkt sich für Stellen aus, die derzeit für denselben Sachverhalt unterschiedliche Meldeformulare ausfüllen müssen. Ob eine zentrale Meldestelle in der EU eingerichtet wird, ist noch nicht absehbar.

15.2. Datenpannenmanagement an Uni-Kliniken und Krankenhäusern hat Licht und Schatten

Wie gehen größere Einrichtungen in NRW mit Datenpannen um? Die LDI NRW wollte das wissen und hat deshalb 33 Kliniken zu ihren Fallzahlen und zum Datenpannenmanagement befragt. Das Ergebnis ist teilweise überraschend.

„Wo gehobelt wird, fallen Späne" ist ein bekanntes deutsches Sprichwort. Es soll ausdrücken, dass dort, wo gearbeitet wird und Dinge umgesetzt und verbessert werden, auch Fehler passieren. Im Datenschutz ließe es sich auf die Formel bringen: „Wo personenbezogene Daten verarbeitet werden, kommt es zu Datenpannen". Denn kein Umgang mit Daten ist dauerhaft völlig fehlerlos und unangreifbar.

Der Begriff „Datenpanne" meint dabei eine „Verletzung des Schutzes personenbezogener Daten" nach Art. 4 Nr. 12 DS-GVO. Dies kann beispielsweise geschehen, wenn Daten aus Versehen an die falsche Person versendet werden oder wenn durch einen kriminellen Cyberangriff Daten verloren gehen. Selbst wenn höchste Standards bei Schutzmaßnahmen berücksichtigt und umgesetzt werden, kann es dennoch im Einzelfall dazu kommen, dass personenbezogene Daten ungewollt vernichtet, verloren, verändert, unbefugt zugänglich gemacht oder offengelegt werden.

Auch Universitätskliniken und Krankenhäuser sind nicht davor geschützt. Die LDI NRW hat deshalb 2025 deren Datenmanagement überprüft, um daraus Schlüsse zu ziehen, wie sorgfältig dort mit den besonders sensiblen Gesundheitsdaten umgegangen wird, und ganz allgemein, wie das Meldeverhalten bei Datenpannen grundsätzlich aussieht. Das Ergebnis zeigt Licht und Schatten.

Die DS-GVO legt in den Art. 33 und 34 fest, dass die für eine Datenverarbeitung Verantwortlichen eine Datenpanne untersuchen, deren Risiko bewerten, Maßnahmen treffen und dokumentieren müssen. Außerdem müssen sie die Datenpanne in bestimmten Fällen der zuständigen Aufsichtsbehörde melden und die betroffenen Personen benachrichtigen. Verantwortliche müssen der LDI NRW allerdings nur Datenpannen melden, für die ein mehr als geringes Risiko für die betroffenen Personen festgestellt wurde. Die nicht gemeldeten Datenpannen müssen jedoch intern dokumentiert werden. Die Dokumentation muss es der LDI NRW ermöglichen, die Datenpanne im Nachhinein prüfen zu können.

Seit dem Inkrafttreten der DS-GVO beobachtet die LDI NRW, dass das Meldeverhalten Verantwortlicher auch innerhalb des gleichen Sektors sehr unterschiedlich ist. Das heißt, wenige Verantwortliche melden regelmäßig Datenpannen, während viele Verantwortliche selten oder gar keine Meldungen vornehmen. Dies kann daran liegen, dass Datenpannen mit einem geringen Risiko nicht gemeldet, sondern nur intern dokumentiert werden müssen. Es kann jedoch auch sein, dass Verantwortliche kein

geeignetes Datenpannenmanagement einschließlich festgelegter und kommunizierter interner Meldewege etabliert haben.

Um diese Frage zu untersuchen, hat die LDI NRW im Berichtsjahr 33 Kliniken zu ihrem Datenpannenmanagement befragt. Ziele des Datenpannenmanagements sind nicht nur, eine aufgetretene Verletzung des Schutzes personenbezogener Daten festzustellen, zu untersuchen und deren Risiko zu bewerten. Es muss auch sichergestellt sein, dass ein solcher Vorfall – soweit erforderlich – der zuständigen Aufsichtsbehörde gemeldet wird, die betroffenen Personen benachrichtigt sowie Maßnahmen zur Behebung, Abmilderung und zur künftigen Gewährleistung eines angemessenen Schutzniveaus getroffen werden.

Angeschrieben wurden die 23 Kliniken der Landschaftsverbände Westfalen-Lippe (LWL) und Rheinland (LVR) sowie die zehn NRW-Unikliniken bzw. deren angeschlossene Kliniken, die der Zuständigkeit der LDI NRW unterliegen. Dass Kliniken für die Prüfung ausgewählt wurden, hat damit zu tun, dass diese insbesondere sensible personenbezogene Daten wie Gesundheitsdaten verarbeiten und sich deswegen Datenverluste für die Betroffenen besonders schwerwiegend auswirken können. Die Prüfung sollte außerdem die ausgewählten Verantwortlichen für ihre Pflichten nach Art. 33, 34 DS-GVO sowie für die Etablierung eines Datenpannenmanagements sensibilisieren und ermitteln, wie viele Datenpannen intern dokumentiert wurden. Schließlich ging es auch darum herauszufinden, wie die Datenpannenmanagementprozesse bei den befragten Kliniken aufgestellt sind.

Im ersten Teil des versandten Fragebogens wurden die Fallzahlen in den Jahren 2023 und 2024 abgefragt. Hierbei zeigte sich, dass die Kliniken im Verhältnis zu den bei der LDI NRW insgesamt gemeldeten Datenpannen wenig von Cyberangriffen betroffen waren. Dies liegt vermutlich an den hohen IT-Sicherheitsstandards, die Kliniken auch wegen anderer Regulatorik bereits umgesetzt haben. Die Rückmeldungen zeigten, dass im Klinikbereich überdurchschnittlich häufig „Erfassungsfehler" zu Datenpannen führten. Die größten Fallgruppen von Datenpannen an Kliniken sind Fehlversendungen und andere unbefugte Weitergaben. Diese Fallgruppen stellen auch bei den allgemein bei der LDI NRW eingegangenen Meldungen den überwiegenden Teil dar.

Überraschend hingegen war, dass zwölf Kliniken angaben, dass ihnen 2023 und 2024 keine einzige Datenpanne bekannt wurde. Dass es über zwei Jahre hinweg bei einer Klinik zu keiner Datenpanne kommt, erscheint unwahrscheinlich, da menschliche und technische Fehler praktisch nicht ausgeschlossen werden können. Anzunehmen ist vielmehr, dass etwaige Datenpannen direkt mit den betroffenen Personen geklärt werden konnten und daher oder aus Unkenntnis der Beschäftigten nicht über die internen Meldeprozesse weitergegeben wurden.

Um dies künftig zu verhindern, sollten Beschäftigte regelmäßig dazu geschult werden, wann ein meldepflichtiger Sachverhalt vorliegt und wie die internen Meldewege aussehen. Denn die Erfassung und interne Dokumentation von Datenpannen – auch von denen mit geringem Risiko – hat auch den Zweck, im Rahmen des Datenschutzmanagements zu prüfen, ob in bestimmten Bereichen ungewöhnliche Häufungen auftreten und daher Nachbesserungsbedarf besteht. Sie ist damit ein wichtiges Element bei der regelmäßigen Evaluierung, ob die getroffenen technischen und organisatorischen Maßnahmen wirksam sind.

Als positiv herausgestellt hat sich bei der Befragung, dass im Jahr 2023 in 21 Prozent und 2024 in 13 Prozent der Datenpannen die betroffenen Personen informiert wurden – obwohl kein hohes Risiko für sie festgestellt wurde und damit keine Benachrichtigungspflicht für die Kliniken bestand. Das ist zu begrüßen, da eine Information der betroffenen Personen in vielen Fällen als Maßnahme angesehen werden kann, die mögliche Folgen für die Betroffenen abmildert.

Mit dem zweiten Teil des Fragebogens wurde abgefragt, wie das Datenpannenmanagement bei den Kliniken umgesetzt wurde. Die Rückmeldungen zeigen, dass alle Kliniken interne Meldewege etabliert haben und für die einzelnen Managementprozesse die relevanten Akteur*innen identifiziert wurden. Weiterhin gaben alle Kliniken an, ihre Beschäftigten hinsichtlich des Datenpannenmanagements (insbesondere bezogen auf die internen Meldewege) zu schulen und zu sensibilisieren.

Fazit

Im Wesentlichen haben die geprüften Klinken ein gutes Datenpannenmanagement etabliert. Hervorzuheben ist, dass Betroffene regelmäßig über sie betreffende Datenpannen informiert werden, denn das hilft Gefahren einzugrenzen. Da es sehr unwahrscheinlich ist, dass in großen Klinikbetrieben gar keine Datenpannen auftreten, sollten diese Kliniken ihre Beschäftigten für die interne Weitergabe von Vorkommnissen sensibilisieren.

16. Zahlen und Fakten

Eingabesituation im Überblick

Im Jahr 2025 haben uns insgesamt **18.060 Eingaben** erreicht, einschließlich Meldungen nach Art. 33 DS-GVO – sog. Datenpannen.

Grundsätzlich nicht erfasst haben wir die zahlreichen telefonischen Anfragen.

Im Jahr 2024 waren es 12.490, 2023 waren es rund 11.050 und 2022 10.500 schriftliche Eingaben.

Das Jahr 2025 markiert damit einen deutlichen Anstieg auf 18.060 Eingaben, was einem Plus von rund 45 Prozent gegenüber 2024 entspricht und einen historischen Höchstwert darstellt.

Von den Eingaben waren

12.592 Beschwerden nach Art. 77 DS-GVO,

898 Hinweise von Dritten,

904 schriftliche Beratungsanfragen,

8 Begleitungen bei Rechtsetzungsvorhaben,

3 Genehmigungsverfahren,

2.844 Meldungen nach Art. 33 DS-GVO zu sog. Datenpannen,

194 Eingaben ohne Kategorie und

421 Eingaben zur Informationsfreiheit.

Beschwerden und Beratungsanfragen

Im Jahr 2025 haben uns **12.592 Beschwerden** erreicht.

Eine Beschwerde liegt nach Art. 77 DS-GVO vor, wenn eine Person vorträgt, dass ein sie persönlich verletzender Verstoß gegen datenschutzrechtliche Bestimmungen vorliegt.

Nach einem relativ stabilen Niveau zwischen 2020 und 2024 (ca. 6.100–7.539 Beschwerden jährlich) zeigt sich 2025 ein massiver Anstieg auf 12.592 Beschwerden. Das entspricht gegenüber 2024 einer Zunahme von rund 67 Prozent.

Eingaben, die auf mutmaßliche Datenschutzverstöße hinweisen, von denen die Einsendenden jedoch nicht selbst betroffen sind, können wir von Amts wegen aufgreifen. Solche **Hinweise von Dritten** haben wir in **898** Fällen erhalten.

Schriftliche **Beratungsanfragen** haben wir insgesamt **904** erhalten, sowohl von Verantwortlichen und Auftragsverarbeitern als auch von betroffenen Personen.

Meldungen von Datenschutzverletzungen

Meldungen nach Art. 33 DS-GVO zu sog. Datenpannen haben uns **2.844** erreicht.

Im Jahr 2024 waren es 2.170, 2023 waren es 2.039 Meldungen und 2022 waren es 1.829 Meldungen.

Eine Verletzung des Schutzes personenbezogener Daten, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, muss der Verantwortliche unverzüglich und möglichst binnen 72 Stunden der zuständigen Aufsichtsbehörde melden (Art. 33 DS-GVO).

Thematische Zuordnung der gemeldeten Datenpannen:

34 Prozent Cyberangriffe

24 Prozent Fehlversand

20 Prozent andere unbefugte Weitergabe

4 Prozent offene E-Mailverteiler

3 Prozent Einbruch/Diebstahl

2 Prozent anderer Verlust von Dokumenten oder Speichermedien

3 Prozent unbefugte Veröffentlichung

10 Prozent Sonstiges

Abhilfemaßnahmen

Um eine Überwachung und Durchsetzung der DS-GVO sicherzustellen, werden den Aufsichtsbehörden in Art. 58 Abs. 2 DS-GVO einheitliche Abhilfebefugnisse eingeräumt.

Bußgeldverfahren

Als Maßnahme nach **Art. 58 Abs. 2 lit. i DS-GVO** wurden bei der Zentralen Bußgeldstelle der LDI NRW **141 Bußgeldverfahren** eingeleitet bzw. zur weiteren Verfolgung von den Staatsanwaltschaften übernommen.

