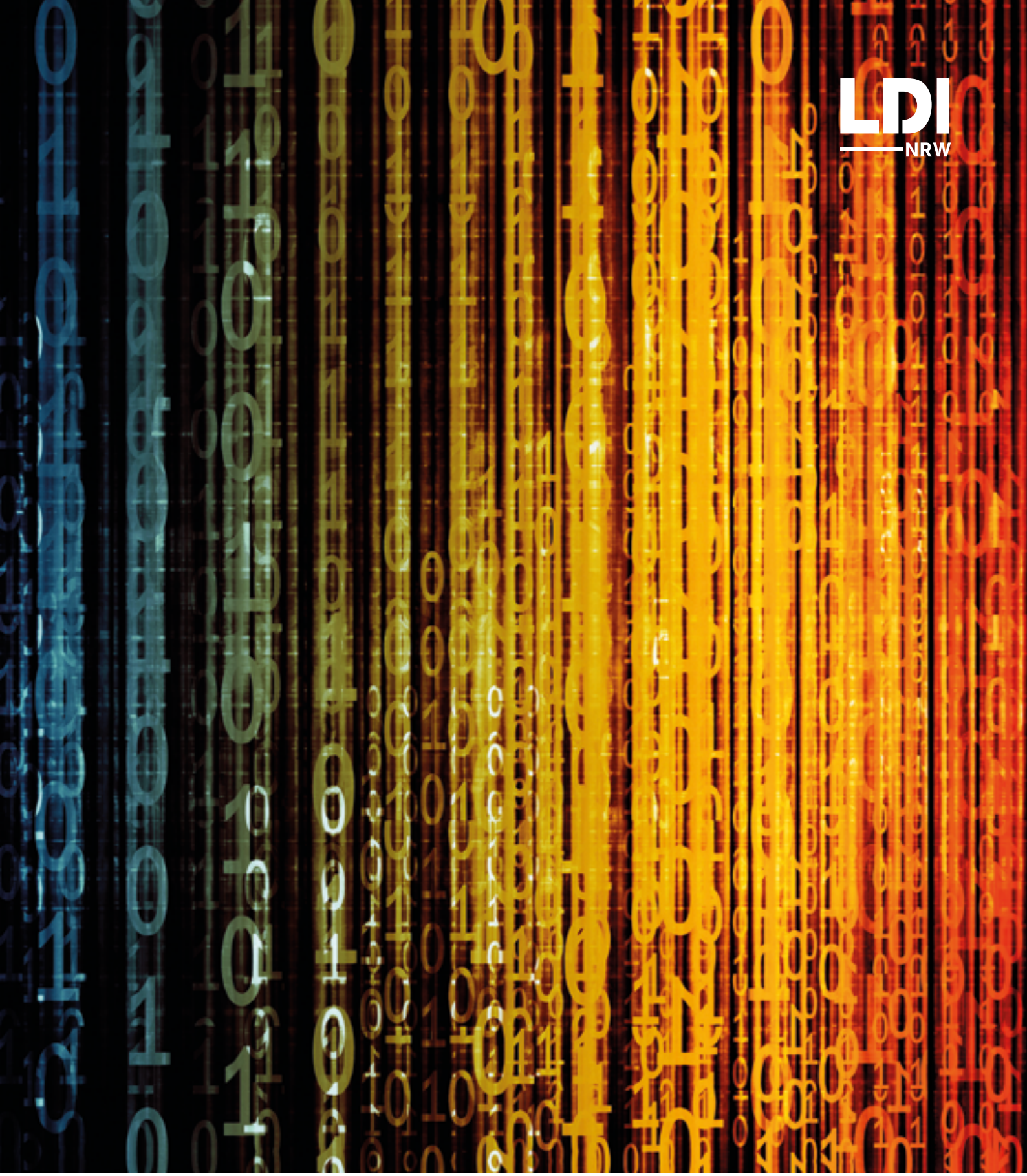


29. Bericht

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Nordrhein-Westfalen

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

zum Datenschutz
für die Zeit vom 1. Januar 2023
bis zum 31. Dezember 2023

Inhalt

Vorwort

Bettina Gayk
Landesbeauftragte für
Datenschutz und Informationsfreiheit

Sie halten einen neu gestalteten Bericht in den Händen. Nicht nur das Format hat eine andere Größe erhalten. Auch innen sieht es etwas aufgelockerter aus. Inhaltlich möchte ich stärker als bisher die Anteile der Aufgaben meiner Behörde sichtbar machen, die neben der Prüfung von Einzelbeschwerden ganz wesentlich unsere Arbeit prägen.

Dies sind unter anderem Beratungen, die wir durchführen. Hier möchte ich auf das immer wichtiger werdende Thema KI hinweisen, zu dem unsere Beratung zunehmend nachgefragt wird. Inzwischen auch über die Medien bekannt geworden ist der kassenlose Supermarkt. Dieser ermöglicht das Einkaufen ohne Warteschlange, geht aber einher mit einer umfassenden Videoüberwachung im jeweiligen Supermarkt. Ein bequemes Einkaufserlebnis so zu gestalten, dass die Persönlichkeitsrechte der Kund*innen nicht zu kurz kommen, ist unter diesen Umständen anspruchsvoll. Entsprechend umfassend haben wir hier beraten. Laufend werden wir auch zum Technikeinsatz in Schulen und Hochschulen befragt. Hierzu finden Sie Beispiele im Bericht. Es ist uns ein wichtiges Anliegen, den Überwachungsdruck gerade bei den Lernenden gering zu halten. Ein Beispiel für eine an Bürger*innen gerichtetes Beratungsinstrument sind unsere FAQ bei Datenpannen, die wir neben vielen anderen laufend aktuellen Informationen über unsere Website bereitstellen.

Durch die DS-GVO sind alle unabhängigen Datenschutzaufsichtsbehörden darauf verpflichtet, die Regelungen der Verordnung einheitlich anzuwenden. In Europa wird dies durch den Europäischen Datenschutzausschuss (EDSA) und seine Fachuntergruppen (Expert Subgroups) gewährleistet. Hier arbeiten die jeweiligen Fachleute aus meiner Behörde in vielen Bereichen mit und tragen so aktiv dazu bei, dass eine rechtssichere und einheitliche Anwendung der DS-GVO gelingt. Sehr aktiv sind wir beispielsweise im Themenfeld der Selbstregulierung. Nach gewissen Anlaufschwierigkeiten tut sich hier inzwischen einiges. Wir haben das erste deutsche Zertifizierungsverfahren im EDSA abstimmen können und konnten im Anschluss die erste deutsche Zertifizierungsstelle akkreditieren. Diese bietet Auftragsverarbeitern nun die Möglichkeit der Zertifizierung ihrer Verfahren. Unternehmen oder andere Stellen, die Auftragsverarbeiter nutzen wollen, können deren Eignung nunmehr aufgrund der Zertifikate besser beurteilen.

Immer mehr Verbände entschließen sich auch dazu, über Verhaltensregeln (Codes of Conduct) die bereichsspezifische Anwendung der DS-GVO mit den Datenschutzaufsichtsbehörden zu klären. Die erste Überwachungsstelle in Deutschland, die die Verhaltensregeln der Auskunfteien überwacht, hat ihren Sitz in NRW und wurde von uns genehmigt. Die Erfahrung aus dieser Genehmigung sind in ein grundlegendes Papier der Datenschutzkonferenz eingeflossen, das für interessierte Verbände nachvollziehbar erläutert, worauf sie bei der Einrichtung der Überwachungsstelle für ihren Code of Conduct achten müssen.

Die Datenschutzkonferenz (DSK) hat eine große Bedeutung für die einheitliche Rechtsanwendung innerhalb Deutschlands. Deswegen arbeiten wir mit den Kolleg*innen im Bund und in den anderen Bundesländern sehr eng und intensiv zusammen. Die DS-GVO gibt Verfahren und Strukturen für die Zusammenarbeit der unabhängigen Datenschutzaufsichtsbehörden vor, wenn Datenverarbeitungen über europäische Grenzen hinweg gehen. Dagegen lässt das BDSG entsprechende Regelungen vermissen. Mit einer laufenden Gesetzesänderung des BDSG soll die DSK nunmehr institutionalisiert werden. Leider sind dabei keine konkreten Verfahren und Zielsetzungen dieser Institutionalisierung vorgesehen. Es gibt keinerlei Anhaltspunkte, wie die einheitliche Rechtsanwendung der DS-GVO unter unabhängigen Datenschutzaufsichtsbehörden national gelingen soll. Dieses Vakuum hat die DSK durch eine Änderung ihrer Geschäftsordnung teilweise gefüllt und über das Instrument der Selbstbindung der Verwaltung ein Verfahren entwickelt, das zu wichtigen Rechtsfragen weitgehende Einigkeit erzielen soll.

Die Fragestellungen, bei denen Abstimmungen über die Rechtsanwendung notwendig sind, sind vielfältig und häufig drängend, weil die Wirtschaft verlässliche Antworten benötigt, ob und wie sie neue Verfahren einsetzen kann. Daneben ist die Rechtssetzung mit Bezug zu Datenverarbeitungsprozessen rasant und erfordert eine enge Abstimmung von Datenschutzstandpunkten in der DSK. Allen voran ist hier die Gesetzgebung im Gesundheitssektor zu erwähnen, bei der es eine enge Zusammenarbeit in der DSK gibt, auf die der Bericht eingeht.

Die nationale Umsetzung der Datenstrategie der Europäischen Union erfordert laufend neue gesetzliche Regelungen mit Einfluss auf die Datenschutzaufsichtsbehörden. Dabei sind die Effekte auf die Datenschutzaufsicht in Bund und Ländern unterschiedlich. Es ist ein Trend zur Zentralisierung von Aufgaben beim Bund zu beobachten. Dies kann zur Zersplitterung einheitlicher Lebenssachverhalte führen, die bisher durch die Datenschutzaufsichten der Länder beurteilt werden. Dank der Unterstützung des für Digitalisierung zuständigen Ministeriums konnte diese Problematik im Fall des Digitale-Dienste-Gesetzes im Gesetzgebungsverfahren gegenüber dem Bund adressiert werden. Weitere Einzelheiten finden Sie dazu in diesem Bericht.

Nach Inkrafttreten der DS-GVO mit ihrem Anspruch auf einheitliche Anwendung ist der Abstimmungsbedarf in der DSK sehr hoch geworden. Die Taktung der Themen ist eng, oft zeitkritisch und inhaltlich anspruchsvoll. Wer den jährlich wechselnden Vorsitz der DSK übernimmt, muss sich durch eine Geschäftsstelle aus dem eigenen Haus unterstützen lassen. Das Personal des Vorsitzes steht für die planmäßigen Aufgaben der Datenschutzaufsichtsbehörde nicht mehr zur Verfügung und wird erst im Laufe des Vorsitzjahres in die Aufgaben eingearbeitet sein.

Mit der beabsichtigten Institutionalisierung der DSK wird der Anspruch an ihre Leistungsfähigkeit noch zunehmen. Daher bedarf es einer kontinuierlichen Unterstützung des Konferenzvorsitzes, die nur eine ständige Geschäftsstelle gewährleisten kann. Die DSK hatte sich bereits frühzeitig dafür ausgesprochen, dass die Institutionalisierung der DSK mit der gesetzlichen Einrichtung und Garantie einer Geschäftsstelle der DSK einher gehen muss. Eine solche Geschäftsstelle, die bei einer Datenschutzaufsichtsbehörde angesiedelt sein könnte, aber dem jeweiligen Konferenzvorsitz zuarbeitet, gewährleistet professionelle, kontinuierliche und jederzeit nachvollziehbare Arbeit der DSK und kann einheitliche Ansprechstelle für Politik, Verwaltung, Wirtschaft, Verbände und NGOs zur DSK sein. Sie kann dabei auch einheitliche Schnittstellen für den Kontakt mit einzelnen Aufsichtsbehörden erarbeiten, etwa bei der Meldung von Datenpannen. Leider hat das Thema im Gesetzgebungsverfahren zur Änderung des BDSG bisher keinen Eingang gefunden. Die Einrichtung einer solchen Geschäftsstelle auch über eine Verwaltungsvereinbarung wäre denkbar, wenn dazu keine Regelung im BDSG getroffen würde.

Mir ist dieses Anliegen sehr wichtig und ich würde mich freuen, wenn ich hier im Lande dafür Unterstützung erhalten würde.

Im Laufe des letzten Jahres haben wir die erste Stufe der Umstrukturierung des Hauses umgesetzt, die uns unter anderem die Stellenzuweisung durch den Landtag ermöglicht hat. Auch dies hat einen Teil unserer Arbeit im zurückliegenden Jahr ausgemacht. Deswegen geben wir auch darüber einen kurzen Überblick im Bericht.

Abschließen möchte ich mit dem Hinweis, dass wir weder über die Finanzverwaltung noch über den Gebühreneinzug der Rundfunkanstalten berichten. In der Diskussion über meinen vorherigen Bericht im Landtag war das kritisiert worden. Ich darf daher darauf aufmerksam machen, dass ich für diese Bereiche keine Kontrollzuständigkeit besitze.
Ich wünsche Ihnen eine interessante Lektüre.

Bettina Gayk
Frühjahr 2024

1. Zusammenarbeit in Europa

Die von der DS-GVO angestrebte Symphonie des europäischen Datenschutzrechts mit ausbalancierten Interessen von Wirtschaft, Behörden und Verbraucher*innen verlangt einen Ort des Zusammenkommens, und manchmal auch ein*e Dirigent*in. Die Musik spielt hier beim Europäischen Datenschutzausschuss, einer Einrichtung mit einem Sekretariat in Brüssel, die von der EU unabhängig ist. Der EDSA setzt sich aus den Leiter*innen aller Aufsichtsbehörden im Europäischen Wirtschaftsraum sowie dem Europäischen Datenschutzbeauftragten zusammen. Der EDSA erstellt unter anderem Leitlinien sowie Stellungnahmen und trifft insbesondere auch verbindliche Entscheidungen.

Der EDSA hat in seiner Strategie bis 2027 die Ziele seiner Arbeit in sog. Säulen festgelegt, und dabei die wichtigsten Maßnahmen pro Säule benannt:

- Säule 1 – Verbesserung der Harmonisierung und Förderung der Einhaltung
- Säule 2 – Stärkung einer gemeinsamen Durchsetzungskultur und der wirksamen Zusammenarbeit
- Säule 3 – Schutz des Datenschutzes in der sich entwickelnden digitalen und aufsichtsübergreifenden Landschaft
- Säule 4 – Beitrag zum globalen Datenschutzdialog

Der strategische Plan knüpft an die Prioritäten der Vorjahre an. Neu ist der besondere Fokus auf das Zusammenspiel mit dem digitalen Regulierungsrahmen der EU (Europäische Datenstrategie). Neue Gesetze, wie das Gesetz über digitale Märkte (DMA) oder das Gesetz über digitale Dienste (DSA), haben Auswirkungen auf den Datenschutz und die Privatsphäre. Der EDSA beabsichtigt, die Zusammenarbeit mit anderen Regulierungsbehörden zu verbessern, um das Recht auf Datenschutz in die allgemeine Regulierungsarchitektur einzubetten. Darüber hinaus wird sich der EDSA auch weiterhin

auf die Herausforderungen konzentrieren, die sich durch neue Technologien wie KI ergeben.

Der Europäische Datenschutzausschuss 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,
- Compliance, E-Government & Health (CEH),
- Financial Matters und
- Technology (seit 2024)

aktiv und vertritt dort die deutschen Aufsichtsbehörden.
Die erste Ländervertretung der Key Provisions ESG hat eine Mitarbeiterin der LDI NRW im Berichtsjahr übernommen. Diese ESG befasst sich mit den Schlüsselthemen der DS-GVO und entwickelt dazu grundlegende Empfehlungen. Diesen Arbeiten kommt eine besondere Bedeutung im Hinblick auf die einheitliche Rechtsanwendung zu. Aktuell setzt sich die ESG mit der Frage auseinander, unter welchen Rahmenbedingungen ein berechtigtes Interesse eine Datenverarbeitung legitimieren kann. Wie weit insbesondere Unternehmen ihre berechtigten Interessen zur Legitimation ihrer Datenverarbeitung heranziehen können ist eine zentrale Frage des Datenschutzes in der Wirtschaft.

In der CEH ESG hat die LDI NRW als Berichterstatterin an dem Entwurf der Stellungnahmen zu nationalen Zertifizierungskriterien und zu den europäischen Datenschutzsiegeln mitgewirkt. Zertifizierungen sind ein nützliches Instrument für die Wirtschaft, die sich vergewissern will, dass die eigene Datenverarbeitung rechtskonform ist. Siehe dazu den Beitrag 13.a – Zertifizierungskriterien: EDSA-Dokument beschleunigt Genehmigungsverfahren.

Der EDSA trägt zur einheitlichen Anwendung der DS-GVO durch die Bereitstellung solcher Stellungnahmen und Orientierungshilfen bei, darunter Leitlinien, Empfehlungen und bewährte Verfahren.

An dieser Stelle möchten wir besonders auf die EDSA-Leitlinien zum Auskunftsrecht sowie zum Einsatz von Gesichtserkennungstechnologie im Anwendungsbereich der JI-Richtlinie hinweisen.

EDSA-Leitlinien zum Auskunftsrecht

In seinen Leitlinien zum Auskunftsrecht nach Art. 15 DS-GVO gibt der EDSA eine umfassende Hilfestellung für die einheitliche Anwendung des Auskunftsrechts im Geltungsbereich der DS-GVO. Das Auskunftsrecht ist das zentrale Datenschutzrecht, das Betroffene in die Lage versetzt, die Konsequenzen der Verarbeitung sie betreffender Daten zu überschauen. Für die Daten verarbeitenden Stellen kommt es darauf an, dass sie die rechtlichen Verpflichtungen zur Auskunft kennen, um sich rechtskonform zu verhalten und nicht der Gefahr eines Bußgeldes auszusetzen. Um sich über die richtige rechtliche Anwendung zu vergewissern, können Sie nun auf die Empfehlung zurückgreifen. Da diese Leitlinien in der Key Provisions ESG vorbereitet wurden, hat die LDI NRW intensiv daran mitgewirkt. Die Leitlinien sind unter www.edpb.europa.eu abrufbar. Zu den Leitlinien und weiteren Informationen zu Art. 15 DS-GVO siehe auch den Beitrag 6. – Konkretisierung des Auskunftsrechts – EuGH-Rechtsprechung und EDSA-Leitlinien.

EDSA-Leitlinien zum Einsatz von Gesichtserkennungstechnologie im Anwendungsbereich der JI-Richtlinie

Gegenstand der „Guidelines on the use of facial recognition technology in the area of law enforcement - Version 2.0“ ist der Einsatz von Gesichtserkennungstechnologie im Anwendungsbereich der JI-Richtlinie, also insbesondere durch Sicherheitsbehörden zur Strafverfolgung oder zur damit zusammenhängenden Gefahrenabwehr. Die Leitlinien sind unter www.edpb.europa.eu abrufbar.

Der Einsatz von Gesichtserkennungstechnologie ist immer mit der Verarbeitung biometrischer Daten verbunden, die grundsätzlich nicht geändert werden können. Sie sind damit von besonderer Sensibilität. Die datenschutzrechtliche Kritikalität steigt noch, wenn diese Daten zur Strafverfolgung oder Gefahrenabwehr eingesetzt werden. Da dies vielfach dann sogar heimlich erfolgt, sind klare Regeln für den Einsatz einer solchen Technologie besonders wichtig. Die Leitlinien geben auf knapp 50 Seiten Hilfestellungen für die Gesetzgebung und für verantwortliche Stellen zu Einsatzmöglichkeiten. Praktische Hilfestellungen zum Einsatzmanagement solcher Technologien und Beispielsfälle enthalten die Annexe der Leitlinie, die die Bewertung der rechtlichen Zulässigkeit einzelner Projekte erleichtern sollen.

2. Zusammenarbeit in Deutschland

Die Aufsichtsbehörden in Deutschland stimmen sich in der Datenschutzkonferenz (DSK) ab. Hier bearbeiten die Datenschutzaufsichtsbehörden des Bundes und der Länder wichtige Datenschutzthemen und streben einen einheitlichen Datenschutz in Deutschland an. Im Berichtsjahr hatte Schleswig-Holstein den Vorsitz inne und einen Schwerpunkt bei der effektiven Zusammenarbeit gesetzt. Die DSK traf sich unter anderem in Kiel und Lübeck.

Die DSK hat zur Unterstützung ihrer Arbeit Arbeitskreise eingerichtet. Im Rahmen der DSK leitet die LDI NRW die Arbeitskreise

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

Über unsere Vorsitze der Arbeitskreise wurden mehrere fachliche Impulse an die DSK geleitet.

Die Beschlüsse und Entschließungen des Jahres 2023 sind im Anhang abgedruckt. Diese und alle weiteren Veröffentlichungen sind auch auf der Website der Datenschutzkonferenz www.datenschutzkonferenz-online.de abrufbar.