53 Bußgeldbescheide wurden erlassen und **86 Verfahren** wurden durch Rechtskraft, Einstellung oder Gerichtsentscheidungen **abgeschlossen.** Die **Summe aller Bußgelder beträgt 431.900 Euro,** das **höchste Bußgeld** betrug **300.000 Euro,** der **Mittelwert** aller Bußgelder beträgt **8.150 Euro** und der **Median 500 Euro.**

Weitere Abhilfemaßnahmen

Von den weiteren in Art. 58. Abs. 2 DS-GVO genannten Abhilfemaßnahmen hat die LDI NRW die folgenden Maßnahmen ergriffen:

2.033 Hinweise nach Art. 58 Abs. 1 lit. d,

6 Warnungen nach Art. 58 Abs. 2 lit. a,

4 Anweisungen nach Art. 58 Abs. 2 lit. c,

35 Verwarnungen nach Art. 58 Abs. 2 lit. b,

236 Anweisungen nach Art. 58 Abs. 2 lit. d,

3 Beschränkungen nach Art. 58 Abs. 2 lit. f,

3 Aussetzungen der Übermittlung nach Art. 58 Abs. 2 lit. j.

Davon erfasst sind Verfahren, die bereits in den Vorjahren eingeleitet wurden, während viele im Jahr 2025 begonnene Verfahren noch nicht beendet und nicht erfasst sind. Oft sind die Verfahren sowohl in zeitlicher als auch in rechtlicher Hinsicht aufwendig. Nicht selten bedarf es vieler Kontakte und eines umfangreichen Schriftwechsels, bis es am Ende zu einer Abhilfemaßnahme etwa in Form eines Bußgeldbescheides kommt. Zudem setzt die LDI NRW im Kontakt mit den Verantwortlichen und Auftragsverarbeitern nach wie vor den Schwerpunkt auf Beratung und Sensibilisierung. Häufig werden so ohne eine förmliche Abhilfemaßnahme einvernehmliche, konstruktive Lösungen gefunden, die nicht nur den Einzelfall datenschutzgerecht lösen, sondern auch für die zukünftige Praxis der Verantwortlichen und Auftragsverarbeiter einen Gewinn für den Datenschutz bedeuten.

Europäische Verfahren

Die DS-GVO sieht Verfahren für eine europäische Meinungsbildung und Entscheidungsfindung der Datenschutzaufsichtsbehörden vor. Das einheitliche europäische Recht soll in den Mitgliedstaaten auch einheitlich angewendet werden. Da die Regelungen der DS-GVO oft allgemein gehalten sind, haben die Aufsichtsbehörden die Aufgabe, das neue Recht in der Interpretation und in der Praxis zu harmonisieren. Dazu müssen sich die Behörden abstimmen und – teils verbindliche – Rechtsauffassungen entwickeln. Die Meinungsbildung der europäischen Aufsichtsbehörden findet in Abstimmungsverfahren der Behörden untereinander und im EDSA statt.

Für viele Abstimmungsprozesse wird das Binnenmarkt-Informationssystem (Internal Market Information System, abgekürzt IMI) als IT-Plattform eingesetzt. Die Plattform IMI unterstützt die Verfahren der Zusammenarbeit und Kohärenz über komplexe Module. Wird ein Modul in IMI gestartet, generiert das System eine automatische Benachrichtigung, die bei der empfangenden Behörde bearbeitet werden muss. Arbeitssprache in IMI ist Englisch.

Unter anderem tauschen sich die betroffenen Aufsichtsbehörden über grenzüberschreitende Fälle aus und stimmen Entscheidungen ab. Geht beispielsweise bei uns eine Beschwerde in Bezug auf eine grenzüberschreitende Datenverarbeitung ein, leiten wir als Eingangsbehörde die ersten notwendigen Schritte über IMI in die Wege. Geht über IMI eine Meldung über eine grenzüberschreitende Datenverarbeitung ein, prüfen wir, ob wir europaweit federführend sind oder uns als betroffene Behörde an den weiteren Verfahrensschritten beteiligen.

Im Jahr 2025 war die LDI NRW in **2.863 Fällen** mit gestarteten **IMI-Modulen** befasst. Damit setzte sich der kontinuierliche Anstieg der Fallzahlen und die damit verbundene Arbeitsbelastung fort, nachdem 2023 noch 2.182 Fälle und 2024 dann 2.272 Fälle verzeichnet wurden. Im ersten vollständigen Jahr, nachdem die DS-GVO wirksam geworden ist, nämlich in 2019, waren es nur 1.390 Fälle. Damit verzeichnen wir binnen sieben Jahren eine Verdoppelung der Fallzahlen

Wir hatten bei **sechs** europäischen Verfahren die **Federführung,** bei **69** Verfahren waren wir in unserer **Zuständigkeit betroffen** und in **zwei** Verfahren nach Art. 60 ff. DS-GVO **(Zusammenarbeit oder Kohärenzverfahren)** beteiligt.

Förmliche Begleitung bei Rechtsetzungsvorhaben

Im Jahr 2025 wurde die LDI NRW bei mehreren Rechtsetzungsvorhaben beteiligt.

Die LDI NRW ist frühzeitig über Entwürfe für Rechts- und Verwaltungsvorschriften zu unterrichten, wenn diese eine Verarbeitung personenbezogener Daten vorsehen (vgl. § 27 Abs. 5 Satz 2, § 57 Abs. 5 DSG NRW).

Wir wurden in unterschiedlicher Intensität und in verschiedenen Phasen der Verfahren beteiligt. Nicht alle Verfahren hatten dabei einen datenschutzrechtlichen Bezug, so dass wir dazu keine inhaltliche Stellungnahme abgegeben haben. Eine inhaltliche Stellungnahme wurde insbesondere zu folgenden Gesetzentwürfen verfasst:

- Achtes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen (siehe hierzu unter 8.1)
- Gesetz zur Neuverkündung des Verfassungsschutzgesetzes Nordrhein-Westfalen und zur Änderung weiterer Gesetze (siehe hierzu unter 8.2)
- Änderung der VollzugsdatenverarbeitungsVO
- Zweites Gesetz zur Änderung des Strafrechtsbezogenen Unterbringungsgesetzes (StrUG NRW)
- Gesetz betreffend die Stärkung der Hochschullandschaft (Hochschulstärkungsgesetz)
- Gesetz zur Änderung des Schülerinnen- und Schülerdatenübermittlungsgesetzes NRW
- Verordnung zur Regelung der Verarbeitung von Schülerinnen- und Schülerdaten am Übergang von der Schule in den Beruf (Schülerinnen- und Schülerdatenverarbeitungsverordnung NRW)
- Gesetz über den Brandschutz, die Hilfeleistung und den Katastrophenschutz NRW
- Gesetzes zur Verarbeitung von personenbezogenen Daten zum Schutz der Beschäftigten öffentlicher Stellen vor gefährdenden Personen (Beschäftigtenschutzgesetz - BSchG NRW)
- 2. Staatsvertrag zur Neuregulierung des Glücksspielwesens in Deutschland (2. Änderungsglücksspielstaatsvertrag 2021)
- Zweites Gesetz zur Änderung des Landesfischereigesetzes
- Neufassung des Gesetzes zur Neuregelung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Erkrankungen
- Gesetz zur Neuregelung des Rettungsdienstes im Land Nordrhein-Westfalen

- Gesetz zur Änderung des Registerzensuserprobungsgesetzes (RegZensEG)
- Gesetz zur Festlegung auskunftspflichtiger Stellen nach § 99 Absatz 7c i. V. m. § 102 Abs. 2 S. 2 des SGB VIII
- Verordnung über die pauschale Krankenhausförderung (PauschKHFVO)
- Gesetz zur Umsetzung des Pflegestudiumstärkungsumsetzungsgesetzes (PflStudStUG)
- Gesetz über die klinische und epidemiologische Krebsregistrierung im Land Nordrhein – Westfalen (Landeskrebsregistergesetz - LKRG NRW)
- Gesetz zur Stärkung der Informationssicherheit des Landes Nordrhein-Westfalen (Informationssicherheitsgesetz Nordrhein-Westfalen – InfoSiG NRW)
- 9. Medienänderungsstaatsvertrag
- Politische-Werbung-Transparenz-Gesetz (PWTG)
- Gesetz zur Sicherung von Tarifentgelten bei öffentlichen Vergaben in Nordrhein-Westfalen (Tarifentgeltsicherungsgesetz)
- Gesetz betreffend die Stärkung der Hochschullandschaft (Hochschulstärkungsgesetz)

Transparenz

Diese und weitere Informationen sind unter **www.ldi.nrw.de/zahlen-und-daten** veröffentlicht.

Anhang
Veröffentlichungen der Datenschutzkonferenz 2025

1. Entschließungen der Datenschutzkonferenz 2025

12.12.2025 – DS-GVO-Reform: Rechtssicherheit und Innovation gehen Hand in Hand – Anpassungen für KI erforderlich

Die Datenschutzkonferenz (DSK) begrüßt im Ansatz die Initiative der Kommission, durch Rechtsanpassungen mehr Rechtssicherheit für die Entwicklung und den Betrieb von KI-Systemen und KI-Modellen mit personenbezogenen Daten anzustreben. Die DSK stellt einen datenschutzrechtlichen Regelungsbedarf für Verarbeitungen personenbezogener Daten bei Entwicklung, Training und Betrieb von KI-Modellen und -Systemen fest. Sie hält es darüber hinaus für erforderlich, nicht nur das Thema der Rechtmäßigkeit von Verarbeitungen in den Blick zu nehmen, sondern auch in weiteren Abschnitten der DS-GVO einen KI-spezifischen Regelungsbedarf zu prüfen. Die Anpassung der DS-GVO hinsichtlich KI muss die Technologie ganzheitlich adressieren. Die DSK sieht bei den Rechtsgrundlagen einen dringenden Anpassungsbedarf. Sie betont, dass angesichts der Schwierigkeiten bei der effektiven Verwirklichung von Betroffenenrechten gleichwertige Äquivalente dringend erforderlich sind. Durch mehr Rechtssicherheit wird aus Sicht der DSK ein wirksamer Vollzug der DS-GVO erleichtert, der Schutz der Grundrechte der betroffenen Personen gewahrt und gleichzeitig die Möglichkeiten zur Innovation im eindeutigen Rechtsrahmen gestärkt.

Rechtsgrundlagen für Entwicklung und Betrieb von KI-Modellen und -Systemen

Die DSK hält es für erforderlich, für die Verarbeitungen von personenbezogenen Daten bei der Entwicklung und dem Betrieb von KI-Modellen und KI-Systemen neue, spezifische Regelungen, insbesondere Rechtsgrundlagen zu erlassen. Sie sollten sowohl für nicht-öffentliche als auch nach Maßgabe vorhandener Kompetenzen für öffentliche Stellen gelten und Schutzmaßnahmen für Betroffene gewährleisten. Die Anforderungen der Rechtsgrundlagen müssen die technischen Besonderheiten von KI-Modellen und KI-Systemen, die sehr vielfältigen Einsatzmöglichkeiten sowie die unterschiedlichen Rollen der Beteiligten berücksichtigen. Dies ist der beste Weg, die betroffenen Grundrechtspositionen im Sinne der praktischen Konkordanz in einen angemessenen Ausgleich zu bringen.

Relevante Regelungsbereiche können sein:

- Verarbeitung von durch Web Scraping erlangten personenbezogenen Daten einschließlich besonderen Kategorien für die Entwicklung von KI-Modellen,
- Weiterverarbeitung von für andere Zwecke erhobenen personenbezogenen Daten einschließlich besonderer Kategorien, um interne domänenspezifische KI-Modelle zu entwickeln
- Verarbeitungen beim Betrieb von in KI-Modellen memorisierten personenbezogenen Daten

Diese Regelungen müssen einerseits klare Voraussetzungen rechtmäßiger Verarbeitungen für die besonders relevanten Konstellationen abbilden und zugleich rote Linien in Form von Verboten aufzeigen.

Betroffenenrechte mitdenken

Zur Einhaltung des Datenschutzes bei der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen und -Systemen gehört auch, Transparenzvorgaben und Betroffenenrechte der DSGVO nach der Rechtsprechung des Europäischen Gerichtshofs zu gewährleisten.[1] Bei der Entscheidung zur Einführung eines KI-Systems, also möglichst frühzeitig, sollte die Sicherung der Rechte der betroffenen Person eine Rolle spielen, quasi als ”Betroffenenrechte by Design”. Gleichwohl zeigt sich, dass die Gewährleistung der Betroffenenrechte beim Einsatz vieler KI-Systeme in der Praxis schwierige Fragen aufwerfen kann, wenn die Umsetzung aufgrund der zugrundeliegenden Modelle kaum möglich erscheint.

Um die Rechte der Betroffenen zu wahren und einen eindeutigen rechtssicheren Rahmen für KI zu schaffen, sollten daher im Rahmen des europäischen Reformprozesses zum Datenschutzrecht und den Digitalrechtsakten auch Anpassungen in Form von funktionsäquivalenten oder kompensatorischen Schutzmaßnahmen in den Blick genommen werden.

Bislang sind Verantwortliche im Rahmen der datenschutzrechtlichen Transparenzpflichten nicht explizit verpflichtet, Betroffene ausdrücklich darüber zu informieren, dass ihre personenbezogenen Daten in einem KI-System verarbeitet werden. Daher wird die Aufnahme einer entsprechenden Informationspflicht in die Art. 13 Abs. 2 und Art. 14 Abs. 2 DSGVO vorgeschlagen. Entsprechendes ist für das Recht der Betroffenen auf Auskunft festzustellen. Um diese Regelungslücke zu schließen, wird die Einführung einer entsprechenden Ergänzung in Art. 15 Abs. 1 DSGVO vorgeschlagen.

---

1 Siehe dazu die Orientierungshilfe der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und beim Betrieb von KI-Systemen, Version 1.0 (Stand Juni 2025). Vgl. EuGH, Urteil vom 4. Oktober 2024, Koninklijke Nederlandse Lawn Tennisbond, C-621/22, EU:C:2024:857, Rn. 40, 41 und 49

Aus technischen Gründen könnte es in manchen Fällen für den Verantwortlichen nur mit unverhältnismäßigem Aufwand möglich sein, beispielsweise dem kompletten Neutraining eines LLMs, die Erfüllung der Betroffenenrechte aus Art. 16 Abs. 1, Art. 17 Abs. 1, Art. 18 Abs. 1 und Art. 21 DSGVO zu gewährleisten. Hier sollte der europäische Gesetzgeber prüfen, wie die spezifischen Risiken für nicht umgesetzte Transparenz-, Löschungs-, Berichtigungsrechte und Widerspruchsrechte im KI-Modell mitigiert oder Betroffenenrechte funktionsäquivalent gewährleistet werden können, so dass praxistaugliche Lösungen geschaffen und gleichzeitig der Schutzstandard gehalten werden kann.

Die DSK wird den laufenden Prozess der DSGVO-Reform weiter konstruktiv begleiten und erneut Stellung nehmen.

12.12.2025 – DSGVO-Reform: IT-Hersteller in die Verantwortung nehmen!

Die Datenschutzkonferenz (DSK) unterstützt das gemeinsame Ziel des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder2, die Hersteller und Anbieter von Standardlösungen künftig in die Verantwortung zu nehmen, damit die Anwender unkompliziert und rechtssicher Standardlösungen nutzen können. Sie hält es für erforderlich, die Reform der DSGVO dafür zu nutzen, das System der datenschutzrechtlichen Verantwortlichkeiten durch das Prinzip der Herstellerverantwortung fortzuentwickeln und diesbezüglich an das anderer Digitalrechtsakte wie den Cyber Resilience Act oder die KI-Verordnung anzugleichen. Dies würde zu einer erheblichen Entlastung der Anwender, insbesondere kleinere und mittlere Unternehmen (KMU), und einer substanziellen Vereinfachung für sie führen, wenn sie personenbezogene Daten verarbeiten.

Die DSGVO stellt bereits heute mit Data Protection by Design and by Default (Art. 25 DSGVO) Grundsätze auf, die sich in der Sache an Hersteller, Importeure und Anbieter richten, nimmt aber nicht diese, sondern ausschließlich die Anwender von Hard- und Software datenschutzrechtlich in die Pflicht. Die Einbeziehung der Anbieter bzw. Hersteller von Standard-Hard- und Software in das etablierte System datenschutzrechtlicher Pflichten würde daher die Verantwortung dorthin verlagern, wo die Entscheidungen über grundsätzliche Weichenstellungen in Systemen getroffen werden. Gleichzeitig würden die Anwender von IT-Produkten, die keinen Einfluss auf das Produktdesign haben, die Haftungsrisiken nicht alleine tragen.

2 Beschluss des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder vom 4. Dezember 2025: Die Förderale Modernisierungsagenda, https://www.bundesregierung.de/resource/blob/975228/2397654/c57248be7fa2d61ab6d8b12c0f29f05b/2025-12-04-mpk-staatsmodernisierung-data.pdf

Die DSK hat bereits in ihrer ersten Evaluation der DSGVO im Jahr 20193 Vorschläge für eine solche Erstreckung des Grundsatzes von Data Protection by Design auf Hersteller und Anbieter von IT-Produkten unterbreitet, die im Wesentlichen unverändert vorgeschlagen werden.

Die Ergänzungen entsprechen der grundsätzlichen Ausrichtung der Kommissionsvorschläge, die Anwendung der DSGVO insbesondere für KMU zu vereinfachen und mit den nach ihr erlassenen Digitalrechtsakten zu harmonisieren. Sie erhöhen die Rechtssicherheit für Anwender, denen durch die künftig von Herstellern und Anbietern bereitzustellenden Konformitätserklärungen die Erfüllung ihrer Rechenschaftspflicht erleichtert wird. Demgegenüber entstehen für Hersteller und Anbieter keine erheblichen Zusatzpflichten, da sich diese bereits weitgehend aus dem Cyber Resilience Act ergeben.

In einer weiteren Stufe kann zudem ein an datenschutzrechtliche Zertifizierungen angelehntes Modell auch für Produktzertifizierungen entwickelt werden.

Ergänzend sollten die bisher alleine an den Verantwortlichen gerichteten Verpflichtungen zu den datenschutzfreundlichen Voreinstellungen (Art. 25 DSGVO) auch auf Auftragsverarbeiter erstreckt werden, um neben Herstellern auch deren Rolle bei der Gewährleistung des Datenschutzes durch Technikgestaltung hervorzuheben und Verantwortliche möglichst umfassend von Aufgaben zu entlasten, die an anderer Stelle effektiver geklärt werden können.

20.11.2025 – Verbesserung des Datenschutzes von Kindern in der DS-GVO

1. Besondere Schutzbedürftigkeit von Kindern

Kinder unterliegen einer besonderen strukturell bedingten Gefährdungslage: Sie verstehen je nach Reifegrad die meist langfristigen Nachteile der Verarbeitung ihrer personenbezogenen Daten noch unzureichend, sind aber für die meist kurzfristigen positiven Effekte der Nutzung von datenverarbeitenden Systemen und Diensten sehr offen und für Verführungen zu ihrer Nutzung leicht zugänglich. Wissen über Handlungsfolgen und -möglichkeiten müssen sich bei Kindern erst nach und nach herausbilden und festigen. Ihnen ist oft nicht klar, dass aus den Daten, die sie preisgeben und die durch die Beobachtung ihres Verhaltens entstehen, neue Daten über sie generiert werden, die ihr Weltverständnis bestimmen, ihre sozialen Beziehungen beeinflussen, ihr Selbstbild prägen und Vorhersagen über ihr Verhalten ermöglichen. Kinder können abhängig

3 DSK: Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO, November 2019, https://www.datenschutzkonferenzonline.de/media/dskb/20191213_erfahrungsbericht_zur_anwendung_der_ds-gvo.pdf

von ihrem Reifegrad die Risiken der Verarbeitung ihrer Daten weniger gut vermeiden und sich gegen Eingriffe in ihre Grundrechte weniger gut wehren als Erwachsene dies können. Schließlich ist zu berücksichtigen, dass Kinder in der Regel ihre eigenen Rechte als betroffene Person nicht kennen. Selbst wenn sie ihnen bekannt wären, sind sie meist nicht in der Lage, sie wahrzunehmen. Aus diesen Gründen haben Kinder einen besonderen Bedarf an Schutz und Fürsorge im digitalen Raum und insgesamt bezüglich der Verarbeitung ihrer Daten. Dies ist aufgrund von Art. 24 der EU- Grundrechte-Charta und der UN-Kinderrechtskonvention geboten.

2. Datenschutz von Kindern in der DS-GVO

Diese besondere Schutz- und Fürsorgepflicht des Gesetzgebers berücksichtigt auch die DS-GVO in vielen Zusammenhängen – allerdings nicht in allen notwendigen Aspekten. Nach Erwägungsgrund 38 S. 1 DS-GVO verdienen Kinder „bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind". Unter „Kind" versteht das Unionsrecht entsprechend Art. 1 der UN-Kinderrechtskonvention jede Person, die das 18. Lebensjahr noch nicht erreicht hat.

Die besondere Schutzbedürftigkeit von Kindern berücksichtigt die DS-GVO in sechs Regelungen für unterschiedliche datenschutzrechtliche Zusammenhänge:

- Nach Art. 8 Abs. 1 S. 1 DS-GVO gilt die Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, als rechtmäßig, wenn das Kind das 16. Lebensjahr vollendet hat. Nach Art. 8 Abs. 1 UAbs. 2 DS-GVO dürfen Mitgliedstaaten diese Grenze auf das 13. vollendete Lebensjahr senken. Von der Öffnungsklausel des Art. 8 Abs. 1 UAbs. 2 DS-GVO hat die Mehrzahl der Mitgliedstaaten Gebrauch gemacht und diese Grenze durch gesetzliche Regelung gesenkt. Neun haben die Altersgrenze auf 13 Jahre festgesetzt, sechs auf 14 Jahre, vier auf 15 Jahre und neun Staaten haben die Altersgrenze der DS-GVO beibehalten.
- Nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO muss eine Interessenabwägung die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person in besonderer Weise berücksichtigen, „wenn es sich bei der betroffenen Person um ein Kind handelt".
- Nach Art. 12 Abs. 1 S. 1 DS-GVO sind Informationen nach Art. 13 und 14 DS-GVO sowie Mitteilungen nach Art. 15 DS-GVO „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten".

- Eine Löschung personenbezogener Daten hat nach Art. 17 Abs. 1 lit. f. DS-GVO zu erfolgen, wenn die Daten von Kindern aufgrund einer Einwilligung nach Art. 8 Abs. 1 DS-GVO erhoben worden sind.
- Nach Art. 40 Abs. 2 lit. g DS-GVO können Verbände in Verhaltensregeln auch „Unterrichtung und Schutz von Kindern und Art und Weise, in der die Einwilligung des Trägers der elterlichen Verantwortung für das Kind einzuholen ist," regeln.
- Nach Art. 57 Abs. 1 lit. b DS-GVO ist es eine von vielen Aufgaben der Aufsichtsbehörden, „die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung (zu) sensibilisieren und sie darüber auf(zu)klären. Besondere Beachtung finden dabei spezifische Maßnahmen für Kinder."

3. Ergänzungsbedürftigkeit der DS-GVO

Das sind allerdings nicht alle Situationen, in den der besondere Schutz von Kindern erforderlich ist oder ihre besonderen Interessen zu berücksichtigen sind. In den anderen Regelungen differenziert die DS-GVO nicht explizit zwischen Kindern und Erwachsenen. Für sie gelten grundsätzlich die gleichen Erlaubnistatbestände und die gleichen Verarbeitungsgrundsätze. Sie haben die gleichen Rechte wie Erwachsene. Die Verantwortlichen haben ihnen gegenüber grundsätzlich die gleichen Verpflichtungen und können ihre Daten unter den gleichen Voraussetzungen in Staaten außerhalb des Geltungsbereichs der DS-GVO übermitteln. Jedoch gebieten Art. 1 Abs. 2 DS-GVO i. V. m. Art. 24 der EU-Grundrechte-Charta und der UN-Kinderrechtskonvention sowie Erwägungsgrund 38 die besondere Schutzbedürftigkeit von Kindern bei ihrer Anwendung besonders zu berücksichtigen.

In diesen Fällen bestimmt die DS-GVO jedoch nicht unter welchen Bedingungen welche Rechtsfolgen gelten sollen. Unter anderem wird daher diese Pflicht zur Berücksichtigung von den für die Datenverarbeitung Verantwortlichen in der Praxis oft nicht erkannt oder erfüllt.