Smart Meter beim Wasserverbrauch

Auf Initiative des von der LDI NRW geleiteten Arbeitskreises Wirtschaft hat die Datenschutzkonferenz den Appell an den Bundesgesetzgeber gerichtet, dass spezialgesetzliche und möglichst bundesweit einheitliche Regelungen für die Datenverar-

beitung im Zusammenhang mit funkbasierten Kaltwasserzählern geschaffen werden, vergleichbar den Regelungen für den Strom- und Wärmeverbrauch.

Die voranschreitende technische Entwicklung der Funkmesstechnik (Smart Meter) ermöglicht eine immer weitergehende Erhebung und Auswertung von Daten des Wasser-, Strom- und Wärmeverbrauchs in Privathaushalten. Anders als etwa für Zähler für den Strom- und Wärmeverbrauch fehlen bisher jedoch für funkbasierte Kaltwasserzähler bundesweit geltende einheitliche datenschutzrechtliche Grundlagen für den Einsatz und das Auswerten der Daten. Sofern digitale Funkwasserzähler eine hohe Auslesetaktung ermöglichen oder weitere Verbrauchsdaten verarbeiten, lassen solche Daten jedoch Rückschlüsse auf die Verbrauchsprofile, das Verhalten und die Lebensgewohnheiten der Verbraucher*innen zu. Eine Gefährdung für das Recht auf informationelle Selbstbestimmung der betroffenen Personen ist vor allem dann anzunehmen, wenn die erhobenen Daten mit anderen Erhebungen verknüpft werden oder Unbefugte nicht hinreichend geschützte Daten auslesen können.

Die von der Datenschutzkonferenz geforderten Regelungen sollten unter anderem Aussagen enthalten zu den Verarbeitungszwecken, den Datenkategorien, der Auslesehäufigkeit, dem Einsatz der aktuellen Technologie und den Löschfristen. Die Stellungnahme der Datenschutzkonferenz „Daten der Verbraucherinnen und Verbraucher beim Einsatz von Smart Meter zur Erfassung des Kaltwasserverbrauchs durch einheitliche Regelungen schützen“ vom 11. Mai 2023 ist unter www.datenschutzkonferenz-online.de abrufbar.

Transparenz beim Scoring

Basierend auf den Arbeiten in dem von der LDI NRW geleiteten AK Kreditwirtschaft hat die DSK der Bundesregierung konkrete Vorschläge unterbreitet, wie mehr Transparenz über Scoring geschaffen werden kann. Ausgangspunkt ist der Koalitionsvertrag des Bundes „Mehr Fortschritt wagen – Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit“ für die Legislaturperiode 2021-2025. Dort heißt es: „Wir werden umgehend prüfen, wie die Transparenz beim Kredit-Scoring zugunsten der Betroffenen erhöht werden kann. Handlungsempfehlungen werden wir zeitnah umsetzen“ (Zeilen 5773 bis 5774).

Das ist für Verbraucher*innen, die aufgrund eines schlechten Scores Nachteile im Wirtschaftsverkehr erleiden, ausgesprochen wichtig. Ohne Transparenz über die Verfahren können sie unrichtige Score-Elemente nicht identifizieren und einen möglichen Anspruch auf Löschung dieser Elemente nicht durchsetzen. Die Vorschläge der DSK hat die Bundesregierung weitgehend aufgegriffen. Sie haben Eingang in den Entwurf zur Änderung des BDSG gefunden. Die Vorschläge für Handlungsempfehlungen an die Bundesregierung zur Verbesserung des Datenschutzes bei Scoringverfahren vom 11. Mai 2023 sind unter www.datenschutzkonferenz-online.de abrufbar.

Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten

Die DSK hat mit dem „Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten“ vom 27. September 2023 (Abdruck im Anhang) die datenschutzrechtlichen Aspekte für die Durchführung von Entwicklungs- und Erprobungsfahrten aufgezeigt. Dieses Papier entstand in Kooperation mehrerer Datenschutzaufsichtsbehörden und im Austausch mit dem Verband der Automobilindustrie e. V. Die LDI NRW war als Aufsichtsbehörde für die in NRW ansässigen Automobilhersteller und Zulieferer beteiligt. Siehe dazu den Beitrag 14. f – Autonomes Fahren: Grenzen für Datensammeln bei der Entwicklung.

Positionspapier zu Kriterien für Souveräne Clouds

Das unter der Mitwirkung der LDI NRW entstandene Positionspapier „Kriterien für Souveräne Clouds“ vom 11. Mai 2023 nennt Kriterien, die ein Cloud-Angebot mindestens erfüllen muss (Mindestkriterien), wenn in der Cloud personenbezogene Daten verarbeitet werden sollen. Darüber hinaus gibt es weitergehende Empfehlungen, die eine besonders datenschutzfreundlich und langfristig datenschutzkonforme Cloud auszeichnen. Siehe dazu den Beitrag 15. c. – Wann ist eine „Souveräne Cloud“ tatsächlich souverän?.

Programm P 20 vereinheitlicht und harmonisiert das Informationswesen der Polizei

Mit dem Programm Polizei 2020 (jetzt „P 20“) wird die bisherige polizeiliche Datenhaltung im Bund und in den Ländern vollkommen neu aufgestellt. Betroffen sind sämtliche polizeilich gespeicherten personenbezogene Daten und deren künftige Verarbeitung in polizeilichen Fachanwendungen. Dies birgt im Sinne des Datenschutzes sowohl Chancen als auch Risiken. Das Programm – mit seinen über 30 Teilprojekten – begleitet die LDI NRW mit anderen Aufsichtsbehörden in der AG INPOL als Unterorganisation des AK Sicherheit der DSK.

Anlass für P 20 ist auch, dass die IT der Polizei des Bundes und der Länder über Jahrzehnte organisch gewachsen ist. Es existieren verschiedene Systeme und Verfahren, die nur zum Teil miteinander verbunden sind und nur unzureichend untereinander Daten austauschen können. Die Daten werden nicht flächendeckend nach gleichen Standards erhoben und verwendet. Teilweise müssen Daten nach wie vor aufgrund fehlender Austauschmöglichkeiten mehrfach in unterschiedliche Systeme eingegeben werden.

Mit P 20 soll das Informationswesen der Polizeien des Bundes und der Länder vereinheitlicht und harmonisiert werden. Dazu sollen die verschiedenen Systeme konsolidiert und an zentraler Stelle einheitliche, moderne Verfahren entwickelt werden, die von allen Polizeien nach den gleichen Standards genutzt werden. Ziel ist es, der Polizei nach Maßgabe des Gesetzes und unter besonderer Berücksichtigung des Datenschutzes zu jeder Zeit an jedem Ort die Daten zur Verfügung zu stellen, die für die polizeiliche Arbeit erforderlich sind. Vorgesehen dafür ist ein einheitliches Verbundsystem mit zentraler Datenhaltung im Bundeskriminalamt, wobei der Datenbesitz und damit die Verantwortung für die Daten weiterhin bei den jeweiligen Polizeien des Bundes und der Länder verbleiben. a durch schlechte Datenverarbeitung sowohl die Arbeit der Polizei, als auch die Freiheitsrechte der von der Datenverarbeitung betroffenen gefährdet sein können, hat die weitere datenschutzrechtliche Begleitung des P 20 für uns einen hohen Stellenwert.

3. Zahlen und Fakten

Eingabesituation im Überblick

Im Jahr 2023 haben uns insgesamt rund 11.050 schriftliche Eingaben erreicht, einschließlich Meldungen nach Art. 33 DS-GVO – sog. Datenpannen. Grundsätzlich nicht erfasst haben wir die zahlreichen telefonischen Anfragen.

Im Jahr 2022 waren es rund 10.500 schriftliche Eingaben, 2021 waren es 11.900 und 2020 waren es insgesamt 12.150.
Von den Eingaben waren

- **6.298 Beschwerden** nach Art. 77 DS-GVO,
- **682 Hinweise von Dritten,**
- **819 schriftliche Beratungsanfragen,**
- **20 Begleitungen bei Rechtsetzungsvorhaben,**
- **2 Genehmigungsverfahren,**
- **2.039 Meldungen nach Art. 33 DS-GVO** zu sog. Datenpannen und
- **429 Eingaben ohne Kategorie.**

Beschwerden und Beratungsanfragen

Im Jahr 2023 haben uns 6.298 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.

Eingaben, die auf mutmaßliche Datenschutzverstöße hinweisen, von denen die Einsendenden jedoch nicht selbst betroffen sind, können wir von Amtswegen aufgreifen. Solche **Hinweise von Dritten** haben wir **682** erhalten.

Schriftliche **Beratungsanfragen** haben wir **819** 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 **2.039** erreicht. Im Jahr 2022 waren es 1.829, 2021 waren es 1.841 Meldungen und 2020 waren es 1.775 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).

Abhilfemaßnahmen

Um eine einheitliche 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 Buchstabe i** wurden bei der Zentralen Bußgeldstelle der LDI NRW **111** Bußgeldverfahren eingeleitet bzw. zur weiteren Verfolgung von den Staatsanwaltschaften übernommen. **65** Bußgeldbescheide wurden erlassen und **115** Verfahren wurden durch Rechtskraft, Einstellung oder Gerichtsentscheidungen abgeschlossen. Das höchste Bußgeld betrug 10.000 Euro, der Mittelwert aller Bußgelder 994 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:

- **862** **Hinweise** nach Art. 58 Abs. 1 d),
- **9** **Warnungen** nach Art. 58 Abs. 2 a),
- **28** **Verwarnungen** nach Art. 58 Abs. 2 b),
- **242** **Anweisungen** nach Art. 58 Abs. 2 d),
- **1** **Beschränkung** nach Art. 58 Abs. 2 f).

Davon erfasst sind Verfahren, die bereits in den Vorjahren eingeleitet wurden, während viele im Jahr 2023 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 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 2023 war die LDI NRW in **2.181 Fällen** mit gestarteten IMI-Modulen befasst. Im Jahr 2022 waren es 1.721Fälle sowie in den Jahren 2021 und 2020 jeweils 1.558 Fälle.

Wir hatten bei sieben europäischen Verfahren die Federführung, bei 24 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 2023 wurde die LDI NRW bei mehreren Rechtsetzungsvorhaben beteiligt.

Die LDI NRW ist immer 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 von der Landesregierung beteiligt. Nicht alle Verfahren hatten dabei einen datenschutzrechtlichen Bezug, so dass wir dazu keine inhaltliche Stellungnahme abgegeben haben.

Stellung genommen haben wir bei den folgenden Rechtsetzungsvorhaben:

- Verordnung betreffend Rechtsfragen der Digitalität in Lehre, Wahlen und Gremienarbeit in der Hochschule
- Gesetz zur Übermittlung von Schülerinnen- und Schülerdaten am Übergang von der Schule in den Beruf
- Änderungsverordnung zur Etablierung von Distanzunterricht in den Bildungsgängen des Berufskollegs/ Siebte Verordnung zur Änderung der Ausbildungs- und Prüfungsordnung Berufskolleg
- Siebtes Gesetz zur Änderung des Polizeigesetzes des Landes Nordrhein-Westfalen
- Verordnung zum Nachweis der Zuverlässigkeit, der gesundheitlichen Eignung und zur Prüfung der Sprachkenntnisse bei der Berufszulassung der Gesundheitsfachberufe in Nordrhein-Westfalen
- IMPP Staatsvertrag „Abkommen zur Änderung des Abkommens über die Errichtung und Finanzierung des Instituts für medizinische und pharmazeutische Prüfungsfragen“
- Zweites Gesetz zur Änderung des Landeskrebsregistergesetzes NRW
- Digitale-Dienste-Gesetz
- Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (Einwilligungsverwaltungsverordnung)

Zudem haben wir zwei Stellungnahmen gegenüber dem Bundesverfassungsgericht abgegeben:

- Verfassungsbeschwerdeverfahren gegen § 23 Abs. 6 PolG NRW
- Verfahren gegen § 16a und 17 PolG NRW a.F.

Transparenz

Auf unserer Webseite www.ldi.nrw.de/zahlen-und-daten veröffentlichen wir weitere Informationen.

4. Neue Organisationsstruktur bei der LDI NRW

Im November 2023 hat sich die LDI NRW eine neue Organisationsstruktur gegeben. Sie reagiert damit auf die sich wandelnden Rahmenbedingungen von Datenschutz und Informationsfreiheit und passt die Organisation geänderten Bedürfnissen an.

Aktuelle Rechtsprechung, neues Recht, technische Entwicklungen oder einfach die Bedürfnisse der Bürger*innen, Verwaltung und Wirtschaft – alles zusammen muss von einer Datenschutzaufsichtsbehörde beachtet und bewertet werden. Mit der organisatorischen Umstrukturierung reagiert die LDI NRW auf die gewachsenen Herausforderungen und baut ihre Fachkunde und Entscheidungsgeschwindigkeiten aus. Das Inkrafttreten der DS-GVO und der JI-Richtlinie im Mai 2018 haben für die LDI NRW bereits zu weiteren Aufgaben geführt. Auch die Sensibilität der Bürger*innen für datenschutzrechtliche Fragestellungen ist in allen Arbeitsbereichen der LDI NRW gestiegen. Dies manifestiert sich vor allem in den seit Jahren konstant hohen Eingabezahlen. Ein erster Personalzuwachs war nicht ausreichend, die gestiegene Arbeitsbelastung zu bewältigen. Nicht nur die von der DS-GVO neu hinzugekommenen europaweiten Abstimmungsverfahren mussten bewältigt werden. Die neue Rechtslage hatte auch zu einer Verdreifachung der jährlichen Eingaben geführt. Im weiteren Verlauf sind Klageverfahren hinzugekommen, die von uns geführt werden müssen, falls Bürger*innen mit unseren Entscheidungen nicht einverstanden sind. Eine solche gerichtliche Überprüfung unserer Sachentscheidungen gab es nach der alten Rechtslage nicht. Zudem haben wir auf die rasanten technischen Entwicklungen zu reagieren. Hier sind die Anwendungen im Bereich Social Media, Netz- und Cloudtechnologien sowie die rasante Entwicklung der Verfahren mit KI besonders zu erwähnen.

Um die damit einhergehende Mehrbelastung stemmen zu können, hat die LDI NRW die dringend benötigte personelle Unterstützung erbeten und vom Landtag erhalten. Er bewilligte der LDI NRW mit dem Haushalt 2023 erfreulicher Weise 19 neue Stellen. Das ermöglichte uns, die personell und fachlich große Leitungspanne der Referate zu verkürzen und dadurch neue thematische Schwerpunkte zu setzen.

Die LDI hat mit den neuen Stellen eine Gruppenstruktur mit zwei Gruppenleitungen eingeführt und neue Schwerpunktreferate gebildet. Mein Vertreter ist mit der wachsenden Behörde im Bereich Personal, Organisation und IT-Ausstattung zunehmend gefordert. Die zweite Gruppenleitung betreut nun im Wesentlichen den Schwerpunkt Datenschutz in der Wirtschaft, der für sich genommen ein weites Feld ist. Damit entlastet sie meinen Vertreter thematisch in diesem Bereich.

Aber auch durch kleiner Referatszuschnitte, konnten wir neue Schwerpunkte setzen. So ist die Datenschutzkontrolle überwiegend im Bereich der JI-Richtlinie nun in einem eigenen Referat angesiedelt und nicht mehr mit den sonstigen zu überwachenden Verwaltungsbereichen vereint. Dies ist sachlich sinnvoll, da unterschiedliche Rechtsgrundlagen zur Anwendung kommen. Zudem haben wir dort zwei weitere Einheiten angesiedelt, die eine hohe Expertise in Bezug auf rechtsförmliche Verfahren erfordern. Eine ganz neue Einheit soll dort eine zentrale Funktion für das gesamte Haus wahrnehmen und Vorgaben für eine einheitliche und sichere Rechtsdurchsetzung erarbeiten. Außerdem baut sie ein Wissensmanagement aus den von uns geführten gerichtlichen Verfahren auf, das allen Referaten zur Verfügung stehen wird. Schließlich wurde unsere Bußgeldstelle in das neue Referat verlagert.

Der Datenschutz bei Online- und Mediendiensten ist nun ein Schwerpunktthema in einem weiteren neuen Referat. Es ist offensichtlich, dass der Medienbereich mit der technischen Entwicklung ein stetig wachsender Bereich ist, der ein eigenes Referat erfordert. Für eine gleichmäßige Aufgabenverteilung über alle Referate hinweg sind dort außerdem der Internationale Datenverkehr und Selbstregulierungsmechanismen angesiedelt. Auch diese beiden Themen gewinnen an Bedeutung. Schließlich wurde das Wirtschaftsreferat auf zwei Referate aufgeteilt, weil die Themenspanne zu breit geworden ist. Außerdem haben wir kleinere Aufgaben verlagert, um Reibungsverluste zu vermeiden. So wurde etwa der Beschäftigtendatenschutz bei öffentlichen und bei privaten Stellen in einem Referat zusammengeführt.

Mit diesen Schritten haben wir wichtige Aufgaben personell und fachlich stärken können. Die Neuorganisation werden wir mit einem zweiten Schritt fortführen, der mit der zum Ende des Jahres anstehenden Einführung der eAkte in der Behörde umgesetzt werden soll. Einfache Aufgaben sollen dann durch eine eigenständige Einheit schnell, unbürokratisch und bürger*innenfreundlich erledigt werden. Damit erhalten die Fachreferate weitere Freiräume für die fachlich anspruchsvollen Prüfungen.

Fazit

Wenn sich die Rahmenbedingungen im Datenschutz und in der Informationsfreiheit ändern, muss sich die Aufsichtsbehörde anpassen. Dies geschieht einerseits durch personelle Aufstockung, anderseits durch das Setzen von Arbeitsschwerpunkten. Das neue Organigramm der Behörde ist unter www.ldi.nrw.de/organisation abrufbar.

5. Die Europäische Datenstrategie schreitet voran

Die Europäische Datenstrategie wurde bereits im letzten Bericht vorgestellt. Mit ihr will die Europäische Union Innovation und Datennutzung voranbringen und zugleich ein hohes Schutzniveau für die Grundrechte der Europäer*innen gewährleisten. Inzwischen sind weitere Rechtsakte in Kraft getreten. Teils sind nun die nationalen Zuständigkeiten für die Aufgaben festzulegen, die aufgrund der neuen europäischen Gesetze durch nationale Behörden wahrzunehmen sind.

Innovationspotenziale sollen gemäß der Europäischen Datenstrategie durch eine Regulierung von Datenzugangsrechten, Datenverträgen und Interoperabilitätsregelungen gehoben werden. In sog. Datenräumen soll der Umfang der Datennutzung auch für öffentliche Zwecke festgelegt werden. Das neue europäische Datenrecht lässt die DS-GVO regelmäßig unberührt, löst aber Abstimmungsbedarf und neue Diskussionen über die Tragweite des Datenschutzrechts aus. Teils haben sich die Behörden, die die neuen Rechtsakte verwalten, deswegen mit den zuständigen Datenschutzaufsichtsbehörden abzustimmen.

Bereits im letzten Bericht sind der Data Governance Act (DGA), der Data Services Act (DSA), der Data Market Act und der Data Act beschrieben worden, die allesamt bereits im Jahr 2022 in Kraft traten.

Der DGA gilt nach Ablauf einer Nachfrist von 15 Monaten seit September 2023. Die darin vorgesehenen Mittel, um eine Datennutzung zu erleichtern – nämlich Datentreuhänder, Datenmittler und Datenspenden – haben bisher noch keinen spürbaren Eingang in die Datenverarbeitungspraxis gefunden. Von der EU-Kommission allerdings mit Nachdruck vorangebracht werden die nach dem Gesetz vorgesehenen Datenräume:

- **Europäischer Gesundheitsdatenraum – European Health Data Space (EHDS)**

Mit dem EHDS soll ein gemeinsamer europäischer Regelungsrahmen für die Nutzung und den Austausch von Gesundheitsdaten geschaffen werden. Gesundheitsdaten sollen in einem sicheren Format europaweit austauschbar werden. Dies soll Betroffenen ebenso wie behandelnden Ärzt*innen einen leichteren Zugriff auf die Daten ermöglichen. Zugleich soll aber auch eine leichtere sekundäre Nutzung der Daten für Forschung und als Grundlage für Verwaltungsentscheidungen ermöglicht werden.

Für die betroffenen Bürger*innen ist wichtig zu wissen, dass die Einwilligung als Basis für die Nutzung der eigenen Gesundheitsdaten durch Dritte nach den Plänen der EU-Kommission als Standard voraussichtlich abgelöst werden wird. Insbesondere die Nutzung von Gesundheitsdaten für Forschung und für Verwaltungsaufgaben soll durch das Regelwerk sehr stark gefördert und grundsätzlich nicht von einer vorherigen Einwilligung von Betroffenen abhängig gemacht werden. In Teilen soll es aber Möglichkeiten von Betroffenen geben, der Nutzung der eigenen Gesundheitsdaten zu widersprechen. Siehe hierzu auch den Beitrag 11. a – Datenschutz und Digitalisierung im Gesundheitsbereich.