Die DS-GVO schützt Kinder in einer ihrer Schutzbedürftigkeit entsprechenden Weise ausdrücklich bisher nur punktuell. Hinter den wenigen Regelungen ist kein Gesamtkonzept erkennbar, das den Verantwortlichen klare Regelungen an die Hand gibt, in welchen Situationen Kinderrechte mit welchen Rechtsfolgen berücksichtigt werden müssen.

Ein Konzept zum effektiven Schutz von Kindern sollte alle wesentlichen Situationen legislativ hervorheben, in denen Kinder besonderen Risiken ausgesetzt sind und in denen ihre Möglichkeiten, Risiken zu erkennen, zu bewerten und sich gegen sie zu schützen, eingeschränkt sind. Dabei sind auch die in der Praxis beschränkten Möglichkeiten ihrer Erziehungsberechtigten, sie zu schützen, zu berücksichtigen. Für diese Situationen sind spezifische datenschutzrechtliche Regelungen erforderlich.

4. Vorschläge zur Ergänzung der DS-GVO

Daher sollte die DS-GVO um weitere spezifische Regelungen zum Schutz von Kindern dort ergänzt werden, wo besondere Gefahren bestehen, dass die für die Verarbeitung im Einzelfall Verantwortlichen diese besondere Schutzbedürftigkeit mit den gebotenen Folgen außer Acht lassen könnten. Der Wortlaut der Verordnung sollte zumindest in folgenden Vorschriften den besonderen Aspekt des Kindeschutzes zusätzlich und ausdrücklich berücksichtigen:

4.1 Vereinbarkeit eines neuen Verarbeitungszwecks (Art. 6 Abs. 4 DS-GVO)

Bei der Prüfung der Vereinbarkeit eines neuen Verarbeitungszwecks mit dem bisherigen Verarbeitungszweck nach Art. 6 Abs. 4 DS-GVO muss der Schutz von Kinderrechten ebenso ein hervorgehobenes Gewicht haben, wie bei der Ersterhebung. Wenn die Daten eines Kindes für einen anderen Zweck verwendet werden sollen, sollte die Feststellung der Vereinbarkeit einer Zweckänderung mit dem ursprünglichen Zweck restriktiver erfolgen als bei Daten von Erwachsenen. Der Wortlaut des Art. 6 Abs. 4 UAbs. 1 lit. d DS-GVO ist wie folgt zu ergänzen (kursiv):

> „d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen, *insbesondere wenn es sich um die personenbezogenen Daten eines Kindes handelt;"*

4.2 Keine Einwilligung in Profiling und Werbezwecke (Art. 8 DS-GVO)

In den Normtext des Art. 8 DS-GVO sollte die Wertung des Erwägungsgrunds 38 S. 2 DS-GVO ausdrücklich übernommen werden: „Ein solch besonderer Schutz sollte insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen."

Dadurch würde die Regelung des Art. 28 Abs. 2 Digital Services Act (DSA) sinnvoll ergänzt, der das Ausspielen personalisierter Werbung an Kinder untersagt. Der Unionsgesetzgeber sollte in Art. 8 DS-GVO festlegen, dass die Einwilligung von Kindern in die Verwendung personenbezogener Daten für Werbezwecke oder Persönlichkeits- oder Nutzerprofile unzulässig ist. Ein solches Verbot würde die Werbung für Spiele und Spielsachen nicht ausschließen, sondern nur die Nutzung von Persönlichkeits- oder Nutzerprofilen und andere Sammlungen von Kinderdaten für Werbezwecke. In Art. 8 Abs. 1 sollte nach S. 1 folgender Satz (kursiv) eingefügt werden. Die bisherigen Sätze 2 und 3 werden 3 und 4:

„Die Verarbeitung personenbezogener Daten eines Kindes für Werbezwecke und für die Erstellung von Persönlichkeits- und Nutzerprofilen ist nicht zulässig."

4.3 Keine Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO

Von der Ausnahme des Verbots der Verarbeitung besonderer Kategorien von personenbezogenen Daten bei einer Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO sollte die Einwilligung eines Kindes grundsätzlich ausgenommen werden. Etwas anderes soll nur dann gelten, wenn das Kind die Reife besitzt, die Auswirkungen seiner Einwilligung zu überschauen und die Verarbeitung dem Wohl des Kindes nicht widerspricht. Im Übrigen bliebe trotz des grundsätzlichen Verbots eine Einwilligung oder Zustimmung durch einen Träger der elterlichen Verantwortung weiterhin möglich. Hierzu wird folgende Ergänzung (kursiv) vorgeschlagen:

> „a) Die erwachsene ~~betroffene~~ Person hat für sich oder als Träger der elterlichen Gewalt für ein Kind in die Verarbeitung der genannten personenbezogenen Daten für einen oder *mehrere festgelegte Zwecke ausdrücklich eingewilligt oder ein Kind hat im Rahmen der für die Entscheidung erforderlichen Reife in eine dem Kindeswohl eindeutig nicht widersprechende Verarbeitung eingewilligt,* es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,"

4.4 Datenverarbeitung für Präventions- und Beratungsdienste sowie ärztliche Untersuchungen und Heileingriffe

Die Zielsetzung des Erwägungsgrunds 38 S. 3 DS-GVO, dass „die Einwilligung des Trägers der elterlichen Verantwortung (…) im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, nicht erforderlich sein" sollte, hat im Text der Verordnung keinen Ansatzpunkt gefunden. Ein Kind sollte in psychischen Zwangslagen zum Beispiel eine Sucht- oder Schwangerschaftsberatung in Anspruch nehmen können, ohne befürchten zu müssen, dass die Eltern davon erfahren. Die gleiche Möglichkeit sollte bestehen, wenn das Kind eine ärztliche Untersuchung oder einen Heileingriff durchführen lassen möchte. Dies könnte in Art. 9 Abs. 2 lit. a DS-GVO als S. 2 wie folgt geregelt werden:

> *„Die ausdrückliche Einwilligung eines Kindes nach Vollendung des [zwölften] Lebensjahres in die Verarbeitung von personenbezogenen Daten im Zusammenhang mit Präventions- oder Beratungsdiensten, die unmittelbar einem Kind angeboten werden, und im Zusammenhang mit ärztlichen Untersuchungen oder Heileingriffen ist bei vorliegender Reife und Einsichtsfähigkeit auch ohne die Einwilligung des Trägers der elterlichen Verantwortung zulässig."*

Zu Erwägungsgrund 38 DS-GVO ist in den Erwägungsgründen der Reform-Verordnung der bisherige Satz 3 durch folgenden Satz zu ersetzen:

> *„Um einen Missbrauch von Präventions- oder Beratungsdiensten zur*

Verarbeitung personenbezogener Daten besonderer Kategorien von Kindern auszuschließen, sollte diese Verarbeitung nur für anerkannte Präventions- oder Beratungsdienste im öffentlichen Interesse, nur für die Zwecke dieser Dienste und nur im für diese Dienste erforderlichen Umfang zulässig sein."

4.5 Widerspruch zur Verarbeitung von Kindesdaten

Nicht nur bei der Forderung nach Löschung, sondern auch beim Widerspruch nach Art. 21 Abs. 1 DS-GVO sollte es in besonderer Weise erwähnt werden, wenn die personenbezogenen Daten im Kindesalter erhoben worden sind. Kinder sind sich gemäß Erwägungsgrund 38 S. 1 DS-GVO „der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst". Um hier Missverständnisse auszuschließen und Rechtsklarheit zu schaffen, sollte der Wortlaut des Art. 21 Abs. 1 DS-GVO klarstellen, dass der Verantwortliche bei der Prüfung der Berechtigung des Widerspruchs den Umstand, dass er Daten von Kindern verarbeitet, besonders berücksichtigen muss. Dies würde auch mit der Pflicht des Verantwortlichen nach Art. 6 Abs. 1 UAbs. 1 lit. f DS-GVO korrespondieren, bei seiner Interessenabwägung die entgegenstehenden Interessen oder Grundrechte und Grundfreiheiten in besonderer Weise zu berücksichtigen, „wenn es sich bei der betroffenen Person um ein Kind handelt". Für Datenverarbeitungen, die auf Art. 6 Abs. 1 UAbs. 1 lit. E DS-GVO und spezifischen Regelungen des Unions- oder des nationalen Rechts beruhen, dürfte die „spezifische Situation" gemäß Art. 21 Abs. 1 S. 1 DS-GVO nicht vorliegen, wenn die Regelung – wie zum Beispiel im Schulrecht – alle Kinder betrifft. Alternativ könnte diese Regelung zum „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses" gemäß Art. 23 Abs. 1 lit. e DS-GVO Ausnahmen vorsehen, die die Verarbeitung von Kinderdaten ermöglicht. Der Wortlaut des Art. 21 Abs. 1 S. 1 DS-GVO ist um folgenden Einschub (kursiv) zu ergänzen:

> „(1) Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, *insbesondere wenn es sich um die personenbezogenen Daten eines Kindes handelt,* jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Artikel 6 Absatz 1 Buchstaben e oder f erfolgt, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling."

4.6. Keine Einwilligung in automatisierte Entscheidungen

Von der Ausnahme des Verbots der Verarbeitung personenbezogener Daten bei einer automatisierten Entscheidung aufgrund einer Einwilligung nach Art. 22 Abs. 2 lit. c DS-GVO sollte die Einwilligung eines Kindes ausdrücklich ausgenommen werden. Die Wertung von Erwägungsgrund 71 S. 5 DS-GVO („Diese Maßnahme sollte kein Kind betreffen") findet bisher im Normtext keinen Niederschlag. Der Wortlaut ist um ein Adjektiv (kursiv) zu ergänzen:

> „c) mit ausdrücklicher Einwilligung der *erwachsenen* betroffenen Person erfolgt."

4.7 Datenschutzgerechte Systemgestaltung

Bei der datenschutzgerechten Systemgestaltung nach Art. 25 Abs. 1 DS-GVO sollte der Schutz der Grundrechte und Interessen von Kindern in besonderer Weise hervorgehoben werden.

Gerade bei der Systemgestaltung wäre ein grundlegender Schutz von Kindern – vor allem in Social Networks und anderen Angeboten mit datengetriebenen Geschäftsmodellen – besonders wichtig – und meist auch leicht zu realisieren. Der Wortlaut des Abs. 1 ist ein weiterer Satz (kursiv) anzufügen:

> „(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen, trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie zum Beispiel Pseudonymisierung —, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen. *Dabei ist dem Schutz der Rechte von Kindern besonders Rechnung zu tragen."*

4.8 Datenschutzfreundliche Voreinstellung

Auch bei der datenschutzfreundlichen Voreinstellung nach Art. 25 Abs. 2 DS-GVO sollte der Schutz von Kindern in besonderer Weise gefordert werden. Sie übernehmen – mehr noch als Erwachsene – die voreingestellten Werte und konzentrieren sich allein auf die Nutzung des Geräts oder des Dienstes. Diese spezifische Voreinstellung für Kinder ist vor allem für Social Networks wichtig. Gerade von Kindern kann nicht angenommen werden, dass sie Voreinstellungen erkennen und deren Bedeutung für ihre informationelle Selbstbestimmung verstehen.

Sie sind in besonderer Weise darauf angewiesen, dass die Grundeinstellung jedes Risiko für ihren Datenschutz vermeidet. Der Wortlaut ist um einen neuen Satz 4 (kursiv) zu ergänzen:

> *„Die Voreinstellungen berücksichtigen insbesondere die Schutzbedürftigkeit von Kindern."*

4.9 Meldung von Datenschutzverletzungen

Bei Verletzungen des Schutzes personenbezogener Daten ist eine Meldung an die zuständige Aufsichtsbehörde nicht erforderlich, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Als Risiken, die zu berücksichtigen sind, gelten vor allem ökonomische Nachteile, Verletzungen des Persönlichkeitsrechts, Veröffentlichung geheimhaltungsbedürftiger Daten und möglicher Missbrauch der Daten für weitere Angriffe. Die besonderen Risiken von Kindern stehen bei der Risikobewertung nicht im Vordergrund, obwohl bereits die Kenntnisnahme ihres Namens und ihres Wohn- oder Aufenthaltsorts bedeutsame Risiken für sie verursachen können. Daher sollte auf diese Risiken besonders hingewiesen und Art. 33 Abs. 1 S. 1 DS-GVO um folgenden Passus (kursiv) ergänzt werden.