- **Mobilitätsdatenraum – Mobility Data Space (EMDS)**

Ihre Vorstellungen zum EMDS hat die EU-Kommission in einer Stellungnahme vom 29. November 2023 veröffentlicht. Darin geht sie davon aus, dass datengetriebene Innovationen zu einer besseren Nutzung der Verkehrssysteme führen und einer wesentlich effizienteren Mobilität und der Weiterentwicklung eines vernetzten, klimaneutralen und wettbewerbsfähigen Verkehrssektors in der EU dienen können. Die EU-Kommission beobachtet bisher eine Fragmentierung der Informationen aus dem Verkehrssektor, die es zu beseitigen gelte, damit die EU die Vorteile der Digitalisierung für die Entwicklung im Mobilitäts- und Verkehrssektor erfolgreich nutzen kann. Im Interesse des Schutzes der Grundrechte und insbesondere des Rechts auf Datenschutz wird bei diesem Projekt darauf zu achten sein, dass Daten in einer Weise verarbeitet werden, die keinen Personenbezug haben, damit keine Bewegungsprofile von Personen in diesem Datenraum entstehen.

Auch die anderen im Jahr 2022 in Kraft getretenen Rechtsakte kommen nun schrittweise in Geltung und erfordern teils nationale Umsetzungsgesetze. Im Zusammenhang mit dem DSA ist die Festlegung der nationalen Überwachungszuständigkeit im Hinblick auf die Nutzung bestimmter personenbezogener Daten bemerkenswert, die dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zugewiesen wurde. Die Überwachung für die Rechtmäßigkeit der Nutzung derselben personenbezogenen

Daten ist nämlich zwei Behörden zugewiesen. Neben dem BfDI, der die Bestimmun-gen des DSA überwacht, überwachen die Datenschutzaufsichtsbehörden hinsichtlich derselben Daten bei denselben digitalen Diensten die Einhaltung der Datenschutzvorschriften (weitere Einzelheiten siehe unter 7. a. – Digitale-Dienste-Gesetz zur Plattformregulierung: Länder folgen der Kritik der Datenschutzaufsichtsbehörden, Bundesgesetzgeber nicht).

Dieser aus hiesiger Sicht missglückte Umsetzungsschritt weist auf ein Problem, das sich in der nationalen Umsetzung anderer Rechtsakte der Europäischen Datenstrategie wiederholen kann. Die meisten Rechtsakte der Strategie enthalten neue Aufgaben für nationale Behörden, die die Regulierung der Nutzung von Daten zum Gegenstand haben. Bisher gibt es bei personenbezogenen Daten im Wesentlichen eine einheitliche Überwachung der Rechtmäßigkeit ihrer Verarbeitung durch die Datenschutzaufsicht. Dabei sind von jeher eine Reihe von Fachgesetzen relevant, die die Nutzung von Daten erlauben oder determinieren. Diese Regelungen sind bisher integraler Bestandteil der Prüfungen der Datenschutzaufsichtsbehörden.

Nunmehr scheint im Bund ein Trend zu bestehen, die Überwachung der Nutzung von personenbezogenen Daten nach einzelnen Gesetzen aus der Europäischen Datenstrategie generell Bundesbehörden zuzuweisen. In der Diskussion ist etwa, die Bundesnetzagentur zu einer Digitalagentur auszubauen. Dies dürfte bei personenbezogenen Daten zu einer Fragmentierung in der Aufsicht über die Nutzung von Daten führen. Daraus resultiert dann wiederum ein erheblicher Abstimmungsaufwand zwischen der neuen Datenaufsichtsbehörde des Bundes und den jeweils zuständigen Datenschutzaufsichten über Sachverhalte, die sowohl gemäß der DS-GVO als auch gemäß einzelner Rechtsakte aus der Europäischen Datenstrategie zu bewerten sind. Unabhängig davon ist zweifelhaft, ob eine zentrale Überwachung der Allgegenwärtigkeit und Vielfalt von Datenverarbeitung überhaupt gerecht werden kann. Zentrale Verwaltungszuständigkeiten führen in einem föderalen Staat häufig nicht zu sachgerechten Lösungen und sind nicht nah an den Bürger*innen, um deren Daten es in diesem Fall geht. Die Datenschutzaufsichtsbehörden der Länder haben zu diesen sich abzeichnenden Problemen von Doppelstrukturen und Bürokratiezuwachs bei der nationalen Umsetzung der Datenstrategie ein Positionspapier verabschiedet. Die LDI NRW hat dieses Positionspapier der Landesregierung für ihre Beratungen zur Verfügung gestellt (Abdruck im Anhang).

Weder der bereits erwähnte EHDS, noch die viel diskutierte Verordnung zur Regulierung Künstlicher Intelligenz sind im Berichtszeitraum in Kraft getreten. Es wird aber für beide Regelwerke mit einer Verabschiedung noch vor der Europawahl im Juni 2024 gerechnet. Gleiches gilt für eine Verordnung zur Interoperabilität des öffentlichen Sektors, deren Verabschiedung noch im ersten Halbjahr 2024 erwartet wird. Sie befasst sich mit der Erleichterung

des Datenaustauschs öffentlicher Stellen in der Europäischen Union untereinander und dem leichteren Zugang zu Informationen öffentlicher Stelle.

Der vorliegende Bericht spiegelt wider, dass auch ohne eine Verordnung zur Regulierung von KI die LDI NRW jetzt schon die Verarbeitung personenbezogener Daten mittels KI-Verfahren betrachten muss. Im Bereich der Auswertung von Videobildern mittels KI haben wir sowohl Forschungsprojekte (siehe hierzu unter 8. – Beratung zu Verfahren mit Künstlicher Intelligenz), als auch einen digitalen Supermarkt bewertet (siehe hierzu unter 14. e. – Bezahlen Kund*innen im kassenlosen Supermarkt mit ihren Daten). Für die Schulen gibt es immer mehr Programme am Markt, die den Lernfortschritt mit KI auswerten und diesem Fortschritt entsprechend dann weitere mehr oder weniger anspruchsvolle Übungen individuell für die jeweiligen Lernenden anbieten. Auch hierzu haben wir eine Einschätzung abgegeben (siehe hierzu unter 9. a. – Einsatz von intelligenten tutoriellen Systemen in Schulen). Schon heute zeichnet sich damit ab, dass es zwischen der Anwendung der DS-GVO und der erwarteten KI-Verordnung zu Aufgabenüberschneidungen kommen wird, die hoffentlich besser gelöst werden, als bei der Umsetzung des DSA.

6. Konkretisierung des Auskunftsrechts – EuGH-Rechtsprechung und EDSA-Leitlinien

Nach der DS-GVO können betroffene Personen von Verantwortlichen eine Auskunft über die Verarbeitung ihrer Daten verlangen. Das Auskunftsrecht ist besonders wichtig, denn nur wer weiß, welche Daten unter welchen Umständen verarbeitet werden, kann weitere Rechte geltend machen, etwa Berichtigung, Löschung oder Schadenersatz verlangen. Dementsprechend versteht auch der EuGH das Auskunftsrecht als starkes und weitreichendes Recht und hat es in verschiedenen Entscheidungen bekräftigt. Flankiert werden die Urteile durch eine umfassende Hilfestellung des EDSA zur Anwendung des Auskunftsrechts.

Die vier Entscheidungen des EuGH

1. Die Auskunft umfasst auch die Identität von Empfänger*innen – Urteil vom 12. Januar 2023, Az. C-154/21

Verantwortliche müssen betroffenen Personen grundsätzlich die Identität der Empfänger*innen mitteilen, gegenüber denen sie deren Daten offengelegt haben. Kategorien von Empfänger*innen genügen in der Regel nicht.
Der EuGH betont, wie wichtig Transparenz über Datenverarbeitungen ist: Betroffene Personen müssen prüfen können, ob Daten zulässig verarbeitet werden. Die Nennung von Kategorien von Empfänger*innen genügt ausnahmsweise nur dann, wenn es nicht möglich ist, sie zu identifizieren oder wenn der Auskunftsantrag ansonsten nachgewiesen offenkundig unbegründet oder exzessiv ist.

Der Wortlaut der DS-GVO lässt zwar eine Auskunft sowohl über die Empfänger*innen als auch nur über Kategorien von Empfänger*innen zu (Art. 15 Abs. 1 Buchstabe c DS-GVO). Der EuGH hat nun aber klargestellt, dass darüber entscheidet, wer die Auskunft verlangt, und nicht, wer die Auskunft erteilen muss.

2. Die Auskunft betrifft auch Protokolldaten - Urteil vom 22. Juni 2023, Az. C-579/21

Zur Auskunft gehört auch die Information aus Protokolldaten, wann und warum auf die Daten zugegriffen wurde. Die DS-GVO schreibt vor, dass Prozesse der Datenverarbeitung nachvollziehbar sein müssen. Um die Nachvollziehbarkeit sicherzustellen, werden in manchen Fällen sogenannte Protokolldateien geführt. Diese Protokolldateien dokumentieren, wer wann auf welche Daten zugegriffen oder sie bearbeitet hat. Das passiert bei Behörden und der Polizei ebenso wie in Unternehmen der privaten Wirtschaft.

Nach dem EuGH ist es im Regelfall ausreichend, der betroffenen Person die protokollierten Datenabfragen mitzuteilen, ohne die Namen der Beschäftigten zu nennen. Die Identität der Beschäftigten, die auf Weisung des Verantwortlichen handeln, muss nach dem EuGH nur preisgegeben werden, wenn dies – etwa bei Zweifeln am tatsächlichen Zweck der Abfrage – im Einzelfall erforderlich ist, um zum Beispiel die Rechtmäßigkeit der Verarbeitung der Daten überprüfen zu können. Dabei müssen die Rechte und Freiheiten des Beschäftigten berücksichtigt werden.

3. Der Auskunftsanspruch muss nicht begründet werden und die erste Kopie ist auch bei Patient*innenakten kostenlos – Urteil vom 26. Oktober 2023, Az. C-307/22

Patient*innen haben auch ohne Angabe von Gründen einen datenschutzrechtlichen Anspruch auf eine erste unentgeltliche Kopie ihrer Patient*innenakte. Das gilt auch dann, wenn aus ihr Daten vor Gericht gegen Ärzt*innen verwendet werden könnten.

Das war umstritten, weil es im deutschen Bürgerlichen Gesetzbuch eine Regelung zur Kostenerstattung gibt. Mit dem Urteil steht fest, dass allenfalls bei einem erneuten Antrag für die Patient*innen Kosten entstehen könnten.

Das Auskunftsrecht umfasst grundsätzlich den Anspruch der Patient*innen, eine vollständige Kopie der Dokumente zu erhalten, die sich in der Akte befinden. Denn diese vollständige Kopie ist nach den zutreffenden Feststellungen des EuGH erforderlich, „[...] um der betroffenen Person die Überprüfung der Richtigkeit und Vollständigkeit der Daten zu ermöglichen und die Verständlichkeit der Daten zu gewährleisten“. Der EuGH wies weiter darauf hin, dass anderenfalls die Gefahr bestünde, dass bestimmte relevante Daten ausgelassen oder unrichtig wiedergegeben werden oder dass jedenfalls die Überprüfung ihrer Richtigkeit und Vollständigkeit sowie ihr Verständnis durch die Patienten*innen erschwert werden. Eingeschlossen sind etwa Informationen wie Diagnosen, Untersuchungsergebnisse, Befunde und Angaben zu Behandlungen oder Eingriffen.

4. Das Recht auf Kopie ist das Recht auf die Reproduktion der Daten – Urteil vom 4. März 2023, Az. C-487/21

Der Verantwortliche muss bei einer Auskunft eine Kopie der personenbezogenen Daten zur Verfügung stellen (Art. 15 Abs. 3 DS-GVO). Was das bedeutet, hat der EuGH klargestellt: Es geht um eine „originalgetreue und verständliche Reproduktion" der Daten. Kopien von Auszügen aus Dokumenten oder von ganzen Dokumenten oder von Auszügen aus Datenbanken, die diese Daten enthalten, sind erforderlich, wenn sie unerlässlich sind, um der betroffenen Person die wirksame Ausübung ihrer Datenschutzrechte zu ermöglichen. Der Verantwortliche muss dabei die Rechte und Freiheiten anderer berücksichtigen. Daten, die in einem gängigen elektronischen Format zur Verfügung zu stellen sind (Art. 15 Abs. 3 Satz 3 DS-GVO) sind nur die Daten, von denen der Verantwortliche eine Kopie zur Verfügung stellen muss.

EDSA-Leitlinien zum Auskunftsrecht

In seinen Leitlinien zum Auskunftsrecht nach Art. 15 DS-GVO gibt der EDSA eine umfassende Hilfestellung für die Anwendung des Auskunftsrechts. Damit soll eine möglichst einheitliche Verwirklichung dieses Rechts in allen Ländern erreicht werden, in denen die DS-GVO gilt. Nach einer Konsultation wurde die Endfassung der Leitlinien erstellt und veröffentlicht. Die LDI NRW hatte im Rahmen der europäischen Gremienarbeit an den Leitlinien intensiv mitgewirkt.

Die Leitlinien bieten zunächst einen Überblick über die etwas komplizierte Struktur der Regelung und stellen die wesentlichen Prinzipien vor, die beim Auskunftsrecht zu beachten sind. Anschließend werden die Fragen ausführlich behandelt, die sich dem für die Datenverarbeitung Verantwortlichen stellen, der eine Auskunftsbitte erhalten hat:

Wann ist von einem Auskunftsantrag im Sinne der DS-GVO auszugehen, wie wird er interpretiert und wem darf Auskunft erteilt werden?

- Auf welche der verarbeiteten Daten bezieht sich der Antrag und welche Informationen über die Verarbeitung müssen darüber hinaus bereitgestellt werden?
- Welche Maßnahmen müssen zum Auffinden der Daten ergriffen werden, auf welche Art und Weise müssen die Informationen erteilt werden?
- Was ist unter einer „Kopie der Daten" oder unter einem „gängigen elektronischen Format" zu verstehen?
- Welche Beschränkungen des Auskunftsanspruchs sind zu beachten und unter welchen Bedingungen muss von einer Auskunft ganz oder teilweise abgesehen werden?

Die Leitlinien enthalten zudem ein Flussdiagramm, das die einzelnen Schritte bei der Bearbeitung eines Auskunftsantrags verdeutlicht. Weitere Leitlinien zu Betroffenenrechten, die die DS-GVO gewährleistet (z. B. Widerspruch oder Löschung), sind mittelfristig in Planung.

Für das Auskunftsrecht als grundlegendes Betroffenenrecht liegen mit den Leitlinien nun eingehende, europaweit einheitliche Erläuterungen von Inhalt und praktischer Handhabung durch die Verantwortlichen vor. Die Leitlinien 01/2022 sind in der aktualisierten Fassung seit dem 17. April 2023 unter www.edpb.europa.eu abrufbar.

7. Internet und Medien

7.1. Digitale-Dienste-Gesetz zur Plattformregulierung: Länder folgen der Kritik der Datenschutzaufsichtsbehörden, Bundesgesetzgeber nicht

Die LDI NRW hat den Entwurf für ein Digitale-Dienste-Gesetz vom August 2023 kritisiert. Die Landesregierung hat die Kritik mitgetragen und in die eigene Stellungnahme übernommen.

Obwohl die Landesregierung nicht verpflichtet ist, die LDI NRW an Gesetzesvorhaben des Bundes förmlich zu beteiligen, hat sich die Zusammenarbeit bewährt. Dabei konnten nämlich Friktionen des Gesetzesvorhabens mit der Datenschutzaufsicht in den Ländern deutlich gemacht werden.

Mit dem Digitale-Dienste-Gesetz (DDG) soll die Plattformaufsicht nach dem europäischen Gesetz über digitale Dienste (Digital Services Act, DSA) im deutschen Recht geregelt werden. Das Gesetzesvorhaben soll Teile der Digitalen-Dienste-Aufsicht beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) und damit auf Bundesebene verankern. Ziel sollte ausweislich der Begründung des Gesetzgebers sein, dass zusätzliche Koordinierungs- und Abstimmungsprozesse vermieden und einheitliche Entscheidungen durch den BfDI sichergestellt werden sollen.

Tatsächlich würde die von der LDI NRW kritisierte Regelung in § 12 Abs. 3 des Entwurfs aber nicht zu einer Vereinheitlichung der Datenschutzaufsicht führen. Stattdessen käme es zu einer Spaltung von Kontrollzuständigkeiten bei einem einheitlichen Lebenssachverhalt. So soll der BfDI die Betreiber von Online-Plattformen überwachen, wenn sie Werbung anzeigen, die unter Verwendung besonders sensibler Daten oder personenbezogener Daten von Minderjährigen ausgespielt wird. Die datenschutzrechtliche Überwachung für solche Profiling-Tatbestände nach der DS-GVO liegt allerdings weiterhin in

der Zuständigkeit der Landesdatenschutzbehörden. Durch solche doppelten Zuständigkeiten entstehen Reibungsverluste, Rechtsunsicherheit und kaum eine effektive Kontrolle. Es wird letztlich das Gegenteil des in der Gesetzesbegründung genannten Ziels erreicht.

Weiter ist der Gesetzentwurf in Bezug auf die Zusammenarbeit der Koordinierungsstelle bei der Bundesnetzagentur (BNetzA) mit den zuständigen Datenschutzbehörde zu vage. Weder sind konkrete Verfahren für die Zusammenarbeit implementiert, noch die Berührungspunkte der Aufsicht über digitale Dienste einerseits mit der Datenschutzaufsicht andererseits hinreichend geklärt. Dabei hätte hier eine sorgfältigere Ausarbeitung der Zusammenarbeit sehr viel Sinn ergeben und ein Muster für weitere Verfahren sein können. Im Zuge der Europäischen Datenstrategie werden noch eine ganze Reihe von Rechtsakten der EU in innerstaatliches Recht implementiert werden müssen, die ebenso eine Zusammenarbeitspflicht zwischen der Datenschutzaufsicht und den nationalen Kontrollbehörden für die neuen Rechtsakte erfordern. Hier kann man nun nur hoffen, dass für die Umsetzung dieser Rechtsakte bessere Lösungen für die Zusammenarbeit mit den Datenschutzaufsichtsbehörden national vorgesehen werden. Das Positionspapier der Datenschutzaufsichtsbehörden der Länder zur nationalen Umsetzung der Europäischen Datenstrategie ist im Anhang abgedruckt. Neben der LDI NRW haben sich auch andere Landesdatenschutzbehörden ähnlich kritisch geäußert. Die Landesregierung hat unsere Kritik in die eigene Stellungnahme übernommen.

In dem neuen Regierungsentwurf des Digitale-Dienste-Gesetzes vom Dezember 2023 wurde die Kritik leider nicht berücksichtigt, so dass es gemäß § 12 Abs. 3 DDG bei der Zuständigkeit des BfDI für die Durchsetzung der Art. 26 Abs. 3 und Art. 28 Abs. 2 und 3 DSA geblieben ist. Hinzu kommt, dass die Rolle der Landesdatenschutzbehörden bei der Einbeziehung in Entscheidungen der Koordinierungsstelle der BNetzA nach § 19 DDG im Regierungsentwurf geschwächt wurde. Musste die Koordinierungsstelle der BNetzA nach dem alten Entwurf des DDG vor einer Entscheidung in Datenschutzbelangen noch ein Einvernehmen mit der Datenschutzbehörde erzielen, ist dies nach dem neuen Regierungsentwurf nicht mehr der Fall. Sie muss sich mit der Datenschutzbehörde lediglich ins Benehmen setzen. Das ist weniger als ein Einvernehmen. Ist eine einvernehmliche Lösung nicht erreichbar, kann sich die Behörde, die sich um das Benehmen bemühen soll, letztlich über die Auffassung der anderen Behörde teilweise oder in Gänze hinwegsetzen. Dies ist insoweit bemerkenswert, als die Bundesnetzagentur über keine eigene Datenschutzkompetenz verfügt.

Fazit

Bei der Umsetzung der weiteren Rechtsakte der Europäischen-Datenstrategie werden wir die Landesministerien weiterhin unterstützen und auf eine gute Zusammenarbeit setzen. Zu hoffen bleibt, dass die Bundesregierung dann mehr Verständnis für einen schlüssigen Verwaltungsaufbau und praktikable Verwaltungsverfahren im föderalen Staat zeigt.

7.2. Anleitung für den Einsatz von MS 365

Die Verwendung von Microsoft 365 (MS 365) bereitet weiterhin datenschutzrechtliche Probleme. Die LDI NRW hat zusammen mit weiteren Datenschutzbehörden eine Handreichung für Verantwortliche für den Einsatz von MS 365 erstellt.