> „(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 51 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, *wobei das Risiko für Kinder besonders zu berücksichtigen ist."*

4.10 Datenschutzfolgenabschätzung

In der Datenschutzfolgenabschätzung nach Art. 35 DS-GVO sollte das besondere Risiko und der besondere Schutzbedarf von Kindern in adäquater Weise berücksichtigt werden. Daher sollte sowohl für die Bestimmung der Notwendigkeit einer Datenschutzfolgenabschätzung nach Abs. 2 bis 4 als auch bei der Risikoanalyse und bei der Festlegung der Schutzmaßnahmen nach Abs. 7 dem Schutz der Grundrechte und Interessen von Kindern eine besondere Aufmerksamkeit entgegengebracht werden. Art. 35 Abs. 1 DS-GVO ist um einen neuen Satz 2 (kursiv) zu ergänzen. Der bisherige Satz 2 wird Satz 3:

> „(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der

vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. *Soweit Kinder von der Verarbeitung betroffen sind, ist auf die Risiken und Folgen, die die Verarbeitung für ihre spezifischen Rechte haben kann, ausdrücklich einzugehen.* Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden."

Außerdem ist Art. 35 Abs. 7 lit. c und d DS-GVO um jeweils einen Einschub (kursiv) zu ergänzen:

„(7) Die Folgenabschätzung enthält zumindest Folgendes:

(…)

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1, *die in besonderer Weise berücksichtigt, wenn es sich um die personenbezogenen Daten eines Kindes handelt,* und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener, *insbesondere von Kindern, Rechnung getragen wird."*

Diese Schutzregelungen können mit geringem Aufwand, aber hoher Wirkung in den Text der jeweiligen Vorschrift aufgenommen werden. Sie würden den Datenschutz von Kindern deutlich verbessern und die bisherigen Regelungen zum Schutz von Kindern in der DS-GVO systemgerecht ergänzen.

17.09.2025 – Automatisierte Datenanalyse durch Polizeibehörden verfassungskonform gestalten!

Die aktuelle politische Diskussion über den Einsatz von Verfahren zur automatisierten Datenanalyse durch die Polizei betriff rechtliche und technische Anforderungen an polizeiliches Handeln, die auch unter dem Gesichtspunkt der digitalen Souveränität betrachtet werden sollten. Die bisher bekannten Analyseverfahren, die die Polizei in einzelnen Ländern für die Gefahrenabwehr einsetzt, können jede und jeden betreffen. Nicht nur Straftäterinnen und -täter, sondern etwa auch Geschädigte, Zeuginnen und Zeugen, Sachverständige oder Personen, die den Polizeinotruf genutzt haben, können in eine solche Analyse einbezogen sein: Allein in Bayern bezieht sich das dortige Analyseverfahren auf ca. 39 Millionen

Personendatensätze. Es ist verfassungsrechtlich selbstverständlich, dass die Polizei nur bei sehr schwerwiegenden Rechtsgutverletzungen und unter ganz engen Verfahrensbestimmungen solche einschneidenden Analysemittel einsetzen darf. Vor diesem Hintergrund fordert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) die Einhaltung grundlegender, teils auf der Rechtsprechung des Bundesverfassungsgerichts beruhender, Anforderungen.

1. Kein Einsatz von komplexen Datenanalyseverfahren ohne spezifische Rechtsgrundlage

Die DSK betont, dass die allgemeinen Vorschriften im Polizeirecht und in der Strafprozessordnung den Besonderheiten komplexer Analysemethoden nicht ausreichend Rechnung tragen, die mit intensiven Eingriffen in die Grundrechte der betroffenen Personen verbunden sein können. Dies gilt insbesondere für Analysen von umfassenden Datenbeständen, die – wie eingangs beschrieben – Daten über Personen enthalten, die durch ihr Verhalten keinen Anlass für polizeiliche Ermittlungen gegeben haben. Durch Datenanalysen kann neues Wissen erzeugt werden, zum Beispiel können Zusammenhänge zwischen Personen, Institutionen, Organisationen oder Objekten hergestellt werden. Daraus entsteht für die betroffenen Personen das Risiko, zum Gegenstand polizeilicher Ermittlungen oder Maßnahmen zu werden. Dies greift in die Grundrechte aller hiervon betroffenen Personen ein; für die Personen, die selbst keinen Anlass hierfür gegeben haben, wiegt dieser Eingriff besonders schwer. Für solche komplexen Analysen bedarf es eigener Rechtsgrundlagen, die nach dem Gewicht der unterschiedlichen Grundrechtseingriffe bei der Erhebung und Weiterverarbeitung der Daten differenzieren müssen. Wird ihr Einsatz fachlich als erforderlich angesehen, ist der Gesetzgeber in der Pflicht, die wesentlichen Grundlagen selbst durch spezifische gesetzliche Vorschriften vorzugeben, um insbesondere Art und Umfang der Daten und die Verarbeitungsmethoden zu begrenzen. Dies umfasst grundlegende Anforderungen an die notwendigen technischen Anwendungen und Infrastrukturen.

2. Die gesetzliche Grundlage muss verfassungsrechtlichen Maßstäben genügen

Das Bundesverfassungsgericht hat sich im Urteil vom 16. Februar 2023 (- 1 BvR 1547/19 - und - 1 BvR 2634/20 -) umfassend mit dem behördlichen Einsatz von automatisierten Datenanalysen befasst und hierfür die verfassungsrechtlichen Weichen gestellt. Das Bundesverfassungsgericht hat entschieden, dass das Gewicht des mit der Datenanalyse verbundenen Grundrechtseingriffs insbesondere durch Art und Umfang der zu verarbeitenden Daten und die zugelassene Methode der Datenanalyse bestimmt wird.

Ein besonderes Eingriffsgewicht aufgrund von Art und Umfang der Daten ist regelmäßig gegeben, wenn viele Daten zu Personen in die Datenanalyse eingehen, die selbst keinen Anlass für polizeiliche Maßnahmen gegeben haben oder wenn die Daten verschiedenster Systeme trotz ursprünglich unterschiedlicher Erhebungs- und Verarbeitungszwecke in eine Gesamtauswertung einbezogen werden (Zweckbindung und Zweckänderung). Das triff beispielsweise auf Datenbestände aus der Vorgangsbearbeitung und aus Maßnahmen mit großer Streubreite wie Funkzellenabfragen zu. Funkzellenabfragen betreffen alle Personen, die in der Funkzelle mit ihrem Mobilgerät eingebucht sind. Datenbestände insbesondere aus Vorgängen der Strafverfolgung enthalten regelmäßig auch Daten von Geschädigten sowie Zeuginnen und Zeugen. Die herangezogenen Datenbestände müssen für den Zweck der konkreten Datenanalyse geeignet sein. Den Verhältnismäßigkeitsanforderungen genügt eine Maßnahme der Datenverarbeitung grundsätzlich nur, wenn die einzubeziehenden Daten auf solche beschränkt werden, die für den jeweiligen Zweck der Maßnahme Bedeutung haben können.

Besonderes Eingriffsgewicht aufgrund der Methode der Datenanalyse können insbesondere die Verwendung lernfähiger Systeme – Künstliche Intelligenz („KI") –, aber auch komplexe Formen des Datenabgleichs mit nicht lernfähigen Systemen haben. Die DSK sieht ihre Forderungen aus ihrer Entschließung vom 3. April 2019 „Hambacher Erklärung zur Künstlichen Intelligenz" in dem Urteil bestätigt.

Ermöglicht das Verfahren nach den vom Bundesverfassungsgericht benannten Kriterien schwerwiegende Grundrechtseingriffe, ist ein Einsatz nur zum Schutz gewichtiger Rechtsgüter – wie etwa Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes – und unter strenger Begrenzung des Anlasses für die Maßnahme zulässig. Außerdem sind Transparenz und individueller Rechtsschutz für die betroffenen Personen und eine aufsichtliche Kontrolle gesetzlich vorzusehen.

3. Die digitale Souveränität muss bei der Auswahl von Verfahren gewährleistet werden

Sollen für die Analysen Systeme von Fremdanbietern eingesetzt werden, kommen nicht nur die gesetzlichen Anforderungen an die Datensicherheit gegenüber dem Anbieter zum Tragen, sondern es ist auch sicherzustellen, dass die digitale Souveränität des Staates gewahrt wird. Ganz besonders bei polizeilichen Datenbeständen hat der Staat gegenüber seinen Bürgerinnen und Bürgern eine Schutzpflicht, dass deren Daten nicht ohne vorherige Prüfung in Drittstaaten weiterverwendet werden können, die hinter dem europäischen Rechtsstaatsniveau zurückbleiben. Die DSK hat zur Gewährleistung der digitalen Souveränität bei Cloud-Lösungen Kriterien erarbeitet, die sinngemäß auch auf Datenanalyseverfahren für die Polizei übertragbar sind (Kriterien für Souveräne Clouds – Positions-

papier der DSK vom 11. Mai 2023). Zu diesen Anforderungen gehört der Ausschluss von Zugriffen aus oder Datentransfers in Drittstaaten, deren Rechtsordnung nicht mit dem europäischen Recht vereinbar ist. Darüber hinaus verlangt die digitale Souveränität die Nachvollziehbarkeit und die Beherrschbarkeit der Datenverarbeitung, auch im Wege außergerichtlicher oder gerichtlicher Rechtsdurchsetzung, und die langfristige Vorhersehbarkeit und Verlässlichkeit des Angebots. Diese Ziele können in aller Regel zuverlässig nur durch den Einsatz von Systemen erreicht werden, deren Anbieter ihren Sitz im Europäischen Wirtschaftsraum (EWR) haben.

Zur Wahrung der digitalen Souveränität durch Unterbindung von Abhängigkeiten ist zudem sicherzustellen, dass die eingesetzten Systeme hinreichend offen sind, um nötigenfalls einen Wechsel auf ein geeigneteres System zu ermöglichen.

4. Projekt P20 als Chance für den Datenschutz nutzen

Mit dem IT-Großprojekt „Polizei 20/20" (P 20) wird bereits seit längerem eine gemeinsame IT-Infrastruktur der Polizeibehörden von Bund und Ländern vorbereitet. In diesem Projekt besteht die Möglichkeit, datenschutzkonforme Auswerte- und Analysetools zu entwickeln, ggf. auf Basis von transparenten und kontrollierbaren Open Source-Produkten. Auf dem Markt angebotene umfassende Analysetools können nach hiesiger Einschätzung nicht ohne erheblichen Aufwand die im Projekt zu realisierenden Anforderungen an einen verfassungsgemäßen Austausch von Daten zwischen Bund und Ländern erfüllen.

Die Datenschutzkonferenz bietet weiterhin ihre konstruktive Beratung an, um im Rahmen des Projekts P 20 verfassungskonforme und praxistaugliche Lösungen der Datennutzung für die Polizeien zügig auf den Weg zu bringen. Dies gilt auch in Bezug auf etwaige Analysetools.

16.06.2025 – Ohne Sicherheit keine Freiheit – Ohne Freiheit keine Sicherheit

In der aktuellen Diskussion um die Novellierung verschiedener Sicherheitsgesetze betont die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), dass ein starker Datenschutz kein Selbstzweck, sondern ein wesentliches Element des Rechtsstaats und die Voraussetzung für Sicherheit und Freiheit ist.

Grundrechte sind Errungenschaften moderner Demokratien und sichern Wert und Würde der Person und die Teilhabe der Bürgerinnen und Bürger am Gemeinwesen, zum Beispiel bei der Teilnahme an Versammlungen, bei öffentlichen Meinungsäußerungen oder bei Wahlen. Dazu gehört auch die

freie Entfaltung der Persönlichkeit in der verfassungsrechtlich anerkannten Ausprägung des Rechts auf informationelle Selbstbestimmung.Freiheit ist eine wichtige Voraussetzung für eine Demokratie. Ein Leben in Freiheit setzt zugleich voraus, dass die Sicherheit der Bürgerinnen und Bürger gewährleistet ist. Zur Sicherheit gehört wiederum auch, dass sich die Menschen im Land darauf verlassen können, dass der Staat und seine Institutionen ihre Rechte und Freiheiten achten, sich an verfassungskonforme Gesetze und gegebene Garantien halten.

Auf der Welt lässt sich an vielen Stellen beobachten, wie freiheitliche Demokratien in Bedrängnis geraten. In nichtdemokratischen Systemen werden Eingriffsbefugnisse der Sicherheitsbehörden zur Einschüchterung von Bürgerinnen und Bürgern genutzt, sodass letztlich auch die bürgerliche Teilhabe am staatlichen Gemeinwesen ausgehöhlt wird. Das Datenschutzrecht spielt insofern eine wichtige Rolle, da es staatliche Datenverarbeitungen rechtsstaatlich einhegt. Datenschutz ist daher keine bloße Formalie und kein schmückendes Beiwerk.

Daher appelliert die DSK, in der politischen Diskussion Datenschutz und Sicherheit nicht gegeneinander auszuspielen. Zwar stehen sicherheitspolitische Erfordernisse und das Recht auf informationelle Selbstbestimmung in einem gewissen Spannungsverhältnis, allerdings ist dieses nicht unlösbar und kann in verhältnismäßiger Art und Weise aufgelöst werden. Das Datenschutzrecht zielt nicht darauf ab, Täterinnen und Täter oder Gefährderinnen und Gefährder vor Strafverfolgung oder Gefahrenabwehrmaßnahmen zu bewahren. Vielmehr schützt das Datenschutzrecht die Bürgerinnen und Bürger davor, dass ungerechtfertigt in ihre Freiheitsrechte eingegriffen wird.

Datenschutz und Datenqualität in der polizeilichen Praxis

Die Gewährleistung von Datenqualität, klaren Verantwortlichkeiten, effizienten Verfahrensstrukturen sowie digitaler Souveränität sind Belange, die für die Gewährleistung von Sicherheit ebenso wichtig sind wie für den Datenschutz. Die Sicherheitsbehörden wollen Straftaten verfolgen und nicht Personen, die dafür keinen Anlass gegeben haben. Die Sicherheitsbehörden möchten qualitativ hochwertige und sorgfältig austarierte Datenbestände, weil sie rechtsstaatlich arbeiten und nur mit qualitativ hochwertigen Systemen gute Ergebnisse erzielen können. Nichts Anderes wollen die Datenschutzaufsichtsbehörden. Deren Arbeit ist insofern in weiten Teilen eine wesentliche Instanz der Qualitätssicherung. In der Praxis der Sicherheitsbehörden sehen die Datenschutzaufsichtsbehörden eine breite Akzeptanz datenschutzrechtlicher Vorgaben.

Datenschutz steht notwendigem Fortschritt polizeilicher Datenverarbeitung nicht entgegen

Es ist selbstverständlich, dass Sicherheitsbehörden stetig prüfen, an welcher Stelle sie ihre Arbeit weiter verbessern und modernisieren können. Ein Beispiel ist das polizeiliche Projekt P20 zur Harmonisierung der polizeilichen IT-Struktur und -Architektur, das die Datenschutzaufsichtsbehörden lösungsorientiert und konstruktiv beraten. Hierbei ist es aber wichtig, zunächst den genauen fachlichen Bedarf zu analysieren und abzustecken, welche verhältnismäßigen Lösungen möglich sind. Die DSK hält es hingegen für das falsche Signal, auf Herausforderungen für die innere Sicherheit mit dem Ruf nach weiteren Einschnitten in Grundrechte zu reagieren.

Anstelle voreiliger Gesetzgebungsaktivitäten hält es die DSK für dringend notwendig, die vorhandenen – in den vergangenen Jahren stetig erweiterten – Eingriffsbefugnisse der Sicherheitsbehörden, ihre Anwendung in der Praxis und ihre Wirksamkeit weiter umfassend zu evaluieren. Vorliegende wissenschaftliche Arbeiten zu einer Überwachungsgesamtrechnung, insbesondere die vom Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht im Auftrag des Bundes durchgeführte Studie, bieten hierfür eine geeignete Grundlage.

Die unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder werden künftige Novellierungen der Sicherheitsgesetze eng begleiten und sich weiter dafür einsetzen, dass neue Befugnisse für Sicherheitsbehörden den grundrechtlichen, vom Bundesverfassungsgericht ausgeformten, Maßstäben entsprechen.

16.06.2025 – Confidential Cloud Computing

Der Begriff „Confidential Computing” bezeichnet nicht eine einzelne Technologie, sondern wird von verschiedenen Anbietern unterschiedlich belegt. So wird beispielsweise eine Verschlüsselung von Daten im Arbeitsspeicher oder aber auch eine reine Zugriffsbeschränkung auf reservierte Speicherbereiche als Confidential Computing bezeichnet. Unter dem Begriff „Confidential Cloud Computing” werden teilweise Technologien damit beworben, dass Daten sogar vor dem Cloud-Betreiber geheim gehalten werden können. Eine solche allgemeine Aussage trägt jedoch nicht der tatsächlichen Komplexität der eingesetzten Technologie Rechnung. Um solche Werbeversprechen kritisch einzuordnen, werden im Nachfolgenden wichtige zu berücksichtigende Punkte angesprochen.

Angreifermodell

Zuerst sollte festgehalten werden, dass die zugrundeliegenden Technologien ursprünglich insbesondere dem Szenario entstammen, in welchem sich mehrere Nutzende die gleiche Hardware bei einem Cloud-Betreiber teilen. In einer solchen Situation soll sichergestellt werden, dass die eigenen Daten vor den Daten anderer Nutzender geheim gehalten werden können, möglicherweise sogar dann, wenn sich ein anderer Nutzender Administrationsrechte verschafft und auf Teile der Cloud-Betriebsinfrastruktur zugreift.

Wenn jedoch die Daten nicht mehr nur vor anderen Nutzenden, sondern vor dem Cloud-Betreiber geheim gehalten werden sollen, erfordert dies ein komplett anderes und viel stärkeres Angreifermodell. Denn der Betreiber hat physikalischen Zugang zu den Systemen und umfangreiche Möglichkeiten, die Hardware und Software zu manipulieren. Für eine valide Bewertung der Wirksamkeit von Maßnahmen ist ein differenziertes Angreifermodell erforderlich, das auch unterschiedlichen Gruppen von Mitarbeitenden des Betreibers und seiner Auftragnehmer berücksichtigt.

Eine Verbesserung der Sicherheit kann sich dadurch ergeben, dass (zum Beispiel mittels Verschlüsselung) Zugriffsmöglichkeiten innerhalb der Organisation des Betreibers (und ggf. seiner Auftragsverarbeiter) eingeschränkt werden. Auch vor einer missbräuchlichen Nutzung (zum Beispiel Start geklonter virtueller Maschinen oder Container) oder Manipulation gibt es einen gewissen Schutz.

Solche Maßnahmen gehören aber nicht im engeren Sinne zum „Confidential Computing”: Sie ändern nichts an der Tatsache, dass der Betreiber grundsätzliche Zugriff auf die Daten hat bzw. sich verschaffen kann. Die teilweise anzutreffende Behauptung, dass die Kontrolle über die Datenverarbeitung vollständig auf den Nutzenden übergehe, ist nicht haltbar. So ist es beispielsweise offensichtlich, dass die Kontrolle über die Verfügbarkeit der Datenverarbeitung auch beim Cloud-Betreiber liegt. Auch ist es offensichtlich nicht möglich, jede unrechtmäßige Datenverarbeitung im Cloud-Kontext zu verhindern, beispielsweise eine unrechtmäßige Löschung.

Schlüsselmanagement

Eine besondere Bedeutung kommt dem eingesetzten Schlüsselmanagement zu. Tatsächliche Geheimhaltung vor dem Cloud-Betreiber (als Organisation) ist nur gewährleistet, wenn die Daten zu jedem Zeitpunkt so verschlüsselt sind, dass der Cloud-Betreiber den zur Entschlüsselung notwendigen Schlüssel nicht in Erfahrung bringen oder nutzen kann. Vor dem Hintergrund des oben angesprochenen sehr starken Angreifermodells eines „bösartigen Cloud-Betreibers” müssen hierbei auch Analysen und Manipulationen von Hardware und Software berücksichtigt werden. Das bedeutet auch, dass der Cloud-Betreiber nachweisen muss, dass er zu

keinem Zeitpunkt die Möglichkeit hat, die Verschlüsselung zu manipulieren (zum Beispiel durch Machine-in-the-Middle-Angriffe oder den Austausch eines Nutzenden-Schlüssels durch einen selbst gewählten Schlüssel).

Nicht in allen Fällen ist für die Nutzenden klar überprüfbar, ob Confidential Computing überhaupt eingesetzt wird. Zwar ist es je nach Technologie möglich, dass über auf der Hardware hinterlegte Zertifikate attestiert wird, dass eine Operation in einer vertraulichen Umgebung ausgeführt wird. Um diese Attestierung aber an die Nutzenden durchreichen zu können und somit überprüfbar zu machen, muss die jeweilige Anwendung i.d.R. speziell dafür implementiert werden.

Ein besonderes Augenmerk sollte hier auf die Übergänge zwischen den verschiedenen „Verschlüsselungsdomänen" gelegt werden, etwa der Übergang von „data-at-rest" zu „data-in-use". Wenn bei solchen Übergängen ein Wechsel der eingesetzten Schlüssel vorgenommen wird, und zu diesem Zweck eine kurzzeitige Entschlüsselung der Daten stattfindet, liegen die Daten möglicherweise kurzzeitig in unverschlüsselter Form vor.

Um die Aussagen der Cloud-Betreiber sowie der Hersteller der eingesetzten Hard- und Software (zum Beispiel Hersteller von Chips, Firmware, Virtualisierungssoftware etc.) einordnen zu können, müssen Einsatzszenarien transparent sein. Ebenso müssen die der Sicherheitsanalyse zugrundeliegenden Annahmen offen kommuniziert werden. Eine typische Annahme ist, dass es keine physikalischen Angriffe (zum Beispiel Seitenkanalattacken) gibt. Unter dieser Annahme kann diese Technik einen hohen Mehrwehrt an Sicherheit und Datenschutz bieten. Ist hingegen die Annahme nicht zutreffend (etwa, weil der Cloud-Betreiber einem Dritten physikalischen Zugang zur Hardware ermöglichen oder Schlüssel bzw. Zertifikate auf Hardware herausgeben oder austauschen muss) oder vertraut man Zusagen von Herstellern oder Betreibern nicht, so hat diese Technik nicht den versprochenen Effekt.

Als Fazit kann „Confidential Cloud Computing" das allgemeine Sicherheitsniveau erhöhen und typischerweise einen wertvollen Schutz gegen andere Nutzende auf der gleichen Hardware und gegen einzelne Innentäter bieten – letztlich eine weitere Schicht eines „defense-in-depth"-Ansatzes. Der Einsatz sollte daher empfohlen werden, auch wenn nicht alle Datenschutzprobleme so einfach gelöst werden, wie es teilweise beworben wird: Absolute Vertraulichkeit ist nicht möglich und grundsätzlich ist davon auszugehen, dass ein Cloud-Betreiber Zugriffsmöglichkeiten auf die zu schützenden Daten besitzt. Für eindeutig formulierte Angreifermodelle können jedoch konkretere Aussagen getroffen werden. Die Aussagen, mit denen diese Technologie beworben wird, sind daher im Hinblick auf das differenzierte Angreifermodell kritisch zu hinterfragen und die Schlussfolgerungen und die sich aus dem Angebot ergebenden bzw. zusätzlich zu ergreifenden Maßnahmen aus Gründen der Nachweis- und Rechenschaftspflicht nachvollziehbar dokumentieren.

26.03.2025 – Eckpunkte für eine freiheitliche und grundrechtsorientierte digitale Zukunft

Eine Demokratie beweist ihre Stärke dann, wenn sie die Grundrechte der Bürgerinnen und Bürger auch angesichts großer Herausforderungen gewährleistet. Zu diesen Grundrechten zählt auch das Recht auf Datenschutz, das sich angesichts der fortschreitenden Digitalisierung zu einem zentralen Grundrecht entwickelt. Datenschutz wirkt nicht nur als informationelle Selbstbestimmung, sondern ist auch Basis für freie Meinungsäußerung und politische Partizipation. Deutschland kommt zudem innerhalb Europas daten- und digitalpolitisch eine Schlüsselrolle zu. Umso entscheidender ist es, dass die künftige Bundesregierung ein stimmiges daten- und digitalpolitisches Maßnahmenpaket vorlegt, welches die nachhaltige Digitalisierung in Europa voranbringt und menschenzentrierte Datennutzung sicherstellt.

In diesem Sinne fordert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK):

1. Die Gesetzgebungsprojekte zur Novellierung des Bundesdatenschutzgesetzes und zum Beschäftigtendatenschutz zu finalisieren.