Die DSK hat bereits im November 2022 festgestellt, dass die Standard-Auftragsverarbeitungsvereinbarung von Microsoft (Data Protection Addendum – DPA), die für den Einsatz von MS 365 vorgesehen ist, nicht den Anforderungen der DS-GVO (Art. 28 Abs. 3) entspricht.

Die Handreichung soll Verantwortliche dabei unterstützen, gegenüber Microsoft auf die nötigen vertraglichen Änderungen hinzuwirken. Die wesentlichen Empfehlungen sind im Teil 1 und im Anhang der Handreichung jeweils als hervorgehobene To-dos kompakt dargestellt. Sie helfen zum Beispiel Verantwortlichen für die digitale Ausstattung von Schulen, die notwendigen Anpassungen gegenüber Microsoft einzufordern, damit eine Nutzung der Daten von Schüler*innen und Lehrer*innen für eigene Zwecke von Microsoft unterbleibt. Das Schulrecht schließt eine solche Übermittlung der Daten von Lehrer*innen und Schüler*innen für Unternehmenszwecke grundsätzlich aus (vgl. § 120 Abs. 7 Satz 3 Schulgesetz NRW).

Die Handreichung erläutert die datenschutzrechtlichen Schwierigkeiten, die sich aus den von Microsoft zugrunde gelegten Verträgen ergeben. Gleichzeitig werden Lösungsansätze aufgezeigt, die mit einer Zusatzvereinbarung umgesetzt werden können. Die Handreichung orientiert sich an den Fragestellungen, die im Bericht der DSK aufgeworfen sind. Die Themen Drittlandübermittlungen und extraterritoriale Zugriffe wurden aufgrund laufender Entwicklungen ausgeklammert. Ein zentraler Punkt dabei ist unter anderem, dass insbesondere öffentliche Stellen ausschließen müssen, dass Microsoft die Daten auch zu eigenen Zwecken nutzt, die im Auftrag für diese Stellen verarbeitet werden. Die LDI NRW hat die Landesregierung und die Kommunalen Spitzenverbände in NRW über die Handreichung informiert.

Aber auch nicht-öffentliche Stellen können als Verantwortliche diese Dienste nur dann einsetzen, wenn Microsoft die Transparenz der Datenverarbeitung verbessert und sie auf dieser Basis prüfen können, ob die zentralen datenschutzrechtlichen Anforderungen eingehalten werden.

Insbesondere Schulen empfehlen wir einstweilen, datenschutzfreundlichere Alternativen zu nutzen. Die Vermittlung des Umgangs mit einzelnen Microsoft-Diensten bzw. Programmen und ihren Funktionen (wie PowerPoint oder Excel) ist unterdessen auch nicht ausgeschlossen. Voraussetzung ist jedoch, dass es sich hierbei um lokale Installationen auf schulischen Geräten oder schulische, nicht personalisierte Accounts handelt, die für Microsoft und Dritte keinen Rückschluss auf einzelne Schüler*innen erlauben.

Fazit

Verantwortliche können selbst auf Basis dieser Handreichung MS 365 nur dann datenschutzkonform einsetzen, wenn Microsoft sich kooperativ zeigt. Neben den aufgezeigten vertraglichen Änderungen, die für einen datenschutzkonformen Einsatz der Dienste erforderlich sind, muss Microsoft technische Änderungen an der Datenverarbeitung vornehmen. Hier bleibt zunächst abzuwarten, ob Microsoft bereit sein wird, an einer entsprechenden Lösung mitzuwirken.

7.3. Per Verordnung gegen die Einwilligungsmüdigkeit bei Cookie-Bannern?

Das Bundesministerium für Digitales und Verkehr hat im Juni 2023 eine Einwilligungsverwaltungsverordnung im Entwurf (EinwV-E) veröffentlicht. Die Verordnung regelt die Voraussetzungen für Dienste zur Verwaltung von Einwilligungen, die beim Aufrufen von Websites abgefragt werden. Die LDI NRW brachte auf Anfrage der Landesregierung ihre Kritikpunkte im Rahmen des Gesetzgebungsverfahrens an.

Hintergrund für die Verordnung ist das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG). Danach kann die Bundesregierung per Verordnung regeln, dass Dienste zur Einwilligungsverwaltung eingeführt werden können, die es Websites erlauben, ohne Einwilligungsbanner zur Cookie-Verwendung auszukommen.

Die Verordnung bezweckt, dass sich Internet-Nutzer*innen nicht mehr bei jedem Aufruf einer Website erneut mit einem Einwilligungsbanner auseinandersetzen müssen. Diese Einwilligungsverwaltung soll der Gefahr der „Einwilligungsmüdigkeit“ entgegenwirken.

Aus Sicht der LDI NRW sind die im Entwurf und im TTDSG (§ 26 Abs. 2) normierten Ziele nicht erreichbar. Denn das Einwilligungsbanner auf Websites dient nicht allein dem Zweck, von Nutzer*innen Einwilligungen gemäß § 25 Abs. 1 TTDSG einzuholen. Das Banner ist in den meisten Fällen auch noch erforderlich, um Einwilligungen für die weiteren Datenverarbeitungen nach der DS-GVO abzufragen (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a und Art. 49 Abs. 1 Buchstabe a DS-GVO). Dazu kann eine Verordnung nach TTDSG aber keine Regelung treffen, weil die Kompetenz dazu nicht beim nationalen Gesetzgeber liegt.

Darüber hinaus hat die LDI NRW kritisiert, dass die Verordnung das Erfordernis der Datensparsamkeit von Einwilligungsverwaltungsdiensten nicht

hinreichend berücksichtigt. Solche Dienste müssen besonders datensparsam ausgestaltet sein, weil ansonsten die Möglichkeit besteht, dass die Dienste selbst zur Nachverfolgung von Nutzer*innenverhalten im Internet genutzt werden (Fingerprinting). Diese Gefahr besteht beispielsweise, wenn ein entsprechender Dienst sämtliche Besuche von Websites mit Einwilligungsoptionen und die getroffenen Einwilligungsentscheidungen protokolliert. In der Verordnung fehlt es an näheren Informationen dazu, wie die Einwilligungsverwaltungsdienste technisch funktionieren und welche organisatorischen Maßnahmen vorgesehen werden sollen. Ebenso fehlt es an einer Regelung erforderlicher Schutzmaßnahmen, um sicherzustellen, dass von den geplanten Diensten keine zusätzlichen Gefahren für die Privatsphäre ihrer Nutzer*innen ausgehen.

Ähnlich wie die LDI NRW hat sich auch die DSK kritisch zur Verordnung geäußert. Bislang liegt der LDI NRW kein neuer Entwurf einer Einwilligungsverwaltungsverordnung vor.

Aus Sicht der LDI NRW war hier erfreulich, dass die Landesregierung im Rahmen ihrer Stellungnahme aktiv auf die LDI NRW zugekommen ist. Es besteht jedenfalls keine Pflicht der Landesregierung, die LDI NRW bei bundesrechtlichen Gesetzgebungsverfahren mit Datenschutzbezug zu beteiligen. Dort wo zentrale Fragen des Datenschutzes betroffen sind, ist es dennoch sinnvoll, die Vollzugsexpertise der LDI NRW in Datenschutzfragen einzubeziehen.

Üblicherweise vollzieht die Landesregierung Bundesgesetze mit eigenen nachgeordneten Verwaltungsbehörden. Aufgrund der unabhängigen Stellung der LDI NRW ist das im Datenschutzrecht anders. In einigen anderen Ländern ist deswegen eine Beteiligung der Datenschutzaufsichtsbehörde im Landesrecht bei Stellungnahmen zu Bundesgesetzen mit Datenschutzrelevanz verankert.

Dass die Landesregierung den Rat der LDI NRW ohne rechtliche Verpflichtung eingeholt und genutzt hat, ist vor diesem Hintergrund bemerkenswert. Gern stehen wir auch bei anderen bundesrechtlichen Gesetzgebungsverfahren, die den Datenschutz berühren, Rat gebend zur Verfügung.

Fazit

Selbst wenn eine neue Einwilligungsverwaltungsverordnung einige der genannten Kritikpunkte berücksichtigen sollte, bliebe es dabei, dass der nationale Gesetzgeber nichts zu Einwilligungen regeln darf, die über das TTDSG hinaus gehen. Dienste zur Einwilligungsverwaltung werden daher Einwilligungsbanner auf Websites vorerst nicht überflüssig machen können. Die Zusammenarbeit mit der Landesregierung hat sich hier bewährt – und kann ein Vorbild für weitere Verfahren sein.

7.4. “Pur-Abos“ im Internet können zulässig sein, müssen aber bestimmte Bedingungen einhalten

Pur-Abo-Modelle auf Websites werden immer häufiger. Dabei haben die Nutzer*innen die Wahl, ob sie einen zahlungspflichtigen Abo-Vertrag abschließen oder ihre Zustimmung zum Tracking erteilen möchten. Zulässig ist das nur, wenn die Voraussetzungen einer datenschutzrechtlichen Einwilligung vorliegen.

Bei Pur-Abo-Modellen haben Internet-Nutzer*innen üblicherweise zwei Wahlmöglichkeiten: Entweder schließen sie ein Pur-Abo ab, oder sie willigen ein, dass ihre Daten über Targeting beziehungsweise Tracking zum Zweck der profilbasierten, personalisierten und zielgerichteten Werbung genutzt werden dürfen.

Aus Sicht der LDI NRW kann die Nachverfolgung von Nutzer*innenverhalten (Tracking) grundsätzlich auf eine Einwilligung gestützt werden, wenn alternativ ein trackingfreies Modell angeboten wird – selbst wenn dieses bezahlpflichtig ist. Dabei müssen aber bestimmte Bedingungen eingehalten werden. Diese Auffassung teilt auch die DSK in ihrem Beschluss „Bewertung von Pur-Abo-Modellen auf Websites“ vom 22. März 2023 (Abdruck im Anhang).

Besteht die Möglichkeit des zahlungspflichtigen Pur-Abos, um trackingfrei die Website zu besuchen, dann reicht das Pur-Abo als Alternative zum herkömmlichen Ablehnen-Button grundsätzlich aus, der das Ablehnen des Trackings ermöglicht. Wenn mehrere Verarbeitungszwecke vorliegen, müssen Einwilligungen für jeden einzelnen Zweck oder zumindest für zusammengefasste ähnliche Zwecke erteilt werden können (granulare Einwilligungen).

Weitere Bedingungen sind, dass das verlangte Entgelt marktüblich ist und ein gleichwertiger Zugang zu derselben Leistung eröffnet wird.

Da auch Website-Betreiber*innen aus NRW häufig das Pur-Abo-Modell verwenden, hat die LDI NRW die Websites einiger größerer Unternehmen geprüft. Vier Anbieter haben daraufhin ihre Pur-Abo-Modelle umgestellt und ermöglichen den Nutzer*innen nun eine granulare Einwilligung. Damit ist bereits ein wichtiger Schritt zu mehr Nutzerfreundlichkeit erreicht.

Bedenken bestehen allerdings noch bei der Art und teils großen Anzahl der Tracking-Dienste, denen die Nutzer*innen zustimmen müssen, falls sie sich gegen das Pur-Abo und für die (granulare) Einwilligung entscheiden. Zudem bestehen Zweifel daran, ob die Tracking-Dienste, die von Website-Betreiber*innen in einem Bündel zusammengefasst werden, tatsächlich ähnlichen Zwecken dienen. Insoweit hat sich die LDI NRW Nachprüfungen vorbehalten.

Fazit

Zwar ist der Einsatz datenschutzkonformer Pur-Abo-Modelle durchaus möglich. Hierbei muss jedoch zum einen die alternative Einwilligung zu den einzelnen Zwecken oder Zweckbündeln ermöglicht werden. Zum anderen müssen gebündelte Zwecke einander ähnlich sein und dürfen nur eine überschaubare Anzahl an Zwecken enthalten.

8. Beratung zu Verfahren mit Künstlicher Intelligenz

An die LDI NRW wurden mehrere Beratungsanfragen von Unternehmen gerichtet, bei denen „Künstliche Intelligenz“ (KI) eingesetzt werden sollte. Die LDI NRW berät zu den Datenschutzanforderungen. Bisher ist das Datenschutzrecht das einzige Regelwerk, das zu einer gewissen Regulierung der Verfahren führt, sofern sie personenbezogene Daten zum Gegenstand haben. Eine spezifische KI-Regulierung auf europäischer Ebene wird erwartet, stand aber im Berichtszeitraum nicht zur Verfügung.

Die fortschreitende Digitalisierung durchdringt unseren Alltag zunehmend. In Wirtschaft, Staat und Gesellschaft bis hin in die Privatsphäre ist Digitaltechnik allgegenwärtig. Schlagworte sind Breitbandkommunikation, Internet der Dinge, E-Commerce, Smart Home oder Industrie 4.0. Dieser Trend wird durch die Verheißungen der KI verstärkt. Sie soll, vereinfacht gesagt, menschliche Lern- und Denkprozesse vom Computer durchführen lassen und dem Computer damit eine „Intelligenz“ verschaffen. Dazu kann sie unter anderem anhand von Beispieldaten darauf trainiert werden, ein definiertes Problem möglichst selbstständig zu lösen.

Digitalisierung und auch KI versprechen uns Verbesserungen und Erleichterung im privaten Alltag, ebenso wie bei unseren Aufgaben im Arbeitsleben. Diese Entwicklung geht aber zugleich damit einher, dass unser Handeln nachvollziehbar wird und wir zunehmend „gläsern“ werden. Hier bildet der Datenschutz ein notwendiges Korrektiv und soll gewährleisten, dass wir mit unseren Persönlichkeiten nicht in einem Dschungel von Daten untergehen. Diejenigen, die Daten verarbeiten, müssen dies auf eine Rechtsgrundlage stützen können. Jede Person muss wissen können, welche Daten über sie verarbeitet werden und Menschen dürfen grundsätzlich nicht allein anhand eines Datenprofils beurteilt werden.

Vor diesem Hintergrund betrachtet die LDI NRW bei der Bewertung von Vorhaben insbesondere,

- auf welche Rechtsgrundlage der Verantwortliche seine Datenverarbeitung stützen kann,
- welche Zwecke mit den Datenverarbeitungsprozessen zur Umsetzung des Vorhabens verfolgt werden und ob diese Prozesse für den verfolgten Zweck insgesamt erforderlich sind,
  - also ob der Grundsatz der Datenminimierung beachtet wurde,
  - ob das Vorhaben genauso gut mit anonymen Daten
  - oder zumindest mit pseudonymen Daten realisiert werden kann,
  - ob nicht mehr erforderliche Daten gelöscht werden,
- ob besonders schützenswerte, vor allem in Abhängigkeitsverhältnissen stehende, Personengruppen (zum Beispiel Kinder und Beschäftigte) von der Datenverarbeitung betroffen sind,
- wie die Sicherheit der Verarbeitung ausgestaltet ist,
- ob Datenübermittlungen in Länder außerhalb des Geltungsbereichs der DS-GVO erfolgen und ob dort dann ein angemessenes Datenschutzniveau wie in der Europäischen Union besteht,
- ob Betroffene angemessen über die Datenverarbeitungsvorgänge informiert werden und
- ob die datenschutzrechtlichen Verantwortlichkeiten bei mehreren an einem Datenschutzverarbeitungsprozess Beteiligten klar geregelt sind.

Ein Beratungsersuchen an uns betraf ein Forschungsprojekt an einem Flughafen. Es sollte ein Videoanalysesystem zur Erkennung von Personen getestet werden, das in einem späteren Realbetrieb dem Flughafenbetreiber zur Gewährleistung der Flughafensicherheit zur Verfügung stehen sollte. Insbesondere wurden die Prävention und Verfolgung von Straftaten, wie beispielsweise Gepäckdiebstahl, und die Terrorismusbekämpfung als mögliche zukünftige Einsatzzwecke genannt.

Auf Basis der im Flughafenbereich durch viele Kameras erstellten Videoaufnahmen sollten im Rahmen des Projekts automatisiert Personen erfasst werden. Anschließend sollten für die Personen sog. „Personenmerkmale“ generiert werden. Diese Merkmale sollten eine automatisierte Wiedererkennung ermöglichen. Neu entwickelte Algorithmen sollten anhand der erkannten Gesichter zum Beispiel das Geschlecht und das Alter bestimmen. Mit diesen Merkmalen sollte es möglich sein, eine bestimmte Person jederzeit auf den Live-Aufnahmen zu erkennen. Es war ebenfalls geplant, eine sog. „Watch-List“ mit generierten Merkmalen von bestimmten Personen anzulegen. Sofern die Merkmale einer erfassten Person mit Merkmalen aus der Watch-List übereinstimmten („Matching“), sollte ein Alarm erfolgen.

Das Verfahren zur Detektion, Klassifikation und Identifikation von Personen, Gesichtern, Kleidung und mitgeführten Objekten sollte dabei auf dem Einsatz eines Mustererkennungsverfahrens mittels „Deep Learning“ beruhen. Dem liegt die Annahme zugrunde, dass die Auswertungsleistung („Detektion“) umso besser sei, je mehr Daten generiert und analysiert werden. Der Test sollte zunächst mit Beschäftigten als freiwilligen Testpersonen durchgeführt werden. Anschließend sollten komplexere reale Testdurchläufe in zwei Bereichen eines Flughafenterminals oder im Sicherheitsbereich stattfinden. Später sollte dann die Funktionsfähigkeit und Belastbarkeit im operationellen Betrieb des Flughafens getestet werden.

Für das Forschungsprojekt wären Lösungen notwendig gewesen, die sicherstellen können, dass sich Personen der Erfassung ihrer Daten hätten entziehen können, wenn sie nicht in das Projekt einbezogen werden wollten. Dies wäre spätestens in der dritten Phase des operationellen Betriebs nicht mehr möglich gewesen.

Das Vorhaben vermittelte im Hinblick auf den später geplanten Realeinsatz außerdem den Eindruck, dass das gesamte Areal des Flughafens umfassend und dauerhaft mit allen verfügbaren Kameras mittels des Systems überwacht werden sollte. Zwar ist ein Flughafenbetreiber nach § 8 des Luftsicherheitsgesetzes verpflichtet, Maßnahmen zur Eigensicherung des Flughafens durchzuführen. Eine anlasslose und umfassende Überwachung aller Personen im Flughafengebäude wäre aber auch angesichts dieser Aufgabenstellung unverhältnismäßig. Der Flughafenbetreiber hat das Forschungsprojekt inzwischen beendet.

In einem weiteren Fall wollte ein Unternehmen aus dem Profisport die Zugangsberechtigung von akkreditierten Personen zum Innenraum seiner Sportstätte durch eine Gesichtserkennungssoftware sicherstellen und beschleunigen. Im Rahmen eines Pilotprojekts sollten zunächst biometrische Bilddaten von akkreditierten Beschäftigten des Unternehmens und später auch von Beschäftigten von Fremdfirmen in einer Datei hinterlegt werden, damit diese am Eingang durch eine Software mit den Gesichtern der Betroffenen abgeglichen werden. Für diesen Abgleich sollte ein KI-basiertes System genutzt werden. Das Unternehmen wollte dies für beide Personengruppen auf die Arbeitsverträge der eigenen Beschäftigten bzw. der Fremdbeschäftigten gemäß Art. 9 Abs. 2 Buchstabe b DS-GVO in Verbindung mit § 26 Abs. 3 Satz 1 BDSG stützen.

Wegen der besonderen Schutzbedürftigkeit biometrischer Daten ist deren Verarbeitung im Rahmen eines Beschäftigungsverhältnisses für die Zugangskontrolle nur zu Hochsicherheitsbereichen ausnahmsweise zulässig und verhältnismäßig. Der Innenraum der Sportstätte ist kein derart sensibler Bereich, der nur auf diese Weise gesichert werden kann. Außerdem gab es in

dem Stadium bisher ein solches unberechtigtes Eindringen offenbar noch gar nicht. Jedenfalls konnte man uns solche Vorfälle nicht belegen.

Die LDI NRW hat daher vorgeschlagen, sowohl von eigenen Beschäftigten – als auch später von Beschäftigten der Fremdfirmen – Einwilligungen für die Datenverarbeitungsvorgänge nach Art. 9 Abs. 2 Buchstabe a DS-GVO, § 26 Abs. 3 Satz 2 in Verbindung mit Abs. 2 BDSG einzuholen. Die sichere und zügige Eingangs- und Berechtigungskontrolle liegt vorrangig im Interesse des Unternehmens, gleichzeitig stellt dies aber auch für die Beschäftigten einen Vorteil dar. Daher kann ein eigenes Interesse der Beschäftigten an der Durchführung dieser vereinfachten Einlasskontrolle bestehen, das mit dem Interesse des Verantwortlichen weitgehend im Einklang steht. Einwilligungen sind allerdings nur dann eine tragfähige Datenverarbeitungsgrundlage, wenn sie freiwillig erteilt werden. Das setzt voraus, dass man sich, ohne Nachteile zu erleiden, auch gegen die Einwilligung entscheiden kann. Konkret muss also für diejenigen, die nicht einwilligen, nachteilsfrei ohne Hinterlegung eines biometrischen Passbildes und Gesichtsabgleich die Zugangsberechtigung für den Innenraum gewährleistet sein. Das Unternehmen hat das zugesagt.

In einem anderen Beratungsfall wollte ein ÖPNV-Unternehmen einer Großstadt die technische Infrastruktur zur Datenübertragung und zum Gefahrenmanagement an Bahnhaltestellen – Videotechnik und Notrufsprechstellen – erneuern. Die neue Videotechnik sollte zusätzlich auf KI basierende Videoanalysefunktionen enthalten, über die unter anderem Fahrgaststromanalysen zur frühzeitigen Erkennung und Optimierung der Personenströme erstellt werden können. Der großflächigen Umsetzung sollte eine bis Ende 2023 laufende Testphase im Rahmen eines wissenschaftlichen Projekts vorangehen. Hierfür sollten eine oberirdische Haltestelle und ein Bahnsteig einer unterirdischen Haltestelle mit „intelligenten“ Videokameras ausgestattet werden. Das Testfeld sollte aus 23 Kameras bestehen. Das Testprojekt sollte in gemeinsamer Verantwortlichkeit gemäß Art. 26 DS-GVO mit zwei weiteren Unternehmen und einem Forschungsinstitut durchgeführt werden.

Die Erwartung war, Erkenntnisse für die angewandte Forschung, unter anderem über die Eignung verschiedener Machine-Learning-Modelle in einer realen Umgebung, zu gewinnen. Zwecke der Verarbeitungsvorgänge sollten Klimaschutz, die Steigerung der Attraktivität des ÖPNV und die Erhöhung der Sicherheit sein. Das Erkennen bzw. die Zuordnung von Personen auf Bilddaten sei – so das Unternehmen – für die wissenschaftliche Analyse weder vorgesehen noch beabsichtigt. Nur wenn aufgrund des Verhaltens von Personen die gefahrenabwehrrechtlichen oder strafprozessualen Voraussetzungen vorlägen, könne eine Übermittlung konkreter Videodaten an Behörden erfolgen.

Die datenschutzrechtliche Prüfung der LDI NRW konzentrierte sich auf das Forschungsprojekt, das Erkenntnisse für eine mögliche flächendeckende Umsetzung im Stadtgebiet liefern sollte. Als problematisch erweist sich in diesem Zusammenhang die Tatsache, dass eine hybride Nutzung der Kamerasysteme für die Personenstromanalyse ebenso wie für Sicherheitszwecke erfolgen soll. Die Personenstromanalyse erfordert laut Auskunft der Forschenden einerseits keine Personenerkennung. Andererseits benötigt sie eine flächendeckende Abdeckung, die alle Personen erfasst, die sich an den Haltestellen befinden. Daher sollte es im Testaufbau keine Möglichkeit für Betroffene geben, sich außerhalb der Bereiche der „intelligenten" Videokameras zu bewegen. Ähnlich wie am Flughafen dürfte eine ausnahmslose Überwachung aller Fahrgäste, die die Personen erkennbar lässt, an den Stationen des ÖPNV nicht verhältnismäßig sein. Gegen das Forschungsvorhaben bestehen bei der Nutzung anonymer Daten grundsätzlich keine Bedenken. Würden die Bilder hinreichend unklar aufgezeichnet werden und dies auch technisch nicht reversibel sein, wäre das Forschungsziel auf diesem Wege mit anonymen Daten zu erreichen. Soll hingegen die Erkennbarkeit der Personen erhalten bleiben, weil die Aufzeichnungen zugleich für Sicherheitszwecke genutzt werden, ist die für die Forschung notwendige flächendeckende Haltestellenüberwachung problematisch, weil sie anlasslos in dieser umfassenden Form für Sicherheitszwecke nicht verhältnismäßig ist.

Aufgrund der Gesamtumstände ist das Vorhaben eine besonders riskante Datenverarbeitung, für die eine Datenschutzfolgenabschätzung gemäß Art. 35 DS-GVO durchzuführen ist. Gemäß Art. 89 Abs. 1 DS-GVO in Verbindung mit § 27 Abs. 1 Satz 2 BDSG muss der Verantwortliche zur Wahrung der Rechte und Interessen Betroffener eine Vielzahl von Maßnahmen vornehmen und beachten. Für diese Folgenabschätzung hat die LDI NRW weitere Hinweise gegeben. Eine abschließende Bewertung kann erst auf Basis der Datenschutzfolgenabschätzung getroffen werden.

Fazit

Die an die LDI NRW gerichteten Beratungsersuchen zu KI-Anwendungen mit personenbezogenen Daten sollten Erkenntnisse über das Verhalten von Personen erbringen und der Erkennung von Personen dienen. Solche Anwendungen müssen den Persönlichkeitsrechten aller davon Betroffenen Rechnung tragen und den Datenschutz einhalten. Das hat die DSK in ihrer „Hambacher Erklärung" vom 3. April 2019, abrufbar unter www.datenschutzkonferenz-online.de, betont. Zukünftig werden unsere Prüfungen voraussichtlich auch durch das weltweit erste Gesetz zur Regulierung von KI beeinflusst sein, das in der EU in Kraft treten wird.

9. Schule und Bildung

9.1. Einsatz von intelligenten tutoriellen Systemen in Schulen

Das Lernen wird zunehmend digitaler. Dabei müssen Schulen beim Einsatz von Online-Lernplattformen mit intelligenten tutoriellen Systemen (ITS) einige Besonderheiten beachten.

Online-Lernplattformen mit ITS ermöglichen auf Basis einer Datenanalyse die individuelle Förderung von Schüler*innen. Mit Hilfe von Lernstandserhebungen werden Stärken, Schwächen und Fortschritte der Schüler*innen in bestimmten Kompetenzbereichen erkannt und individuell angepasste Lernmaterialien zur Verfügung gestellt. Dabei sind die datenschutzrechtlichen Vorgaben einzuhalten, die allgemein beim Einsatz digitaler Systeme im Schulunterricht zu berücksichtigen sind. Darüber informieren mit der Veröffentlichung „Digitaler Unterricht in Schulen – Der Grundstein ist gelegt“, abrufbar unter www.ldi.nrw.de.

Darüber hinaus sind beim Einsatz von Online-Lernplattformen mit IST – unabhängig vom Einsatz Künstlicher Intelligenz – einige Punkte besonders zu beachten:

- Auch wenn sich die Schüler*innen bei der Nutzung dieser Online-Lernplattformen häufig nur mit Zahlencodes oder Fantasienamen identifizieren, werden personenbezogene Daten verarbeitet. In der Regel werden bei der Einrichtung von Accounts, mit denen der Zugriff zur Lernplattform gesteuert werden soll, Klarnamen verwendet. Lehrkräfte, die die Accounts einzelnen Schüler*innen zuordnen können, verarbeiten in jedem Fall personenbezogene Daten. Bei der Nutzung von Internetangeboten ist zudem davon auszugehen, dass die Anbieter zumindest IP-Adressen und Geräte-Informationen der Nutzer*innen verarbeiten. Diese Daten sind

dazu geeignet, eine Person bei der Nutzung anderer Dienste wiederzuerkennen und eine auf sie gerichtete Aktion – wie zum Beispiel personalisierte Werbung - auszuführen. Schulleitungen sollten daher kritisch hinterfragen, ob der Anbieter Rückschlüsse auf einzelne Nutzer*innen der Online-Lernplattformen ziehen kann.

- Das Schulgesetz NRW (§ 120 Abs. 5 Satz 2 SchulG NRW) erlaubt den Schulen, unter anderem für den Einsatz digitaler Lehr- und Lernsysteme (§ 8 Abs. 2 SchulG NRW) die Daten der Schüler*innen, Eltern und Lehrkräfte zu verarbeiten, soweit dies für ihre Aufgabenerfüllung, das heißt zur Erfüllung des Bildungs- und Erziehungsauftrags, erforderlich ist. Selbstverständlich muss der Einsatz von ITS im schulischen Kontext darüber hinaus verhältnismäßig sein und darf zum Beispiel keine Emotionserkennung ermöglichen. In jedem Fall müssen die Beteiligten umfassend über die Umstände und den Zweck der Verarbeitung ihrer Daten informiert werden.

- Wenn die Schule die Daten, die beim Einsatz der Online-Lernplattform anfallen, nicht selbst verarbeitet, kann die Plattform im Wege einer Auftragsverarbeitung realisiert werden. Charakteristisch für eine solche Auftragsverarbeitung ist, dass der Auftragsverarbeiter weisungsgebunden gegenüber dem Verantwortlichen und nicht selbst Verantwortlicher für die Datenverarbeitung ist (vgl. Art. 29 DS-GVO). Neben der Auswahl zuverlässiger Anbieter im Sinne der DS-GVO (Art. 28 Abs. 1) kommt es auf die vertragliche Regelung der Umstände der Auftragsverarbeitung an. Es sollte festgelegt sein, dass personenbezogene Daten nur entsprechend der Weisung der Schule sowie ausschließlich für ihre Zwecke verarbeitet werden. Zudem sollte die Vertraulichkeit im Zusammenhang mit der Verarbeitung sichergestellt sein. Sofern Anhaltspunkte dafür bestehen, dass Anbieter*innen bei der Verarbeitung personenbezogener Nutzer*innendaten eigene Zwecke verfolgen, etwa die Daten für Analysen zu Marketingzwecken oder Direktwerbung verwenden, empfiehlt die LDI NRW den Schulleitungen, Regelungen in die Auftragsverarbeitungsvereinbarung aufzunehmen, die dies verhindern.

- Die Schulen dürfen Anbieter die Schüler*innendaten regelmäßig nicht für eine Verarbeitung zu dessen eigenen Zwecken übermitteln, da sie Daten ihrer Schüler*innen an Personen oder Stellen außerhalb des öffentlichen Bereichs nur übermitteln dürfen, wenn die Person oder Stelle einen rechtlichen Anspruch auf die Bekanntgabe der Daten hat (§ 120 Abs. 7 Satz 3 SchulG NRW). Auch Einwilligungen sind regelmäßig keine wirksame Rechtsgrundlage für eine Übermittlung der Schüler*innendaten an den Anbieter. Im Zusammenhang mit dem Unterrichtsgeschehen mangelt es an der für eine wirksame Einwilligung notwendigen Freiwilligkeit der Entscheidung (siehe hierzu auch Ziffer II 2b der Veröffentlichung „Digitaler Unterricht in Schulen – Der Grundstein ist gelegt“).

- Beim Einsatz von Online-Lernplattformen mit ITS ist Art. 22 DS-GVO zu beachten. So hat die betroffene Person das Recht, keiner ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Art. 22 Abs. 1 DS-GVO). Sofern die Online-Lernplattformen den Schüler*innen auf der Grundlage ihrer Auswertungen in den getesteten Kompetenzbereichen individuell angepasste Lernmaterialien zur Verfügung stellen, deutet dies auf automatisierte Entscheidungen hin, die unter Art. 22 DS-GVO fallen. Diese dürfen zum Beispiel nicht alleinige Grundlage der Notengebung oder der Entscheidung über die weitere Förderung der Schüler*innen sein.

Fazit

Der Einsatz von Online-Lernplattformen mit ITS bietet zukunftsweisende Chancen, besser auf die individuellen Bedürfnisse der Schüler*innen einzugehen und den Lehrkräften Freiräume für andere Aufgaben zu schaffen. Dabei müssen im besonders geschützten Verantwortungsbereich der Schulen die Persönlichkeitsrechte der betroffenen Schüler*innen geachtet und deswegen datenschutzrechtliche Vorgaben beachtet werden.

9.2. Verantwortung für die Datenschutzkonformität von Hard- und Software in Schulen

Damit Schulen ihrer Verantwortung für die datenschutzgerechte Verarbeitung personenbezogener Daten nachkommen können, müssen ihnen die Schulträger geeignete Hard- und Software zur Verfügung stellen.

Eine Aussage des OVG NRW in einem seiner Protokolle (vom 22. Februar 2023, Az. 19 B 417/22) hat zu Nachfragen geführt: Danach sieht das Gericht die Verantwortung für die datenschutzgerechte Ausstattung der Schulen mit digitalen Arbeits- und Kommunikationsplattformen beim kommunalen Schulträger – und nicht bei der Schulleitung. Das Schulgesetz NRW (SchulG NRW) verpflichtet die Schulträger unter anderem dazu, den Schulen eine am allgemeinen Stand der Technik und Informationstechnologie orientierte Sachausstattung zur Verfügung zu stellen (§ 79 SchulG NRW). Auf der Grundlage dieser Vorschrift geht das Gericht davon aus, dass die Verpflichtung, datenschutzgerechte digitale Arbeits- und Kommunikationsplattformen zur Verfügung zu stellen, ausschließlich den kommunalen Schulträger trifft.

Die datenschutzrechtliche Verantwortung für die Verarbeitung personenbezogener Daten in inneren Schulangelegenheiten liegt andererseits bei den Schulen. Dies folgt aus § 5 Abs. 1 Satz 2 DSG NRW. Hiernach gelten Schulen

der Gemeinden und Gemeindeverbände, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, als (eigenständige) öffentliche Stellen im Sinne dieses Gesetzes. Die mit dem Einsatz der Arbeits- und Kommunikationsplattformen bezweckte Erfüllung des Bildungs- und Erziehungsauftrags ist eine innere Schulangelegenheit. Das bedeutet, dass allein die Schulen für die im Zusammenhang mit dem Einsatz der Arbeits- und Kommunikationsplattformen stattfindende Verarbeitung personenbezogener Daten verantwortlich sind.

Kommt der für die datenschutzgerechte Sachausstattung zuständige Schulträger seiner vom Gericht hervorgehobenen Verantwortung nicht nach, stehen die Schulleitungen vor einem großen Problem. Sie können die ihnen zur Verfügung gestellte Hard- und Software nicht nutzen, wenn ihr Einsatz unweigerlich mit unzulässigen Verarbeitungen der Daten von Schüler*innen und Lehrkräften verbunden ist. Der Schulträger muss daher darauf achten, Produkte zum Einsatz zu bringen, mit denen die Schulen ihre datenschutzrechtlichen Pflichten erfüllen können.

Sofern die vom Schulträger bereitgestellten Produkte nicht den Datenschutzvorgaben und damit nicht den Erfordernissen eines ordnungsgemäßen Unterrichts entsprechen, können sich die Schulleitungen an die Schulaufsicht wenden. Die Schulaufsichtsbehörden sollen eng mit den Schulträgern zusammenarbeiten (§ 88 Abs. 4 SchulG NRW) und haben unter anderem die Aufgabe, sie zur Erfüllung ihrer Pflichten anzuhalten (§ 86 Abs. 2 Satz 2 SchulG NRW). Hierzu gehört nach § 79 SchulG NRW, den Schulen eine am allgemeinen Stand der Technik und Informationstechnologie orientierte Sachausstattung zur Verfügung zu stellen, die – um zulässigerweise eingesetzt zu werden – auch die datenschutzrechtlichen Vorgaben erfüllen muss.

Fazit

Damit Schulen ihrer Verantwortung im Zusammenhang mit dem Einsatz von Hard- und Software gerecht werden können, benötigen sie die Unterstützung der Schulträger sowie der Schulaufsichtsbehörden.

9.3. Einsatz von Plagiatssoftware durch Hochschulen

Dürfen Hochschulen Daten der Studierenden an externe Unternehmen übermitteln, damit diese Unternehmen unter Einsatz entsprechender Software mögliche Plagiate und damit Täuschungsversuche aufspüren? Auslöser für die LDI NRW, sich mit dieser Frage zu befassen, war ein konkreter Fall: Eine betroffene Person hatte sich bei uns beschwert, nachdem ihre Abschlussarbeit von der Hochschule mit Hilfe von Plagiatssoftware begutachtet wurde. Dabei sollen mehr personenbezogene Daten an ein externes Unternehmen geflossen sein als nötig.

Die Übermittlung von Studierendendaten von Hochschulen an externe Unternehmen zur generellen, anlasslosen Plagiatsüberprüfung eingereichter Arbeiten ist zulässig, wenn die jeweiligen Prüfungsordnungen der Hochschulen dies so regeln (siehe Art. 6 Abs. 1 Unterabsatz 1 Buchstabe e DS-GVO in Verbindung mit § 3 Abs. 1 DSG NRW). Die Abnahme von Prüfungen ist Teil des öffentlichen Bildungsauftrags der Hochschulen. Dabei müssen sie Chancengleichheit für alle Studierenden in den für den Bildungsgang entscheidenden Prüfungen gewährleisten. Insbesondere angesichts der technischen Mittel, die den Studierenden heute zur Verfügung stehen, müssen die Hochschulen sicherstellen, dass einzelne Studierende sich durch das Kopieren fremder Texte keinen unlauteren Vorteil in der Prüfung verschaffen. Dies auszuschließen kann nur durch Plagiatsprüfungen wirksam erreicht werden.

Voraussetzung für eine datenschutzkonforme Plagiatsprüfung ist allerdings, dass die Daten zuvor pseudonymisiert werden. Für den Abgleich der Texte auf Plagiate benötigen die externen Unternehmen in keinem Fall die Klardaten der Studierenden. Es muss aus Sicht der Hochschulen lediglich gewährleistet sein, dass bei der Rückübermittlung die Ergebnisse der Plagiatsüberprüfung sicher bestimmtem Studierenden zugeordnet werden können. Hierfür ist die Vergabe eines Pseudonyms erforderlich, aber auch ausreichend. Dies gewährleistet eine auf das erforderliche Maß beschränkte Datenübermittlung. Von einer Pseudonymisierung kann nur ausgegangen werden, wenn das Pseudonym nicht mit der Matrikelnummer identisch ist und auch sonst keine Rückschlüsse auf die konkrete Person zulässt. Nur unter dieser Voraussetzung können die oben genannten Rechtsvorschriften auch als Rechtsgrundlage für eine regelmäßige Übermittlung von Daten der Studierenden an externe Unternehmen in Betracht kommen.

Eine Einwilligungslösung scheidet im Zusammenhang mit dem Prüfungsverfahren als Rechtsgrundlage für die Datenübermittlung regelmäßig aus. Wesentlich für eine wirksame Einwilligung ist, dass sie freiwillig erteilt wird. Nach Erwägungsgrund 42 DS-GVO sollte nur dann davon ausgegangen werden, dass die betroffene Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Liegt zudem ein Ungleichgewicht zwischen den Akteur*innen vor, wird nach Erwägungsgrund 43 DS-GVO davon ausgegangen, dass in solchen Konstellationen regelmäßig keine Freiwilligkeit der Einwilligungserklärung gewährleistet werden kann. Die Studierenden wären demnach nicht frei in ihrer Entscheidung, sich für oder gegen eine Plagiatsüberprüfung zu entscheiden. Sie könnten sich vielmehr gezwungen sehen, keine Einwände zu erheben, um sich keinem Täuschungsverdacht auszusetzen.

Die Arbeiten müssen nach erfolgter Plagiatsüberprüfung auf den Servern der externen Unternehmen gelöscht werden. Als weitere Maßnahme gemäß

Art. 32 DS-GVO bedarf es zudem einer transparenten Gestaltung des Verfahrens. Die Studierenden sind im Vorfeld in präziser, verständlicher sowie in klarer Art und Weise über den Einsatz einer Plagiatssoftware zu informieren.

Im konkreten Fall hatte die Beschwerde der betroffenen Person Erfolg. Die Hochschule muss für die Zukunft ihre Verfahrensweise in Plagiatsüberprüfungsfällen anpassen und entsprechende Maßnahmen umsetzen, die ein datenschutzgerechtes Vorgehen sicherstellen.

Fazit

Hochschulen können Plagiatssoftware datenschutzgerecht einsetzen, wenn sie die an die externen Unternehmen zu übermittelnden Daten zuvor pseudonymisieren. Voraussetzung ist in jedem Fall zudem eine transparente und hinreichend bestimmte Regelung in Bezug auf das Verfahren zur softwaregestützten Plagiatsüberprüfung in den Prüfungsordnungen der Hochschulen.

10. Verwaltung, Inneres und Justiz

10.1. Stichprobenkontrollen von Telekommunikationsüberwachungen und internationalen Datenübermittlungen der Polizei

Bei der ersten Stichprobenkontrolle von eingriffsintensiven heimlichen Polizeimaßnahmen und internationalen Datenübermittlungen der Polizei stellten wir keine rechtswidrigen Datenverarbeitungen fest. Allerdings müssen die Dokumentation des polizeilichen Handelns und die nachträglichen Benachrichtigungen der von der Überwachung betroffenen Personen verbessert werden.

Mit der Ende 2018 in Kraft getretenen großen Reform des Polizeigesetzes NRW wurden mehrere neue polizeiliche Maßnahmen ins Gesetz aufgenommen. Neben regelmäßigen Benachrichtigungspflichten der betroffenen Personen nach Abschluss der Maßnahmen sind aufgrund von § 33c PolG NRW nun regelmäßige Stichprobenkontrollen durch die LDI NRW vorgesehen.