Die bereits begonnenen Gesetzgebungsvorhaben müssen wieder aufgegriffen werden. Das schafft Rechtssicherheit für diejenigen, die in Wirtschaft und Verwaltung Verantwortung tragen, und sichert eine einheitliche Anwendung des Datenschutzrechts in Deutschland.

Die Novellierung des Bundesdatenschutzgesetzes drängt. Vor allem gilt dies für:

- Regelungen zum Scoringverfahren in Folge der Rechtsprechung des Europäischen Gerichtshofs
- eine zentrale Zuständigkeitsregelung bei innerstaatlichen, länderübergreifenden Sachverhalten (One-Stop-Shop)
- die Institutionalisierung der DSK mit einer Geschäftsstelle. Die DSK als gemeinsame Instanz der Datenschutzaufsichtsbehörden sichert eine effektive Datenschutzaufsicht. Sie bietet eine einheitliche Ansprechpartnerin für Wirtschaft und Verbände, fördert Synergieeffekte bei der Zusammenarbeit und baut Bürokratie ab. Auch das Zusammenwirken von Datenschutzaufsicht und anderen Aufsichtsbehörden, die Aspekte der Digitalisierung überwachen, wird unter Einbeziehung der DSK besser strukturiert. So wird der Aufbau klarer und nachhaltiger Kooperationsbedingungen der beteiligten Behörden erreicht.

Ein Beschäftigtendatenschutzgesetz sollte insbesondere das Unionsrecht konkretisieren durch Regelungen:

- zum Einsatz von algorithmischen Systemen
- zu den Grenzen der Verhaltens- und Leistungskontrolle
- zu Rahmenbedingungen der Einwilligung im Beschäftigtenverhältnis
- zu Datenverarbeitungen auf der Grundlage von Kollektivvereinbarungen
- zu Beweisverwertungsverboten
- zu Datenverarbeitungen im Bewerbungs- und Auswahlverfahren

2. Einen systematischen Grundrechtecheck bei der Fortentwicklung der modernen Sicherheitsarchitektur durchzuführen.

Angesichts eingriffsintensiver Techniken wie Gesichtserkennung, biometrischer Fernerkennung, automatisierter Datenanalysen und Künstlicher Intelligenz ist die Bundesregierung gefordert, zusätzliche Befugnisse der Sicherheitsbehörden grundrechtssensibel und verfassungskonform zu realisieren. Aufbauend auf der bereits begonnenen und fortzuführenden unabhängigen wissenschaftlichen Untersuchung der Sicherheitsgesetze von Bund und Ländern muss die Bundesregierung:

- den rechtsstaatlichen Rahmen für moderne, digitale Befugnisse setzen
- die Streubreite eingriffsintensiver Maßnahmen eindämmen
- den Grundrechtsschutz durch Verfahren und die Transparenz sicherstellen
- für Integrität und Qualität polizeilicher Daten Sorge tragen
- die Datenschutzaufsicht als integralen Bestandteil der Sicherheitsarchitektur garantieren

Die Bundesregierung muss angesichts der enormen technischen Möglichkeiten die Grundrechteverträglichkeit ihrer Gesetzesentwürfe systematisch überprüfen und dabei die Rechtsprechung des Bundesverfassungsgerichts beachten.

3. Sich in Europa dafür einzusetzen, dass EU-Digitalrechtsakte und DS-GVO besser aufeinander abgestimmt werden

Die Digitalrechtsakte der EU[4] verfehlen bisher das Ziel einer effektiven Gesamtregelung der Datennutzung. Die DSGVO als grundlegende und

4 Etwa Data Governance Act, Data Act, Artificial Intelligence Act, Digital Services Act, Digital Markets Act, European Health Data Space u.a.

technologieoffene allgemeine Regelung des Datenschutzrechts gilt umfassend, ist aber an einigen Punkten mit den Digitalrechtsakten

schwer vereinbar. Im Interesse von Rechtssicherheit und effektivem Grundrechtsschutz besteht Handlungsbedarf. Beispielsweise können die in der DSGVO garantierten Betroffenenrechte aufgrund der technischen Architektur in KI-Anwendungen nicht uneingeschränkt verwirklicht werden. Hier könnte und sollte ein gleichwertiger Schutz von Betroffenenrechten für die KI-Technologie als bereichsspezifisches Datenschutzrecht geregelt werden. Auch Synergien können zum Beispiel erreicht werden:

- bei der Regelung der Rechtsfolgen von Konformitätsbewertungen
- oder durch die Zusammenfassung von Meldepflichten (z. B. NIS-2-Richtlinie und DSGVO)

Die Digitalrechtsakte verfolgen das legitime Ziel, den digitalen Binnenmarkt zu stärken und eine angemessene Datennutzung zu ermöglichen. Datennutzung und Datenschutz müssen dabei Hand in Hand gehen, deswegen bedarf es dringend insgesamt einer rechtlichen Fortentwicklung des europäischen Rechtsrahmens bei gleichwertigem Schutz aber besserer Harmonisierung der Rechtsakte untereinander.

4. Produktive Rahmenbedingungen für KI, Forschung und Innovation im Einklang mit dem Datenschutz gesetzgeberisch zu gestalten.

Forschung, Gesundheitsmanagement, Verkehrskonzepte, nutzerfreundliche Produktentwicklung, Effektivität der Verwaltung und viele nützliche, sinnvolle und für die Menschen gewinnbringende Vorhaben können entscheidend vorangebracht werden, wenn Forschende, Entwicklerinnen und Entwickler sowie Verantwortliche in Wirtschaft, Politik und Verwaltung auf eine gute Datengrundlage und den Einsatz künstlicher Intelligenz zurückgreifen können. Dabei müssen die Rechte derjenigen gewahrt bleiben, um deren Daten es geht. Die Förderung von Innovation muss daher mit den im Unionsrecht verankerten Werten menschenzentriert und vertrauenswürdig Hand in Hand gehen.

Hierfür braucht es:

- Rechtsgrundlagen, die Rechtssicherheit schaffen, ob und unter welchen Bedingungen Daten für Forschung und das Training von KI-Modellen bzw. KI-Systemen verwendet werden dürfen. Der zu schaffende Ausgleich zwischen öffentlichen oder wirtschaftlichen Interessen und den Grundrechten und Schutzansprüchen Einzelner im Hinblick auf personenbezogene Daten muss in den wesentlichen Grundzügen durch den Gesetzgeber festgelegt werden, indem die Öffnungsklauseln der DSGVO konstruktiv genutzt werden.

- eine Aufsichtsstruktur, die unabhängig agiert und sich mit der Abwägung von Grundrechten auskennt.
- Experimentierräume in Form von behördlich kontrollierten Reallaboren, die die Erprobung innovativer Datennutzungen ausloten, ohne den Grundrechtsschutz Betroffener zu vernachlässigen. Ein solches Reallaborgesetz sollte den Rahmen zur Zusammenarbeit zwischen den an der Beaufsichtigung der Reallabore beteiligten Behörden und die Vernetzung zwischen Europa, Bund, Ländern und Aufsichtsbehörden beschreiben – vor allem, aber nicht nur im KI-Umfeld.

5. Die von der DSK erstellten Kriterien für Souveräne Clouds zu berücksichtigen und das Datenschutzcockpit zügig weiter auszubauen.

Eine bürgerfreundliche und datenschutzkonform digitalisierte Verwaltung ist Grundbedingung für einen modernen Staat und eine moderne Wirtschaft. Eine weitere Grundvoraussetzung ist digitale Souveränität. Dazu müssen IT-Lösungen auch die Einhaltung der datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft sicherstellen. In Bezug auf den Einsatz von Souveränen Clouds hat die DSK Kriterien formuliert, die erfüllt sein sollten oder müssen, um von einer „Souveränen Cloud" sprechen zu können.[5] Dazu zählen:

- Nachvollziehbarkeit durch Transparenz
- Datenhoheit und Kontrollierbarkeit
- Offenheit
- Vorhersehbarkeit und Verlässlichkeit
- regelmäßige Prüfung der aufgestellten Kriterien

Die Fortentwicklung der Registermodernisierung setzt voraus, dass auch das Datenschutzcockpit zügig ausgebaut wird. Das Datenschutzcockpit ist ein notwendiges Transparenz- und Steuerungsinstrument für die einzelnen Bürgerinnen und Bürger, um die Kontrolle über Datenflüsse und -verarbeitungen in einer digitalisierten Verwaltung zu behalten.

5 Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023: Kriterien für Souveräne Clouds, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kriterien-Souv-Clouds.pdf

2. Beschlüsse der Datenschutzkonferenz 2025

12.12.2025 – Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz (OZG)

1. *Die DSK empfiehlt den gemäß § 8a OZG Verantwortlichen in Bund und Ländern zur Sicherstellung der Datenschutzkonformität der von ihnen entwickelten OZG-Dienste, den diesem Beschluss beigefügten standardisierten Prüfprozess der DSK zu Grunde zu legen.*
2. *Sofern und soweit die jeweils zuständige Aufsichtsbehörde einen länderübergreifenden Onlinedienst gemäß § 8a OZG bewertet, orientiert sie sich an dem standardisierten Prüfprozess als Maßstab.*
3. *Der standardisierte Prüfprozess dient dazu, einen einheitlichen und transparenten Standard im Hinblick auf die Datenschutzprüfung zu etablieren.*

Hinweis: Das Dokument „Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz (OZG)" ist abrufbar unter **www.datenschutzkonferenz-online.de/beschluesse-dsk.html**.

16.06.2025 – Datenschutz bei der Terminverwaltung durch Heilberufspraxen - Positionspapier zum datenschutzkonformen Einsatz von Dienstleistern für Online-Terminbuchungen und das Terminmanagement

Terminvereinbarungen mit Heilberufspraxen finden zunehmend über das Internet statt. Dabei übernehmen häufig externe Dienstleister das Terminmanagement für die Praxen. Dies ist unterschiedlich organisiert: Teilweise buchen die Patientinnen und Patienten die von ihnen gewünschten Termine auf der Homepage der einzelnen Praxis über einen dort eingebetteten Terminbuchungsbutton, der technisch von einem externen Dienstleister betrieben wird; teilweise werden die Termine über die Plattform eines Terminverwaltungsunternehmens gebucht. Die auf diese Weise gebuchten sowie von der Heilberufspraxis selbst eingetragenen Termine (z. B. bei telefonischer Terminvereinbarung) werden in dem von dem Dienstleister bereitgestellten Terminkalender der Praxis verarbeitet.

Die Auslagerung der Terminverwaltung geht einher mit der externen Verarbeitung von Patientendaten durch die von den Heilberufspraxen beauftragten Dienstleister. Sowohl bei Praxisbetreiberinnen und -betreibern als auch Patientinnen und Patienten besteht Unsicherheit, unter welchen Voraussetzungen externe Dienstleister in die Terminverwaltung eingebunden und in welchem Umfang dabei Patientendaten verarbeitet

werden dürfen. Die zunehmende Anzahl der bei den Datenschutzaufsichtsbehörden eingehenden Beratungsanfragen und Beschwerden belegt dies.

Die Datenschutzkonferenz greift mit diesem Positionspapier den bestehenden Bedarf nach datenschutzrechtlicher Klarstellung und Beratung auf. Die in dem Papier enthaltenen Positionen spiegeln die Rechtsauffassung der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder wider. Sie dienen als Maßstab für datenschutzrechtliche Bewertungen in aufsichtsrechtlichen Verfahren und zugleich der Orientierung für Heilberufspraxen, Terminverwaltungsunternehmen sowie Patientinnen und Patienten.

1. Zulässigkeit der Auslagerung der Terminverwaltung durch Heilberufspraxen

Die Beauftragung von externen Unternehmen zum Terminmanagement durch Heilberufspraxen kann als Auftragsverarbeitung im Sinne von Art. 28 DSGVO zulässig sein. Sie bedarf auf dieser Grundlage keiner Einwilligung durch die Patientinnen und Patienten. Allerdings sind diese durch die Heilberufspraxis über die Einbindung des Dienstleisters zu informieren (Art. 13 DSGVO, s.u.).

Neben der digitalen Terminvereinbarung sollte auch immer eine alternative Möglichkeit bestehen, einen Termin in der Heilberufspraxis vereinbaren zu können (siehe DSK Entschließung vom 19.12.2024 zur menschenzentrierten Digitalisierung).