Bei der im Abstand von zwei Jahren durchzuführenden Kontrolle wurden neben den stets zu prüfenden internationalen Datenübermittlungen der Polizei auch stichprobenartig Telekommunikationsüberwachungsmaßnahmen (TKÜ) geprüft. Hierbei handelt es sich u. a. um die Überwachung von Telefongesprächen, die über Festnetz oder Mobilfunk geführt werden.

Da die private nicht-öffentliche Kommunikation betroffen ist und die Maßnahmen heimlich erfolgen, greifen sie tief in die Privatsphäre ein. Sie sind daher an strenge gesetzliche Voraussetzungen gebunden. Zusätzlich sollen formelle Anforderungen der Eingriffsintensität der Maßnahme Rechnung tragen. So ist jede einzelne Überwachungsmaßnahme umfassend zu protokollieren und die betroffenen Personen sind nach Abschluss der Maßnahme grundsätzlich hierüber zu informieren. Die Benachrichtigung der betroffenen

Person dient der Sicherung ihrer Rechtsschutzmöglichkeiten, weil sie anderenfalls von der heimlichen Maßnahme keine Kenntnis erlangen würde. Die zu protokollierenden Angaben sind für eine effektive Kontrolle durch interne Datenschutzbeauftragte oder die LDI NRW ebenso wichtig wie für eine von einer betroffenen Person angestoßene gerichtliche Prüfung der Rechtmäßigkeit der Überwachungsmaßnahme. Die Umsetzung dieser formellen Vorgaben war bei den geprüften Maßnahmen unzureichend. Notwendige Angaben waren nicht protokolliert, etwa welche Personen von der Maßnahme betroffen waren und welches Mittel seitens der Polizei eingesetzt wurde. Benachrichtigungen erfolgten in keinem Fall. Gründe hierfür wurden nicht dokumentiert. Die Voraussetzungen für die Durchführung der Maßnahme lagen dagegen jeweils vor.

Die geprüften Polizeibehörden räumten die Mängel ein und leiteten Maßnahmen zur Verbesserung des Verfahrens ein. Eine förmliche Beanstandung haben wir deswegen nicht ausgesprochen.

Neben den TKÜ-Maßnahmen haben wir auch internationale Datenübermittlungen durch die Polizei geprüft. Gegenstand der Kontrolle waren die internationalen Übermittlungen personenbezogener Daten aus dem Programm „Konzeption zum Umgang mit rückfallgefährdeten Sexualstraftätern (KURS)“ der Jahre 2019 bis 2021 im Gefahrenabwehrbereich durch das Landeskriminalamt NRW (LKA NRW). Diese Datenübermittlungen in Drittländer erfolgen über das Bundeskriminalamt als zentrale INTERPOL-Kommunikationsstelle. Die Übermittlungen von Daten aus KURS in ein Drittland erfordern eine Einzelfallprüfung der Verhältnismäßigkeit und der Erforderlichkeit unter Berücksichtigung der rechtlichen Situation im Zielstaat. Bei der Prüfung wurden keine materiellen Verstöße festgestellt. Zur Auffindbarkeit der Einzelvorgänge und zum Nachweis der vorgenommenen Bewertungen der rechtlichen Situation im Drittland wurden Verbesserungen beim LKA NRW umgesetzt.

Fazit

Bei den geprüften Maßnahmen handelt es sich um neue gesetzliche Regelungen, zu denen eine geübte und insgesamt rechtskonforme Praxis bei den Polizeibehörden noch nicht festgestellt werden konnte. Die geprüften Behörden haben ihre Verfahren für solche Maßnahmen jedoch zwischenzeitlich angepasst. Im Ergebnis konnte mit der Kontrolle sichergestellt werden, dass die Verantwortlichen nun neben den materiellen Voraussetzungen auch die formellen Vorgaben für die Durchführung der Maßnahmen besser beachten.

10.2. Zweite Kontrolle der „Strategischen Fahndung“ hat Bedenken noch nicht ganz ausgeräumt

Der Einsatz der sog. „Strategischen Fahndung“ ist inzwischen polizeiliche Routine. Im Rahmen einer ersten Überprüfung dieses Instruments im Jahr 2019 wurde durch die LDI NRW festgestellt, dass tausende Kontrollen von Passant*innen von der Polizei durchgeführt wurden, ohne den angestrebten Erfolg zu erreichen. Die Folgekontrolle in 2023 zeigte, dass die überprüften Behörden inzwischen sensibler mit dem Instrument umgehen.

Mit § 12a Polizeigesetz NRW wurde Ende 2018 die gesetzliche Grundlage für das Instrument der „Strategischen Fahndung“ geschaffen. Die Polizei kann danach bei Vorliegen bestimmter Voraussetzungen für einen Zeitraum von zunächst bis zu 28 Tagen in einem festgelegten Gebiet ohne konkreten Verdacht Personenkontrollen und Identitätsfeststellungen durchführen sowie Einsicht in Fahrzeuge nehmen. Zweck ist die Gefahrenabwehr.

Die LDI NRW berichtete bereits in ihrem 25. Bericht unter 10.2 über die Ergebnisse der Überprüfung in 2019. Inzwischen wurden drei weitere Anwendungen der „Strategischen Fahndung“ geprüft – ohne dass es Beanstandungen gab. Die Behörden sind datensparsamer vorgegangen als noch 2019. Möglich wurde das durch einen spezifischeren Zuschnitt der festgelegten Rahmenbedingungen sowie durch Beschränkung des kontrollierten Personenkreises. Die Kontrollen wurden – anders, als es die Maßnahme durchaus auch zulassen würde – teilweise nicht gegenüber sämtlichen Passanten durchgeführt, sondern lediglich bei Personen, deren Verhalten nach konkreter Auswertung des Personals vor Ort Auffälligkeiten aufwies.

Festgestellt wurde zudem, dass die erhofften Erfolge der „Strategischen Fahndung“ zwar teilweise erreicht wurden, jedoch hinter den eigentlichen Erwartungen zurücklagen. Bei einer Behörde wurde die durchgeführte Maßnahme nicht ausreichend dokumentiert. Die Dokumentation sollte – neben Ausführungen zu den Gründen und der Art der Durchführung der jeweiligen Maßnahme – auch eine Abwägung zu möglichen milderen Maßnahmen beinhalten. Entsprechende Erläuterungen wurden im Rahmen der Prüfung von der überprüften Behörde nachgeliefert.

Unsere im Gesetzgebungsverfahren geäußerten Bedenken in Bezug auf die Verhältnismäßigkeit der Eingriffe in die Grundrechte zahlreicher Personen im Vergleich zum Zweck der Maßnahme konnten durch die Kontrollen allerdings nicht ausgeräumt werden. Es fehlen nach wie vor nennenswerte Erfolge, die eindeutig auf die Maßnahme zurückführbar sind. Das lässt weiterhin Zweifel an der Verhältnismäßigkeit dieses Instruments zu.

Fazit

Auch wenn die kontrollierten Polizeibehörden seit unserer ersten Prüfung sensibler geworden sind, bleibt die „Strategische Fahndung“ im Hinblick auf die Streubreite der Eingriffe in die Rechte Betroffener ein kritisches Instrument. Die LDI NRW wird es daher weiter im Blick behalten.

10.3. Videoüberwachung von Containerstandorten

Altglas- oder Altpapier-Container steigern die Ressourceneffizienz. Ärgerlich ist, wenn die Standorte missbraucht werden, um auch noch allen anderen Abfall dort loszuwerden – vom Sperrgut bis zum Sondermüll. Trotzdem haben Kommunen grds. nicht das Recht, die Umgebung der Containerstandorte mit Videokameras zu überwachen, weil sie damit auch das Verhalten der Bürger*innen erfassen, die sich ordnungsgemäß verhalten.

Die Videoüberwachung abseits gelegener und schwer einsehbarer Standorte erscheint Kommunen auf den ersten Blick erfolgversprechend, um illegale Müllablagerung zu verhindern.

Die Regelung für die Videoüberwachung öffentlich zugänglicher Bereiche durch öffentliche Stellen findet sich im Datenschutzgesetz NRW (§ 20 DSG NRW). Damit eine Videoüberwachung zulässig ist, muss sie einen in Absatz 1 des § 20 DSG NRW genannten Zweck verfolgen.

Eine Videoüberwachung kann etwa zur Wahrnehmung des Hausrechts im Sinne von § 20 Abs. 1 Nr. 1 DSG NRW dienen, wenn es sich bei dem Containerstandort um ein „befriedetes Besitztum“ (im Sinne des § 123 Abs. 1 Strafge-

setzbuch) handelt, das nicht jeder betreten darf. Dies dürfte regelmäßig nicht der Fall sein. Die Videoüberwachung kann auch den Schutz des Eigentums an den Containern selbst bezwecken (§ 20 Abs. 1 Nr. 2 DSG NRW), etwa weil es zu häufigen Brandstiftungen an den Containern gekommen ist. Hier kann eine Videoüberwachung zum Schutz am Containereigentum in Betracht kommen, wenn ausreichende technische Vorkehrungen getroffen sind, die dem Schutz der unbescholtenen Nutzer*innen und Passant*innen des Containerstandorts Rechnung tragen. Dazu zählen beispielsweise ein eng auf die Container gerichteter Kamerafokus, Auswertung der Daten nur bei Zerstörungen am Container und regelhaftes und kurzfristiges Überschreiben der Daten, wenn es keine Vorkommnisse gibt. Sofern die beabsichtigte Videoüberwachung allerdings ausschließlich darauf zielt, das möglicherweise rechtswidrige Verhalten von Personen im Umfeld der Containerstandorte zu kontrollieren, ist dies durch § 20 DSG NRW nicht gedeckt. Ein Rückgriff der Kommunen auf die polizeigesetzliche Norm zur Videoüberwachung einzelner öffentlich zugänglicher Orte (§ 15a Polizeigesetz NRW) ist im Ordnungsbehördengesetz NRW (§ 24 Abs. 1 Satz 1 Nr. 6) nicht vorgesehen und scheidet für die kommunalen Ordnungsbehörden deshalb ebenfalls aus.

Zu beachten ist: § 20 DSG NRW erlaubt eine Videoüberwachung nur, um Schaden von einem Rechtsgut abzuwenden. Eine Videoüberwachung zu Zwecken der Verfolgung zivilrechtlicher Ansprüche, der Strafverfolgung oder der Verfolgung von Ordnungswidrigkeiten wird dadurch nicht erfasst.

Bisweilen verweisen Kommunen auf § 20 Abs. 3 DSG NRW, um sich zu rechtfertigen. Dabei handelt es sich lediglich um eine „Zweckänderungsvorschrift“. Sie besagt, dass die erhobenen Daten (also die gemachten Aufnahmen) zwar für einen anderen als den ursprünglichen Zweck verwendet werden dürfen (zum Beispiel zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten). Sie erlaubt aber keinen weiteren über Absatz 1 hinausgehenden Zweck für die Erhebung der Daten.

Eine Videoüberwachung unter dem präventiven Aspekt der Abschreckung vor illegalen Müllentsorgungen ist auch deshalb keine Lösung des Problems, weil sich die illegale Müllentsorgung dann nur an andere Orte verlagern dürfte, die nicht überwacht werden.

Fazit

Für eine Videoüberwachung von Containerstandorten, an denen es zu einer widerrechtlichen Entsorgung von Abfall kommt, gibt es in NRW regelmäßig keine rechtliche Grundlage.

10.4. Waffenrecht: Durch Zuverlässigkeitsüberprüfungen gewonnene Daten müssen gelöscht werden

Die gesetzliche Verpflichtung, regelmäßig die Zuverlässigkeit von Personen zu prüfen, die waffenrechtliche Erlaubnisse besitzen, darf nicht dazu führen, dass die so gewonnenen Daten dauerhaft gespeichert werden. Im Regelfall ist nur das zuletzt festgestellte Ergebnis zur Beurteilung der waffenrechtlichen Zuverlässigkeit von Bedeutung. Nur wenn eine waffenrechtliche Erlaubnis aus bestimmten Gründen versagt wird, dürfen Daten für einen deutlich längeren Zeitraum gespeichert werden.

Nach dem Waffengesetz hat die zuständige Behörde die Zuverlässigkeit aller Personen, die eine waffenrechtliche Erlaubnis besitzen, in regelmäßigen Abständen – mindestens jedoch nach Ablauf von drei Jahren – zu überprüfen. Zuständige Waffenbehörde ist in NRW die Polizei. Die Überprüfungen erfolgen mit Hilfe des Waffenverwaltungssystems „CitkoWaffe“. Dabei wird automatisiert eine Überprüfung der Zuverlässigkeit angestoßen. Zur Überprüfung werden auch polizeiliche Datenbanken herangezogen. Die Prüfungsergebnisse werden in „CitkoWaffe“ gespeichert, zudem werden sie meist der Papierakte beigefügt.

In den waffenrechtlichen Unterlagen sind mitunter sehr sensible Informationen enthalten. Bislang war eine regelmäßige Löschung von Daten, die für die Überprüfung nicht mehr erforderlich waren, nicht vorgesehen. Vielmehr waren seit der Inbetriebnahme von „CitkoWaffe“ alle Daten im Waffenverwaltungssystem hinterlegt und abrufbar. Auch die Papierakte enthält in vielen Fällen die gesamten Überprüfungsergebnisse – seit Bestand der Akte. Eine Rechtsgrundlage für das Vorhalten dieser Daten über die aktuelle Überprüfung hinaus gibt es bei fortbestehender Zuverlässigkeit nicht. Dies könnte im Einzelfall dazu führen, dass Daten aus früheren Überprüfungen zur Beurteilung der Zuverlässigkeit herangezogen werden, die nicht mehr verwertet werden dürften.

Die Thematik wurde bereits mit dem Innenministerium NRW erörtert. Dort wird die Rechtsauffassung der LDI NRW geteilt und eine Handlungsnotwendigkeit erkannt. Auf Grundlage der Beratung durch die LDI NRW wird im Ministerium aktuell an einer Lösung zur Einführung einer Löschroutine in „CitkoWaffe“ sowie der Anpassung der Aktenhaltung gearbeitet.

Fazit

Nur weil es keine spezialgesetzliche Regelung zur Datenlöschung gibt, heißt das nicht, dass Daten langfristig gesammelt und gespeichert werden dürfen. Es gilt immer der Grundsatz, dass Daten nur so lange gespeichert werden dürfen, wie sie für eine konkrete Aufgabe erforderlich sind. Die Beratung der verantwortlichen Stelle hat hier Wirkung gezeigt. Die LDI NRW begrüßt dies und wird die Umsetzung weiter begleiten. Betroffenen empfiehlt die LDI NRW, sich zwecks Bereinigung ihrer Akte direkt an die für sie zuständige Waffenbehörde zu wenden.

10.5. Veröffentlichung der Vorschlagsliste für Schöff*innen

Es ist die Aufgabe der Kommunen, den Amtsgerichten Bürger*innen für das Schöffenamt vorzuschlagen. Zu diesem Zweck wird eine Liste erstellt, die neben den Namen der potenziellen Schöff*innen weitere persönliche Angaben enthält. Diese kommunalen Vorschlagslisten dürfen nicht im Internet veröffentlicht werden.

Im vergangenen Jahr haben einige Kommunen die Vorschlagslisten für Schöff*innen für jeden einsehbar im öffentlichen Bereich des Ratsinformationssystems im Internet veröffentlicht. Zudem enthielten die Listen teilweise die vollständigen Adressen und Geburtsdaten der Vorgeschlagenen. Dies stellt einen Datenschutzverstoß dar. Welche Daten die Listen enthalten dürfen bzw. müssen und wie von kommunaler Seite mit ihnen zu verfahren ist, ist in § 36 Gerichtsverfassungsgesetz (GVG) geregelt.

Das GVG sieht ausdrücklich nur ein Auflegen „in der Gemeinde“, also vor Ort vor. Zudem ist die Dauer des Auslegens auf eine Woche befristet. Eine Veröffentlichung im Internet – dazu noch für einen längeren Zeitraum – ist davon nicht abgedeckt. Darüber hinaus muss die Liste Familienname, Vornamen, ggf. einen vom Familiennamen abweichenden Geburtsnamen, Geburtsjahr, Wohnort einschließlich Postleitzahl sowie Beruf der vorgeschlagenen Person enthalten. Bei häufig vorkommenden Namen ist auch der Stadt- oder Ortsteil des Wohnortes aufzunehmen. Weitere personenbezogene Angaben sind gesetzlich nicht vorgesehen und dürfen daher in den Listen nicht vorhanden sein.

Fazit

Für die Veröffentlichung personenbezogener Daten von Schöff*innen im Online-Ratsinformationssystem gibt es keine Rechtsgrundlage. Die Vorgaben des § 36 GVG müssen beachtet werden.

10.6. Digitale Verwaltung: LDI NRW regt Erlass einer Rechtsvorschrift für automatisierte Förderentscheidungen an

Förderverfahren sind eines der wichtigsten Instrumente der Verwaltung, um politische Ziele zu erreichen. In der Praxis werden sie regelmäßig auf der Grundlage von verwaltungsinternen Förderrichtlinien durchgeführt. Schon bei der analogen Abwicklung stellt sich daher häufig die Frage, ob eine ausreichende Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten von Antragsteller*innen besteht (vgl. 29. Tätigkeitsbericht des BayLfD 2020, Kapitel 5.4). Zwei aktuelle Gerichtsurteile machen nun klar: Mit der voranschreitenden Digitalisierung der Verwaltung stößt die überkommene Praxis endgültig an ihre Grenzen. Die LDI NRW regt daher an, zeitnah eine Rechtsvorschrift für automatisierte Förderentscheidungen zu erlassen.

NRW arbeitet intensiv an der Digitalisierung von staatlichen Förderverfahren. Schon seit einigen Jahren wird ein Landesstandard für digitale Förderverfahren entwickelt (§ 1 Nr. 8 Rechtsverordnung zur Aufgabenübertragung auf die d-NRW AöR; Landtags-Vorlage 17/5623, Seite 25 f.; Landtags-Vorlage 17/6009, Randnummer 223 ff.).

Das Ziel ist die Ende-zu-Ende-Digitalisierung. Nicht nur sollen Förderanträge digital eingereicht werden können; auch ihre Bearbeitung in der Verwaltung soll digital erfolgen. Es wird zudem darüber nachgedacht, Förderungen im Wege von Pauschalzahlungen vorzunehmen. Auch dies soll die digitale Abwicklung erleichtern (Zukunftsvertrag für Nordrhein-Westfalen: Koalitionsvereinbarung von CDU und Grünen 2022 – 2027, Seite 108). Damit sind die Weichen für digital und automatisiert durchgeführte Förderverfahren gestellt.

Bei den rechtlichen Grundlagen wird jedoch noch immer in erster Linie über den Abbau von Schriftformerfordernissen und die Angleichung von Förderrichtlinien diskutiert. Mit Blick auf die digitale Zukunft der Förderverfahren greift dies aber zu kurz, wie zwei aktuelle Gerichtsurteile zeigen.

Mitte März 2023 urteilte das OVG NRW zur NRW Soforthilfe 2020, mit der NRW auf die wirtschaftlichen Auswirkungen der Corona-Pandemie reagiert hatte. Das Förderprogramm sollte finanzielle Notlagen bei gewerblichen Kleinunternehmen, Selbstständigen und Freiberuflichen mildern. Es wurde auf der Grundlage von Förderrichtlinien, öffentlichen Verlautbarungen und erläuterten Antragsformularen der Landesregierung abgewickelt. Die Bewilligungsbescheide wurden zwar noch von Sachbearbeiter*innen erlassen. Die Erstellung der Schluss- und Rückforderungsbescheide erfolgte jedoch automatisiert.

Das OVG NRW stellte klar, dass nach dem Verwaltungsverfahrensgesetz NRW (VwVfG NRW) die vorläufigen Bewilligungsbescheide und die Schlussbescheide als getrennte und jeweils eigenständige Verwaltungsentscheidungen anzusehen seien. Nach § 35a VwVfG NRW seien die Schlussbescheide unter anderem deshalb rechtswidrig, weil die rein automatisierten Entscheidungen nicht durch Rechtsvorschrift zugelassen gewesen seien (OVG NRW, Urteil vom 17. März 2023, Az. 4 A 1987/22, juris Randnummer 191 bis 196).

Anfang Dezember 2023 befasste sich der Europäische Gerichtshof (EuGH) in einem Grundsatzurteil mit Art. 22 DS-GVO. Diese Norm untersagt Entscheidungen, die ausschließlich auf einer automatisierten Verarbeitung personenbezogener Daten beruhen, solange sie nicht aufgrund einer Rechtsvorschrift zulässig sind.