2. Anforderungen an eine datenschutzkonforme Verarbeitung von Patientendaten im Zusammenhang mit der Terminvergabe

Soweit Heilberufspraxen zur Vergabe von Behandlungsterminen Patientendaten verarbeiten, ist dies datenschutzrechtlich zulässig, sofern die Heilberufspraxis die entsprechenden Datenverarbeitungen auf eine Rechtsgrundlage – also entweder eine gesetzliche Regelung oder eine Einwilligung - stützen kann. Werden zur Terminverwaltung externe Dienstleister eingesetzt, ändert sich an dieser datenschutzrechtlichen Vorgabe nichts. Je nachdem, um welche Datenverarbeitung es geht, ist zu differenzieren:

- Nur erforderliche Datenverarbeitungen sind ohne Einwilligung zulässig

  Datenverarbeitungen, die für die medizinische Behandlung erforderlich sind, können Heilberufspraxen auf Art. 6 Abs. 1 Satz 1 lit. b und Art. 9 Abs. 2 lit. h DS-GVO stützen.

  Das Eintragen von Patientendaten in einen Terminkalender ist für die Behandlung erforderlich, wenn die konkrete Patientin oder der

konkrete Patient einen in der Zukunft liegenden Termin in der Praxis vereinbart. Eingetragen werden dürfen nur diejenigen Patientendaten, die zur Wahrnehmung des konkreten Termins erforderlich sind, also insbesondere Name, Geburtsdatum, behandelnde Ärztin oder behandelnder Arzt, Art des Termins (z. B. Kontrolle, Röntgen) und eine Kontaktmöglichkeit zur eventuell notwendigen kurzfristigen Absage des Termins. Erforderlich im datenschutzrechtlichen Sinne bedeutet, dass die Daten für das Terminmanagement unbedingt notwendig sein müssen.

- Keine pauschale Übermittlung aller Patientenstammdaten an den Dienstleister im Vorfeld

  Zur Durchführung der Terminvergabe durch einen Dienstleister bedarf es nur der zur Vereinbarung eines konkreten Termins erforderlichen Patientendaten. Termindaten werden bei einer Online-Terminvereinbarung regelmäßig durch die Patientinnen und Patienten selbst mitgeteilt oder bei einer Terminvereinbarung vor Ort oder telefonisch durch die Heilberufspraxis erhoben und in den Terminkalender eingetragen. Vor diesem Hintergrund bedarf es im Vorfeld im Regelfall insoweit keiner pauschalen Bereitstellung von Stammdaten aller in der Heilberufspraxis jemals behandelten Patientinnen und Patienten an das beauftragte Dienstleistungsunternehmen.

- Terminnachrichten nur mit ausdrücklicher Einwilligung

  Für die Wahrnehmung des konkreten Termins nicht erforderlich, allerdings als erweitertes Serviceangebot durchaus denkbar, ist die Versendung einer an die Patientinnen und Patienten gerichteten Terminnachricht (z. B. Terminerinnerung). Sofern die Patientinnen und Patienten auf Nachfrage und entsprechend informiert damit einverstanden sind, dürfen die zu diesem Zweck erforderlichen Kontaktdaten – je nach gewähltem Kommunikationskanal – zusätzlich verarbeitet werden. Die Heilberufspraxis muss nachweisen können, dass die Einwilligung vorliegt.

- Keine Datenverarbeitung von Patientendaten, die Gegenstand der Auftragsverarbeitung sind, zu eigenen Zwecken des Terminverwaltungsunternehmens

  Die Verarbeitung der im Rahmen der Beauftragung durch die Heilberufspraxen stehenden Patientendaten richtet sich gemäß Art. 28 DS-GVO ausschließlich nach den Weisungen der Heilberufspraxis und dem anzuschließenden Auftragsverarbeitungsvertrag. Dementsprechend ist eine weitere Verarbeitung der im Terminkalender eingetragenen Patientendaten durch das Terminverwaltungsunternehmen zu eigenen Zwecken unzulässig. Bei Kenntnis einer Verwendung dieser Daten für eigene Zwecke des Dienstleisters ist die Heilberufspraxis verpflichtet, gegenüber ihrem Dienstleister dafür zu sorgen, dass dieser einen datenschutzkonformen Zustand herstellt.

- Eintragungen im Terminkalender sind innerhalb einer kurzen Frist nach dem Termin zu löschen

  Die zur Terminvergabe zulässigerweise erhobenen Patientendaten dürfen nur solange gespeichert werden, wie dies zur Erreichung des Verarbeitungszwecks erforderlich ist. Sobald der in den Terminkalender eingetragene Termin verstrichen ist, besteht im Regelfall keine Erforderlichkeit mehr, in dem Terminkalender weiterhin die Termindaten des Patienten oder der Patientin zu speichern. Denn Eintragungen im Terminkalender sind als solche nicht Teil der Behandlungsdokumentation und unterliegen somit nicht der berufsrechtlichen Dokumentationspflicht; soweit Inhalte des Terminkalenders dokumentationspflichtig sind, sind diese in die Dokumentation zu übernehmen und dort in der gebotenen Weise zu speichern. Aus dem Terminkalender selbst sind diese Daten dagegen grundsätzlich innerhalb einer kurzen Frist zu löschen. Erfolgt die Terminvergabe durch einen beauftragten Dienstleister, hat dieser die erforderliche Löschung zu gewährleisten.

- Datenschutz ist durch technisch-organisatorische Maßnahmen sicherzustellen

  Die Heilberufspraxen als datenschutzrechtlich Verantwortliche müssen durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass die Vorgaben des Datenschutzes auch bei der Verarbeitung von Patientendaten zur Terminvergabe und -verwaltung eingehalten werden. Dies gilt sowohl bei der Terminvergabe und -verwaltung durch die Praxen selbst als auch bei der Einbindung externer Dienstleister. In diesem Fall müssen die Maßnahmen im Rahmen der Beauftragung vertraglich festgelegt werden.

  Die Heilberufspraxen haben als Verantwortliche deshalb im Vorfeld der Beauftragung insbesondere zu prüfen,

  - welche Patientendaten auf welcher Rechtsgrundlage verarbeitet werden,
  - ob eine Datenverarbeitung im Rahmen des Auftrags und nicht darüber hinaus zu eigenen Zwecken des Dienstleisters erfolgt,
  - dass geeignete Maßnahmen zum angemessenen Schutz der Patientendaten – insbesondere hinsichtlich der Sicherheit der Webanwendung und der Verzahnung des Praxisverwaltungssystems mit dem System des Dienstleisters sowie einer vorhandenen Mandantentrennung beim Dienstleister – ergriffen werden,
  - dass ausreichende Gewähr für die Vertraulichkeit der Verarbeitung durch den Dienstleister geboten wird und
  - dass die Löschvorgaben umgesetzt werden.

- Besondere Anforderungen bei einer Datenverarbeitung in Drittstaaten

  Sofern in die Datenverarbeitung zur Terminvergabe und -verwaltung auch Stellen in einem Drittland i.S.v. Art. 44 DSGVO eingebunden sind, müssen die in diesem Zusammenhang bestehenden besonderen datenschutzrechtlichen Anforderungen der Art. 44 ff. DSGVO durch die Heilberufspraxen als Verantwortliche sichergestellt werden. Vor der Auftragsvergabe ist daher durch die Praxen mit dem Dienstleister zu klären, ob einzelne Verarbeitungsschritte, wie z. B. Support, Wartung oder Administration, in einem Drittland stattfinden und ob in diesem Fall die o. g. Anforderungen erfüllt sind.

- Bereitstellung von aussagekräftigen Informationen über die externe Terminvereinbarung und -verwaltung

  Angesichts der Informationspflicht nach Art. 13 f. DS-GVO sind die Heilberufspraxen verpflichtet, ihre Patientinnen und Patienten über die im Zusammenhang mit der Auslagerung der Terminvergabe und -verwaltung stehenden Datenverarbeitungen zu informieren. Dabei ist insbesondere das konkret beauftragte Terminverwaltungsunternehmen als Empfänger der Daten namentlich zu benennen.

3. Vertragsverhältnis zwischen Patientinnen und Patienten mit Dienstleistern zur Online-Terminbuchung

Sofern einzelne Terminverwaltungsunternehmen ihre Dienstleistung gegenüber Heilberufspraxen in der Art anbieten, dass die Patientinnen und Patienten ein Nutzerkonto bei dem Unternehmen (ggf. unter Zustimmung zu den AGB des Dienstleisters) anlegen können, ist die damit zusammenhängende Verarbeitung personenbezogener Daten durch das Terminverwaltungsunternehmen von der unter Nr. 2 dargestellten Datenverarbeitung im Auftrag der Heilberufspraxen abzugrenzen. Für die Verarbeitung personenbezogener Daten von Patientinnen und Patienten im Zusammenhang mit dem Vertrag, den sie mit dem Terminverwaltungsunternehmen schließen, und dem Nutzerkonto ist das Terminverwaltungsunternehmen datenschutzrechtlich Verantwortlicher. Werden hierbei auch Gesundheitsdaten verarbeitet, benötigt das Terminverwaltungsunternehmen im Regelfall eine wirksame Einwilligung der betroffenen Nutzerinnen und Nutzer.

Dem Terminverwaltungsunternehmen obliegt insoweit die Erfüllung sämtlicher datenschutzrechtlicher Vorgaben. Dabei ist eine saubere Trennung der Verantwortlichkeiten erforderlich, die auch für die Patientinnen und Patienten klar erkennbar sein muss. Die Patientinnen und Patienten müssen bei jeder Interaktion mit der Website, die sie nutzen, um mit der Praxis einen Termin zu vereinbaren, in der Lage sein, zu erkennen, wer für die jeweilige Datenverarbeitung verantwortlich ist.

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
DSK	Konferenz der unabhängigen Datenschutz-aufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz)
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DS-GVO	Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss (englisch: European Data Protection Board: EDPB)
IFG NRW	Informationsfreiheitsgesetz Nordrhein-Westfalen
JI-Richtlinie	Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016
KI-VO	Verordnung (EU) 2024/1689 - Verordnung über künstliche Intelligenz
lit.	Buchstabe
TKG	Telekommunikationsgesetz
UAbs.	Unterabsatz

Bildnachweise

Abbildung 1 | Seite 7 – LDI NRW;
Abbildung 2 | Seite 11 – PantherMedia / artjazz;
Abbildung 3 | Seite 14 – PantherMedia / Vanessa_1;
Abbildung 4 | Seite 17 – PantherMedia / agsandrew;
Abbildung 5 | Seite 22 – PantherMedia / kentoh;
Abbildung 6 | Seite 28 – PantherMedia / Rawpixel;
Abbildung 7 | Seite 31 – PantherMedia / Yuri Arcurs;
Abbildung 8 | Seite 35 – PantherMedia / daisy-daisy;
Abbildung 9 | Seite 38 – PantherMedia / AndreyPopov;
Abbildung 10 | Seite 46 – PantherMedia / rclassenlayouts;
Abbildung 11 | Seite 52 – PantherMedia / Nathan0834;
Abbildung 12 | Seite 61 – iStock.com/ Minerva Studio;
Abbildung 13 | Seite 68 – iStock.com / kynny;
Abbildung 14 | Seite 73 – iStock.com / ronstik;
Abbildung 15 | Seite 80 – iStock.com / Tevarak;
Abbildung 16 | Seite 85 – Europäische Union;
Abbildung 17 | Seite 89 – PantherMedia / Melpomene;
Abbildung 18 | Seite 94 – PantherMedia / DTatiana
Abbildung 19 | Seite 102 – PantherMedia / Denniro;
Abbildung 20 | Seite 107 – PantherMedia / aldona_k;
Abbildung 21 | Seite 111 – iStock.com / Charday Penn;
Abbildung 22 | Seite 118 – iStock.com / Oselote;
Abbildung 23 | Seite 123 – PantherMedia / Andriy Popov;

Impressum

Herausgeberin:
Bettina Gayk
Landesbeauftragte für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

Kavalleriestraße 2–4
40213 Düsseldorf

Tel.: 0211 / 384 24 - 0
Fax: 0211 / 384 24 - 999
E-Mail: poststelle@ldi.nrw.de

Dieser Bericht kann unter www.ldi.nrw.de abgerufen werden.
Zitiervorschlag: 31. Bericht LDI NRW
ISSN: 0179–2431
Düsseldorf 2026
Titelbild © Bildagentur PantherMedia / kentoh (YAYMicro)

Layout und Druck:
jva druck+medien, Geldern
www.jva-geldern.nrw.de

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen
www.ldi.nrw.de