In dem Urteil ging es zwar nicht um ein Förderverfahren der öffentlichen Hand. Gegenstand der Entscheidung waren von Auskunfteien automatisiert erstellte Scorewerte zur Bonität von Personen, die für Kreditentscheidungen

genutzt werden. Das Gericht lässt jedoch keine Zweifel daran, dass der Anwendungsbereich von Art. 22 DS-GVO möglichst weit zu verstehen ist. Nur so könne der Zweck der Vorschrift erreicht werden, „Personen vor den besonderen Risiken für ihre Rechte und Freiheiten zu schützen, die mit der automatisierten Verarbeitung personenbezogener Daten [...] verbunden sind“ (Urteil vom 7. Dezember 2023, Az. C-634/21, juris Randnummer 57).

Zumindest automatisiert erstellte Ablehnungsbescheide in Förderverfahren setzen damit eine datenschutzkonforme Rechtsgrundlage voraus.

Mit dem Fortschritt der Verwaltungsdigitalisierung wird die Zahl der automatisierten Förderverfahren steigen. Die aktuelle Rechtsprechung macht deutlich, dass spätestens ab diesem Zeitpunkt verwaltungsinterne Förderrichtlinien für eine rechtssichere Durchführung nicht mehr genügen. Die Anforderungen an Datenschutz und digitale Verwaltungsverfahren verlangen stattdessen faire und transparente Regelungen durch ein Gesetz.

Die LDI NRW empfiehlt der Landesregierung deswegen, rechtzeitig für künftige automatisierte Förderentscheidungen der Landesverwaltung eine grundsätzliche Regelung zur Zulässigkeit automatisierter Förderentscheidungen mit Widerspruchsmöglichkeit zu treffen. Vorbilder für solche Regelungen gibt es (zum Beispiel § 155 Abs. 4 der Abgabenordnung). Diese können aber nicht auf Förderverfahren des Landes angewendet werden. Insoweit ist ein eigenes Rechtssetzungsverfahren, etwa im Bereich der Landeshaushaltsordnung, sinnvoll.

Fazit

Als Konsequenz aus den aktuellen Entscheidungen von OVG NRW und EuGH regt die LDI NRW an, rechtzeitig für künftige automatisierte Förderentscheidungen der Landesverwaltung eine grundsätzliche Vorschrift zur Zulässigkeit mit Widerspruchsmöglichkeit zu schaffen. Dies ermöglicht in zukünftigen Förderkonstellationen eine schnelle und rechtssichere Bereitstellung von Fördermitteln.

10.7. Energiepreispauschale für Studierende: unbürokratisch, digital, aber auch datenschutzgerecht?

In Notsituationen wollen Politik und Verwaltung schnell und unbürokratisch helfen. Das war auch der Anspruch der Bundesregierung, als es um die Zahlung der Energiepreispauschale für etwa 3,5 Millionen Studierende und Fachschüler*innen ging. Die Ansprüche und ihre digitale Umsetzung müssen aber auch Datenschutzrecht beachten.

Ende 2022 trat das Studierenden-Energiepreispauschalengesetz (EPPSG) in Kraft. Es sah vor, dass Studierende und Fachschüler*innen eine Energiepreispauschale in Höhe von 200 Euro erhalten sollten. Hierdurch sollten die aufgrund des Russisch-Ukrainischen Krieges gestiegenen Energiekosten ausgeglichen werden.

Bereits in der Diskussion über den Entwurf des EPPSG im Bundesrat hatten die Länder darauf hingewiesen, dass datenschutzrechtliche Fragen nicht ausreichend geregelt seien (Bundesrat Drucksache 634/1/22 vom 9. Dezember 2022). Der Vermittlungsausschuss wurde jedoch nicht angerufen, damit die Hilfen möglichst schnell ausgezahlt werden konnten (Bundesrat Plenarprotokoll 1029, 16. Dezember 2022, Seite 540, 561).

Das EPPSG sollte durch die Bundesländer umgesetzt werden. In einer Bund-Länder-Arbeitsgruppe wurden hierzu eine Muster-Rechtsverordnung sowie eine Verwaltungsvereinbarung zum Betrieb einer zentralen Antragsplattform ausgearbeitet. Danach sollten die Hochschulen der jeweils zuständigen Landesbehörde vorab eine Liste von Personalien ihrer Studierenden überlassen, und zwar unabhängig davon, ob die/der Studierende einen Antrag auf Auszahlung der Pauschale stellen würde. Die Landesbehörden sollten diese Listen dann in ein bundesweit einheitliches Softwaresystem eingeben, um im Falle einer Antragstellung die Berechtigung der antragstellenden Person und die Frage überprüfen zu können, ob diese evtl. schon zuvor (etwa aufgrund

eines Parallelstudiums an einer anderen Hochschule) einen solchen Antrag gestellt hat. Dieses Verfahren sollte auch für die Ausbildungsstätten von Fachschüler*innen gelten.

Nachdem zur Umsetzung des EPPSG bereits die Datenschutzaufsichtsbehörden einzelner Länder von der jeweiligen Landesregierung zurate gezogen worden waren, nahm die DSK zu den bundesweit einheitlichen Planungen am 3. Februar 2023 von sich aus Stellung.

Die DSK wies darauf hin, dass eine bereits vor Antragstellung erfolgende Verarbeitung der personenbezogenen Daten aller Studierenden und Fachschüler*innen für die Entscheidung über die Bewilligung der Pauschale nicht zwingend erforderlich sei. Außerdem stelle der bundesweite Abgleich, ob eine antragstellende Person bereits anderweitig einen Antrag gestellt habe, einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Um eine derartige Regelung durch Verordnung der Länder zu treffen, hätte zugunsten der Landesregierungen eine entsprechende Verordnungsermächtigung in das EPPSG aufgenommen werden müssen. Dies sei jedoch nicht geschehen.

In ihrer Stellungnahme erkannte die DSK allerdings auch an, dass es zu einer ganz erheblichen weiteren Verzögerung der Auszahlungen führen würde, wenn nunmehr noch zuvor das EPPSG geändert werden müsste. Um eine zeitnahe Auszahlung an die Berechtigten zu ermöglichen, konzentrierte sich die Stellungnahme daher auf die Empfehlung zur Verwendung geeigneter kryptografischer Verfahren, um eine unbefugte Entschlüsselung und Kenntnisnahme der von den Hochschulen an die vorgesehene zentrale Plattform übermittelten Daten zu verhindern. Schließlich forderte die DSK die Festlegung nachvollziehbarer Fristen zur Aufbewahrung bzw. Löschung der anfallenden Daten.

Die LDI NRW hat die DSK-Stellungnahme dem Kultur- und Wissenschaftsministerium NRW zur Kenntnis gegeben. Die Anfang März 2023 in Kraft getretene nordrhein-westfälische Verordnung zur Durchführung des EPPSG kam der Forderung der DSK nach Einführung konkreter Löschfristen teilweise nach: Die von den Ausbildungsstätten zu erstellenden Listen von Personalien ihrer Studierenden waren spätestens zum 31. Dezember 2023 zu löschen.

Zwischen Mitte März 2023 und Ende September 2023 wurden bundesweit ca 2,8 Millionen Anträge nach dem EPPSG bewilligt, so dass etwa 80 Prozent der ca. 3,5 Millionen Anspruchsberechtigten Leistungen erhielten (Bundestagsdrucksache 20/8545 vom 27. September 2023, Seite 3 f.). Diese Statistik zeigt, dass bei einem Fünftel der Antragsberechtigten personenbezogene Daten verarbeitet wurden, ohne dass ein Antrag auf Förderung gestellt wurde.

Fazit

Förderverfahren der öffentlichen Hand werden häufig in Notsituationen aufgelegt. Politik und Verwaltung wollen den Bedürftigen unbürokratisch helfen und bedienen sich hierzu immer häufiger digitaler Instrumente. Erfolgversprechend ist ein solches Vorgehen jedoch nur, wenn hierbei der Datenschutz beachtet wird. Im Ergebnis ist nämlich mit rechtswidrig gewährten Hilfen niemandem geholfen. Beim EPPSG drückten die Länder im Bundesrat und die Datenschutzaufsichtsbehörden gegenüber den diesbezüglichen Bedenken noch einmal beide Augen zu. Die Stellungnahme der DSK zum EPPSG hat aber nunmehr die datenschutzrechtlichen Anforderungen an solche Förderverfahren ausformuliert. Diese müssen bei zukünftigen Förderverfahren beachtet werden.

11. Gesundheit und Soziales

11.1. Datenschutz und Digitalisierung im Gesundheitsbereich

Mit zahlreichen Gesetzesvorhaben der Europäischen Union (EU) sowie des Bundes wurde die digitale Transformation des Gesundheitsbereichs in 2023 vorangetrieben. Die LDI NRW beteiligt sich an den Arbeiten der DSK, die bereits im Gesetzgebungsverfahren einen besseren Datenschutz erzielen wollen.

In 2023 sind verschiedene Stellungnahmen der DSK, etwa zur Modernisierung medizinischer Register, zur Harmonisierung der Forschungsklauseln in den Landeskrankenhausgesetzen sowie zu den Vorschlägen der EU-Kommission zur Errichtung eines Europäischen Gesundheitsdatenraums entstanden. Auf diese Weise gelingt es der DSK, schon im Gesetzgebungsverfahren – und nicht erst im Nachhinein – konkrete Vorschläge für einen besseren Datenschutz an die Gesetzgeber zu adressieren, um einen bestmöglichen Schutz sensibler Gesundheitsdaten sicherzustellen.

Bereits seit 2022 wird etwa in der EU um einen europäischen Raum für Gesundheitsdaten gerungen. Damit soll etwa die Nutzung von digitalen Gesundheitsdaten für eine bessere medizinische Versorgung, für Forschung, Innovation und Politikgestaltung ermöglicht werden. Parallel hierzu wurde vom Bundestag neben dem „Gesundheitsdatennutzungsgesetz“ auch das „Digital-Gesetz“ verabschiedet, das sich unmittelbar auf den ärztlichen Behandlungsalltag sowie die Patient*innen auswirkt. So wurde mit dem Gesetz nicht nur die Einführung der elektronischen Patientenakte für alle beschlossen, um den Austausch und die Nutzung von Gesundheitsdaten, etwa auch durch Forschende, voranzutreiben und die Versorgung zu unterstützen. Auch weitere digitale Lösungen, wie das E-Rezept oder sog. Digitale Gesundheitsanwendungen, wurden verbindlich eingeführt bzw. weitergehend in die Behandlungswege integriert.

Die Digitalisierung erfasst damit eine immer größere Menge besonders geschützter Daten der Bürger*innen. Mit den erhofften Vorteilen für Behandlung und Forschung gehen zwangsläufig neue Risiken für die Rechte der Betroffenen einher. Damit diese bereits im Rahmen der Gesetzgebung mitgedacht und ihnen wirksam begegnet wird, setzt sich die LDI NRW als Mitglied der DSK für die datenschutzrechtlichen Belange der Betroffenen ein.

Zentrale Forderungen der DSK sind hier unter anderem,

- dass bereits im Gesetz angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person festgelegt werden, damit die sichere und vertrauliche Verarbeitung ihrer Gesundheitsdaten sichergestellt wird. Denn die Digitalisierung des Gesundheitswesens kann nur gelingen, wenn die Bürger*innen darauf vertrauen können, dass ein hoher Schutz ihrer Daten gewährleistet bleibt.
- dass der Mensch bei der weitergehenden Nutzung von Gesundheitsdaten, etwa zu Forschungszwecken, erkennbar im Mittelpunkt steht. Betroffene müssen dazu bei Entscheidungen über die Nutzung ihrer Daten eingebunden und ihre Rechte aus der DS-GVO dürfen nicht verkürzt werden.
- dass die betroffenen Personen eine effektive Kontrolle über die Verarbeitung ihrer personenbezogenen Daten behalten. Verantwortliche müssen ihnen präzise und leicht verständliche Informationen geben. Sämtliche Übermittlungswege und Verarbeitungsprozesse müssen für die Betroffenen transparent sein.
- dass digitale Methoden zur Ausübung der Betroffenenrechte gesetzlich gefördert werden. Beispielsweise können digitale Portale das Einwilligungsmanagement oder die Ausübung von Betroffenenrechten erleichtern.

Weitere Einzelheiten ergeben sich aus:

- Stellungnahme der DSK zum Referentenentwurf des Bundesministeriums für Gesundheit: Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG – Stand 03.07.2023) vom 14. August 2023 (abrufbar unter www.datenschutzkonferenz-online.de)
- Stellungnahme der Datenschutzkonferenz „Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen“ vom 27. März 2023 (Abdruck im Anhang)
- Entschließung der Datenschutzkonferenz „Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register“ vom 22./23. November 2023 (Abdruck im Anhang)
- Entschließung der Datenschutzkonferenz „Datenschutz in der Forschung durch einheitliche Maßstäbe stärken“ vom 23. November 2023 (Abdruck im Anhang)

Fazit

Die zunehmende Digitalisierung des Gesundheitswesens kann die Behandlung der Patient*innen verbessern, eine grenzüberschreitende Nutzung dieser Daten fördern und die medizinische Forschung zum Wohle der Patient*innen voranbringen. Sie birgt jedoch zusätzliche Risiken für die Rechte und Freiheiten der Betroffenen. Um diesen zu begegnen, setzt sich die LDI NRW gegenüber den Gesetzgebern in Land, Bund und EU für die datenschutzrechtlichen Belange der Betroffenen ein.

11.2. Übermittlung erlaubt: Meldedaten helfen bei der Krebsfrüherkennung

Die LDI NRW erreichen regelmäßig Beschwerden von Frauen, deren Meldedaten genutzt wurden, um sie zu Untersuchungen im Rahmen der Krebsfrüherkennung einzuladen.

Bundesweit erhalten Frauen ab 50 Jahren alle zwei Jahre eine Einladung zur freiwilligen Untersuchung im Mammographie-Screening-Programm. Die Untersuchung dient der Krebsfrüherkennung. Für die Einladungen werden im Rahmen der gesetzlichen Bestimmungen Daten der Einwohnermeldeämter genutzt.
Betroffene Frauen, die sich an die LDI NRW wenden, bezweifeln die Rechtmäßigkeit der Verarbeitung ihrer Meldedaten für die Einladung zum Mammographie-Screening. Sie empfinden eine Nutzung ihrer Daten als übergriffig und teilen mit, dass sie ihre Einwilligung dazu nicht erteilt haben.

Da die Datenübermittlung auf einer gesetzlichen Grundlage beruht, bedarf es dazu allerdings keiner Einwilligung der betroffenen Personen. Auch ein Widerspruch gegen die Datenübermittlung ist nicht möglich. Die LDI NRW informiert die Betroffenen bei Beschwerden entsprechend. Laut Sozialgesetzbuch sollen organisierte Krebsfrüherkennungsprogramme angeboten werden (§ 25a Abs. 1 Sozialgesetzbuch Fünftes Buch). Das Nähere regelt die Richtlinie des Gemeinsamen Bundesausschusses über die Früherkennung von Krebserkrankungen (Krebsfrüherkennungs-Richtlinie – FE-RL). Nach § 11 Abs. 5 KFE-RL lädt die Zentrale Stelle bei der Kassenärztlichen Vereinigung zur Teilnahme am Früherkennungsprogramm ein.

Die Zentrale Stelle ist berechtigt, die für die Einladung benötigten personenbezogenen Daten von den Personen, die aufgrund ihres Alters und ihres Geschlechts Anspruch auf eine Krebsfrüherkennungsuntersuchung haben, bei den Meldebehörden zu erheben, zu verarbeiten und zu speichern (§ 16 Abs. 1 Satz 1 Landeskrebsregistergesetz – LKRG NRW).

Die Meldebehörden übermitteln für die Versendung der Einladungen der zuständigen Stelle von jeder Person, die am jeweiligen Stichtag das 50. Lebensjahr vollendet und das 70. Lebensjahr noch nicht vollendet haben, monat-

lich die folgenden Angaben (nach § 10 Meldedatenübermittlungsverordnung MeldDÜV NRW):

1. Familienname
2. frühere Familiennamen
3. Vornamen
4. Geburtsdatum und -ort
5. derzeitige Anschrift und
6. bedingter Sperrvermerk nach § 52 des Bundesmeldegesetzes.

Das LKRG NRW und die MeldDÜV NRW sehen vor, dass eine Datenübermittlung von der Meldebehörde an die Zentrale Stelle nur dann unterbleibt, wenn für die betroffene Person im Melderegister eine Auskunftssperre nach Bundesmeldegesetz (§ 51) eingetragen ist. Eine Auskunftssperre wird im Melderegister eingetragen, wenn Tatsachen vorliegen, die die Annahme rechtfertigen, dass der betroffenen oder einer anderen Person durch eine Melderegisterauskunft eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Interessen erwachsen kann.

Fazit

Die Nutzung von Einwohnermeldedaten für den Versand von Einladungen zur Teilnahme am Mammographie-Screening erfolgt auf gesetzlicher Grundlage. Eine Einwilligung der betroffenen Personen in die Nutzung ist nicht erforderlich, ein Widerspruch gegen die Datenübermittlung ist nicht möglich. Die Übermittlung unterbleibt nur in besonderen Fällen bei Bestehen einer entsprechenden melderechtlichen Auskunftssperre.

11.3. Wann darf eine Patient*innenakte gelöscht werden?

Patient*innen wenden sich oft an die LDI NRW, weil sie eine Löschung ihrer Patient*innenakte erreichen wollen. Ärzt*innen und andere Behandelnde sind nach dem Bürgerlichen Gesetzbuch (BGB) allerdings verpflichtet, die Akte für die Dauer von zehn Jahren nach Abschluss der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen (§ 630f Abs. 3 BGB).

Der Fristbeginn knüpft an den Abschluss der Behandlung an. Das gilt auch bei fortdauernden Behandlungen, etwa bei chronischen Erkrankungen. Zudem sehen einige Fachgesetze im medizinischen Bereich deutlich längere Aufbewahrungsfristen vor. So beträgt die gesetzlich vorgesehene Aufbewahrungspflicht nach Röntgenverordnung (§ 28 Abs. 3) oder Transplantationsgesetz (§ 15 Abs. 1) dreißig Jahre. Diese gesetzlichen Aufbewahrungsvorschriften stehen dem Anspruch auf Löschung gemäß Art. 17 Abs. 3 Buchstabe b DS-GVO entgegen.

Auch Personen, die eine Löschung ihrer Daten bei ihrem Gesundheitsamt anstreben, wenden sich an die LDI NRW. Daten von Personen, die vom Gesundheitsamt untersucht oder von dessen Maßnahmen betroffen werden, werden ebenfalls als Patient*innendaten bezeichnet (§ 2 Gesundheitsdatenschutzgesetz NRW). Häufig berufen sich die kommunalen Gesundheitsämter hinsichtlich ihrer Aufbewahrungspflicht auf die zehnjährige Aufbewahrungsfrist aus dem BGB (§ 630f Abs. 3 BGB). Untersuchungen beim Gesundheitsamt bzw. beim Sozialpsychiatrischen Dienst des Gesundheitsamtes sind jedoch öffentlich-rechtlicher Natur und begründen daher kein Behandlungsverhältnis im Sinne des § 630a BGB, für das die zehnjährige Aufbewahrungsfrist gilt.

Sofern keine ausdrückliche gesetzliche Aufbewahrungsvorschrift existiert, dürfen öffentliche Stellen personenbezogene Daten daher nur so lange aufbewahren, wie das für ihre eigene Aufgabenerfüllung erforderlich ist. Bei der Frage der Erforderlichkeit der Aufbewahrung von personenbezogenen Unterlagen ist die Pflicht öffentlicher Stellen zu berücksichtigen, einen Verwaltungsvorgang als Ausfluss des Rechtsstaatsprinzips vollständig und wahrheitsgetreu zu führen. Hierbei ist zu beachten, dass die Verpflichtung zur Aktenführung bei öffentlichen Stellen

- der Funktionsfähigkeit der Verwaltung,
- der rechtsstaatlichen Kontrolle des Verwaltungshandelns auch im Hinblick einer transparenten Verwaltung sowie
- dem Rechtsschutz der jeweiligen Bürger*innen dient.

Die Erforderlichkeit zur Führung von Akten endet damit nicht automatisch nach Abschluss eines Verwaltungsverfahrens, sondern erst dann, wenn feststeht, dass eine weitere Aufbewahrung der Akten für die Dokumentation des Verwaltungshandelns nicht mehr notwendig ist.

Fazit

Der Anspruch auf Löschung einer Patient*innenakte, die auf Grundlage eines Behandlungsvertrages geführt wird, kann regelmäßig nicht vor Ablauf von zehn Jahren nach Abschluss der Behandlung durchgesetzt werden. Grund sind die gesetzlichen Aufbewahrungspflichten. Bereichsspezifisch können auch längere Aufbewahrungsfristen gelten. Patient*innenakten beim Gesundheitsamt unterliegen dagegen anderen Aufbewahrungsfristen. Sofern keine einfach gesetzlichen Vorgaben bestehen, orientiert sich die Aufbewahrungsdauer am Grundsatz der Erforderlichkeit. Die Dauer wird abhängig von ihrer jeweiligen Verwaltungsaufgabe durch die aktenführende Stelle festgelegt.

11.4. Keine Weitergabe der Daten ohne Einwilligung der Patient*innen

Die Abrechnung über privatärztliche Verrechnungsstellen ist gängige Praxis bei medizinischen Leistungserbringern, um sich unerwünschten Verwaltungsaufwand zu ersparen. Sie setzt jedoch voraus, dass die Patient*innen freiwillig in die hiermit verbundene Verarbeitung ihrer personenbezogenen Rechnungsdaten eingewilligt haben.

Ärzt*innen bedienen sich zur Abrechnung ihrer Forderungen vermehrt privatärztlicher Verrechnungsstellen. Diese kaufen in der Regel die Forderungen auf und übernehmen damit das kreditorische Risiko möglicher Forderungsausfälle. Ärzt*innen können sich so auf die Behandlung konzentrieren und lagern die mit der Abrechnung zusammenhängende Verwaltungsarbeit aus.

Wird die Forderung an eine Abrechnungsstelle abgetreten, dann ist die Abrechnungsstelle im Sinne des Datenschutzrechtes verantwortlich. Werden im Zusammenhang mit der Abtretung Gesundheitsdaten an die Abrechnungsstelle weitergeleitet, ist dafür eine Einwilligung der betroffenen Personen – also der Patient*innen – erforderlich. Wesentliches Merkmal einer Einwilligung ist ihre Freiwilligkeit. Freiwilligkeit bedeutet, dass die betroffene Person die Möglichkeit haben muss, sich frei und ohne Zwang gegen die Verarbeitung zu entscheiden.

Die Einwilligung in die Abtretung ärztlicher Forderungen an Abrechnungsstellen ist jedoch keine Voraussetzung für die Behandlung und deren Abrechnung der Patient*innen, weil Ärzt*innen Abrechnungen auch selbst vornehmen können. Trotzdem wird die LDI NRW regelmäßig mit den Erfahrungen Betroffener konfrontiert, dass diejenigen, die medizinische Leistungserbringen erbringen, die Patient*innen zur Einwilligung drängen. Als Argumente werden vorgebracht, die Praxis habe keine Abrechnungsstelle mehr im Haus, oder man müsse unterschreiben, weil eigentlich alle Patient*innen unterschreiben

würden. Werden solche Aussagen tatsächlich getroffen, beeinträchtigen sie die Freiwilligkeit der Einwilligung. Selbst wenn Patient*innen die Einwilligung unterschreiben ist diese unwirksam und die Verarbeitung durch die Abrechnungsstelle muss unterbleiben.

Wenn – wie immer wieder zu hören – von Ärzt*innen die Behandlung verweigert wurde, weil Patient*innen die Einwilligung nicht unterschrieben haben, stellt das einen Verstoß gegen das Koppelungsverbot dar. Die Einwilligung wurde rechtswidrig mit der Verarbeitung verknüpft. Ärzt*innen dürfen die Behandlung nicht wegen der Verweigerung der Einwilligung ablehnen, sondern müssen in solchen Fällen selbst abrechnen.

Fazit

Ärtzt*innen dürfen dafür werben, dass Patient*innen in die Übermittlung ihrer Daten an eine privatärztliche Vermittlungsstelle einwilligen. Dabei sollte jedoch betont werden, dass die Einwilligung freiwillig ist und eine Nichterteilung keine negativen Auswirkungen auf die Behandlung hat. Wird sie nicht erteilt, müssen Ärzt*innen selbst abrechnen.

12. Datenschutz und Arbeit

12.1. EuGH-Entscheidung zu Datenschutz im Arbeitsverhältnis: Auswirkungen in NRW und Forderung nach einem Beschäftigtendatenschutzgesetz

Der Europäische Gerichtshof hat ein wichtiges Urteil zur Verarbeitung von Beschäftigtendaten gesprochen, das Auswirkungen auch für NRW hat (Urteil vom 30. März 2023, Az. C-34/21). Arbeitgeber*innen können zwar auch weiterhin Daten ihrer Beschäftigten verarbeiten, jedoch nun direkt auf Basis der DS-GVO. Besser würde ein von der Bundesregierung angekündigtes Beschäftigtendatenschutzgesetz als spezifische Norm für mehr Klarheit im Einzelnen über die oftmals strittige Verarbeitung von Daten im Beschäftigungsverhältnis sorgen.

Die Entscheidung des EuGH

In einem Vorlagefall aus Hessen hat sich der Gerichtshof mit der Frage befasst, inwiefern § 23 Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) eine spezifische Vorschrift im Sinne des Art. 88 Abs. 1 und 2 DS-GVO ist und als Rechtsgrundlage für die Durchführung von Videokonferenzen von Lehrer*innen herangezogen werden kann. Im Ergebnis stellt der EuGH fest, dass § 23 HDSIG den besonderen Anforderungen des Art. 88 DS-GVO an spezifische Rechtsgrundlagen nicht gerecht wird und somit neben den bestehenden Regelungen der DS-GVO nicht als eigenständige Rechtsgrundlage herangezogen werden kann. Eine nachfolgende Entscheidung des VG Frankfurt, ob die Erhebung von Daten der Lehrer*innen zwecks Durchführung von Videokonferenzen auf eine andere Rechtsgrundlage gestützt werden kann, liegt noch nicht vor.

Die Entscheidung des EuGH ist bundesweit für Arbeitgeber*innen von großer Bedeutung, da das BDSG und auch viele Landesdatenschutzgesetze sehr ähnlich formulierte Regelungen enthalten wie § 23 HDSIG.

Nach Art. 99 Abs. 2 DS-GVO gilt die DS-GVO seit dem 25. Mai 2018 und ist nach Art. 288 Vertrag über die Arbeitsweise der Europäischen Union unmittelbar in jedem Mitgliedsstaat der Union anzuwenden, ohne dass es einer weiteren Umsetzung durch nationales Recht bedarf. Die Mitgliedsstaaten sind jedoch gemäß Art. 88 DS-GVO in bestimmten Grenzen befugt, spezifische nationale Vorschriften zum Beschäftigtendatenschutz zu erlassen. Die Gesetzgeber in Bund und Ländern müssen nun aufgrund der Feststellungen des EuGH prüfen, ob die bestehenden Regelungen zum Beschäftigtendatenschutz in Deutschland den Vorgaben von Art. 88 DS-GVO entsprechen und ob ergänzende Regelungen zum Beschäftigtendatenschutz getroffen werden sollen, die den Anforderungen des Art. 88 DS-GVO gerecht werden.

Auswirkungen in NRW

Für öffentliche Stellen in NRW weist die Regelung des § 18 Abs. 1 Satz 1 DSG NRW große Ähnlichkeiten zur hessischen Regelung zur Verarbeitung von Beschäftigtendaten im öffentlichen Bereich auf. Auch § 18 Abs. 1 Satz 1 DSG NRW dürfte daher keine spezifische Vorschrift im Sinne des Art. 88 Abs. 1 und 2 DS-GVO darstellen und als Rechtsgrundlage für die Verarbeitung von Daten der Beschäftigten öffentlicher Stellen jedenfalls nicht mehr unmittelbar dienen. Die Verarbeitung von Beschäftigtendaten im öffentlichen Bereich kann in der Folge nur auf die allgemeinen Rechtsgrundlagen der DS-GVO gestützt werden.

Als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten in Betracht kommen derzeit Art. 6 Abs. 1 Unterabsatz 1 Buchstabe c (zur Erfüllung einer rechtlichen Verpflichtung) und Art. 6 Abs. 1 Unterabsatz 1 Buchstabe e (im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt), jeweils in Verbindung mit Art. 6 Abs. 3 DS-GVO in Verbindung mit § 18 Abs. 1 Satz 1 DSG NRW. Auch wenn der § 18 Abs. 1 Satz 1 DSG NRW nicht als eine spezifischere Rechtsnorm im Sinne des Art. 88 Abs. 1 DS-GVO anzusehen ist, so kann er doch als Rechtsnorm im Sinne des Art. 6 Abs. 3 DS-GVO betrachtet werden. Bei der Verarbeitung der personenbezogenen Daten von Beschäftigten öffentlicher Stellen ist ein öffentliches Interesse an einem funktionierenden Staatsdienst zu bejahen. Außerdem erfolgt die Tätigkeit der Arbeitnehmer*innen und Beamt*innen im öffentlichen Dienst in Ausübung öffentlicher Gewalt bzw. im öffentlichen Interesse, sodass die zur Ausübung der Tätigkeit erforderlichen Verarbeitungen der Daten dieser Beschäftigten – zumindest mittelbar – ebenfalls zu diesem Zweck stattfinden.

In privatrechtlichen Arbeitsverhältnissen bewertet das Bundesarbeitsgericht die Sachlage ähnlich: § 26 BDSG, die einschlägige Spezialregelung für die Verarbeitung von Beschäftigtendaten im Arbeitsverhältnis, genügt den Vorgaben der Öffnungsklausel in Art. 88 DS-GVO nicht (Beschluss vom 9. Mai 2023, Az. 1 ABR 14/22). Der Wortlaut der Regelung des Abs. 1 entspricht im Wesent-

lichen der im EuGH-Verfahren betrachteten hessischen Regelung, war aber selbst nicht Gegenstand dieses Verfahrens. Allerdings hat das Bundesarbeitsgericht in seinem Beschluss die Anwendung von § 26 BDSG als Rechtsgrundlage nach Art. 6 Abs. 1 Unterabsatz 1 Buchstabe c DS-GVO in Verbindung mit Art. 6 Abs. 3 DS-GVO anerkannt, zumindest für die Verarbeitung personenbezogener Daten von Beschäftigten zur Erfüllung eines sich aus dem Gesetz ergebenden Rechts des Betriebsrats. Im Übrigen dürften als Rechtsgrundlage für die Verarbeitung von Beschäftigtendaten bei nicht-öffentlichen Stellen die Erlaubnistatbestände des Art. 6 Abs. 1 Unterabsatz 1 DS-GVO in Betracht kommen, vor allem die Datenverarbeitung zur Durchführung des Arbeitsvertrags (Buchstabe b), eine rechtliche Verpflichtung zur Verarbeitung von Beschäftigtendaten (Buchstabe c) sowie die Datenverarbeitung aufgrund überwiegender Interessen der Arbeitgeber*innen (Buchstabe f). Hinzu kommt, dass die übrigen Absätze des § 26 BDSG nach bisheriger Einschätzung von der Entscheidung des EuGH unberührt bleiben. Für Einwilligungen nach § 26 Abs. 2 BDSG, die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO (§ 26 Abs. 3 BDSG) und die Verarbeitung personenbezogener Daten, einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten, für Zwecke des Beschäftigungsverhältnisses auf der Grundlage von Kollektivvereinbarungen finden mithin weiterhin die Regelungen des BDSG Anwendung. Bei Personen, die auf der Grundlage eines Arbeitsvertrags beschäftigt werden, können auch öffentliche Stellen die zur Durchführung des Arbeitsvertrags notwendigen Datenverarbeitungen auf Art. 6 Abs. 1 Unterabsatz 1 Buchstabe b DS-GVO stützen.

Beschäftigtendatenschutzgesetz – Blick zurück und nach vorne

Schon vor Inkrafttreten der DS-GVO war der Datenschutz von Beschäftigten sehr rudimentär im BDSG geregelt. Die Einzelheiten ergaben sich vor allem durch die Rechtsprechung der Arbeitsgerichte, die die Datenschutzinteressen der Beschäftigten mit den Interessen der Arbeitgeber*innen jeweils im Einzelfall herausarbeiteten. Folge war eine ausführliche Kasuistik. Um hier für mehr Klarheit zu sorgen besteht schon seit Jahrzehnten die Forderung nach einem Beschäftigtendatenschutzgesetz. Einige Bundesregierungen haben sich in der Vergangenheit dieses Projekt vorgenommen, bislang aber ohne Ergebnis. Auch die aktuelle Bundesregierung möchte ein Beschäftigtendatenschutzgesetz verabschieden. Es wäre gut, wenn es dieses Mal gelingen würde und unter Beachtung der europarechtlichen Vorgaben die Basis für einen ausgewogenen Datenschutz der Beschäftigten gelegt würde. Die zunehmenden technischen Möglichkeiten der Überwachung der Arbeitsprozesse und auch des Einzugs von KI in die Arbeitswelt erfordern eine Auseinandersetzung mit der Frage, wo die Grenzen zu einer nicht mehr tragbaren Überwachung der Beschäftigten liegen. Vor allem hierzu ist ein von Parlamenten gesetzlich normiertes, spezifisches Austarieren der Interessen von Arbeitgeber*innen und

Beschäftigten in einem Beschäftigtendatenschutzgesetz essentiell. Weitere Einzelheiten, die ein Beschäftigtendatenschutzgesetz berücksichtigen sollte, hat die DSK in ihrer Entschließung „Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz!“ vom 11. Mai 2023 dargelegt (Abdruck im Anhang).

Fazit

Auch wenn einige nationale Regelungen für die Verarbeitung von Beschäftigtendaten nicht den Anforderungen des Art. 88 DS-GVO genügen, steht die Datenverarbeitung in diesem Bereich nicht still. Dennoch sollte der Bundesgesetzgeber dringend durch ein Beschäftigtendatenschutzgesetz für mehr Klarheit über die Verarbeitung von Beschäftigtendaten sorgen.

12.2. Private E-Mails und Telefonate am Arbeitsplatz

Für Arbeitgeber*innen gilt nicht mehr das Fernmeldegeheimnis, wenn sie die private Nutzung der betrieblichen E-Mail- oder Internetdienste erlauben oder dulden. Die LDI NRW empfiehlt im Beschäftigtenverhältnis dennoch weiterhin schriftliche Regelungen zur privaten Nutzung von E-Mail und Telefon.

Nach Inkrafttreten des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG) gehen deutsche Aufsichtsbehörden (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, LDI NRW sowie weitere Landesdatenschutzbehörden) davon aus, dass sich eine rechtliche Bewertung geändert hat: Arbeitgeber*innen, die ihren Beschäftigten die private Nutzung von Internet und E-Mail erlauben oder dulden, unterliegen nicht mehr dem Telekommunikationsrecht. Deshalb haben sie gegenüber ihren Beschäftigten auch nicht das Fernmeldegeheimnis zu garantieren.

Zur Wahrung des Fernmeldegeheimnisses verpflichtet sind nach dem TTDSG vor allem Anbieter von öffentlich zugänglichen und von geschäftsmäßig angebotenen Telekommunikationsdiensten sowie Betreiber von öffentlichen Telekommunikationsnetzen und solche von geschäftsmäßig ausgerichteten Telekommunikationsanlagen.

Bei Arbeitgeber*innen, die die private Nutzung erlauben oder dulden, fehlt es in der Regel am Rechtsbindungswillen: Arbeitgeber*innen treten gegenüber ihren Beschäftigten nicht als geschäftsmäßige Telekommunikationsdienstleister auf. Deshalb wollen sie auch nicht, dass die für diese Dienstleister geltenden Rechtsnormen auf sie angewendet werden.

In der Vergangenheit galt, dass Arbeitgeber*innen nur auf die Protokolldaten oder E-Mails der Beschäftigten zugreifen konnten, wenn dafür deren Einwilligung vorlag. Mit dem TTDSG finden statt der spezifischen telekommunikationsrechtlichen Regeln nun die Vorschriften der DS-GVO Anwendung. Die DS-GVO sichert ein ähnlich hohes Schutzniveau für die personenbezogenen Daten der Beschäftigten. Auch nach der DS-GVO bedarf es einer Rechtsgrundlage für den Zugriff der Arbeitgeber*innen auf die personenbezogenen Daten der Beschäftigten. Die LDI NRW empfiehlt den Arbeitgeber*innen daher wie bislang, über die betriebliche und/oder private Nutzung des Internets und des betrieblichen E-Mail-Accounts eine schriftliche Regelung zu treffen. Darin sollen die Fragen des Zugriffs, der Protokollierung, der Auswertung und der Durchführung von Kontrollen eindeutig geklärt werden. Zudem sind die Beschäftigten auch künftig über mögliche Überwachungsmaßnahmen und Sanktionen zu informieren.

Fazit

Die Rechtslage hat sich geändert. Arbeitgeber*innen sollten aber weiterhin regeln, ob Internet und E-Mail privat genutzt werden dürfen und welche Rahmenbedingungen dafür gelten.

12.3. Kontaktdaten von Beschäftigten des öffentlichen Dienstes

Behörden und sonstige öffentliche Stellen dürfen Kontaktdaten ihrer Beschäftigten nicht ohne Rechtsgrundlage weitergeben. Aus Beschwerden wissen wir jedoch, dass private Handynummern und E-Mail-Adressen an Dritte teils ohne vorherige Absprache weitergegeben wurden.

Personenbezogene Daten von Beschäftigten dürfen allerdings nur verarbeitet werden, um

- ein Beschäftigungsverhältnis einzugehen,
- es durchzuführen,
- es zu beenden oder
- wenn die Durchführung organisatorischer, personeller und sozialer Maßnahmen (insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes) es erforderlich machen.

Zudem dürfen sie verarbeitet werden, wenn eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht – oder Beschäftigte eingewilligt haben (§ 18 Abs. 1 Satz 1 DSG NRW).

Die Prüfung der Beschwerden, die wir erhalten haben, ergab regelmäßig, dass eine Weitergabe privater Kontaktdaten der Beschäftigten weder erforderlich noch durch eine Einwilligung gerechtfertigt war. Häufig wird die Weitergabe der privaten Kontaktdaten damit begründet, dass Arbeitsabläufe unkomplizierter organisiert werden könnten, wenn beispielsweise ein schneller Informationsaustausch über private Handys erfolge. Das etwas nützlich erscheint, rechtfertigt die Übermittlung von Kontaktdaten, wie eine Handynummer, an alle Arbeitsteammitglieder aber nicht.

Eine Behörde hat nach Hinweis durch die LDI NRW Diensthandys eingeführt und von der weiteren Nutzung privater Handynummern abgesehen.

Gar nicht in Ordnung ist, wenn Verantwortliche private Kontaktdaten ihrer Beschäftigten für private Zwecke herausgeben. Aber auch das kommt vor. So hatte etwa eine Schulleitung die private E-Mail-Adresse einer Beschäftigten ohne deren Einwilligung an ein Familienmitglied weitergegeben, um ihm eine private Kontaktaufnahme mit der Beschäftigten zu ermöglichen. Wenn Daten – wie in diesem Fall – gänzlich ohne Zusammenhang zu den dienstlichen Aufgaben verarbeitet werden, ist dies ein Kompetenzüberschreitung. Gegen die Person, die ihre Kompetenzen bei der Datenverarbeitung überschreitet, können wir ein Bußgeld verhängen.

Fazit

Die Organisation oder Vereinfachung von Arbeitsabläufen rechtfertigt keine Weitergabe privater Kontaktdaten von Beschäftigten an Dritte. Werden die Daten dennoch weitergegeben, droht ggf. ein Bußgeld.

12.4. Beim Elternnachweis für die Pflegeversicherung gilt bis 2025 ein vereinfachtes Verfahren

Viele Beschäftigte bekamen im vergangenen Jahr Post von ihren Arbeitgeber*innen: Darin wurden sie aufgefordert, Daten mitzuteilen, die über ihre Elternschaft Auskunft geben. Die LDI NRW erreichten dazu Beratungsanfragen von Beschäftigten und Arbeitgeber*innen gleichermaßen.

Hintergrund: Arbeitgeber*innen mussten kurzfristig neue Regelungen der gesetzlichen Pflegeversicherung zum 1. Juli 2023 für ihre aktiven Beschäftigten umsetzen. Sie sind dazu verpflichtet, die Elterneigenschaft, die Anzahl der Kinder und deren Alter in geeigneter Form gegenüber den beitragsabführenden Stellen (Zahlstelle/Pflegekasse) nachzuweisen, wenn diese Angaben nicht bereits aus anderen Gründen bekannt sind (vgl. § 55 Abs. 3 a Sozialgesetzbuch Elftes Buch – SGB XI).

Laut SGB XI gibt der Spitzenverband „Bund der Pflegekassen“ Empfehlungen darüber, welche Nachweise geeignet sind (§ 55 Abs. 3 a Satz 2 SGB XI).

Im SGB XI sind eine Vielzahl an Dokumenten aufgeführt, die – je nach Art der Elternschaft – als Nachweis in Betracht kommen. Für leibliche Eltern und Adoptiveltern sind beispielsweise Geburts-, Abstammungs- oder Adoptionsurkunden geeignet. Auch der Abruf der elektronischen Lohnsteuerabzugsmerkmale aus der ELStAM-Datenbank wird in den Empfehlungen genannt.

Damit müssen Arbeitgeber*innen zusätzlich zu den bereits vorhandenen personenbezogenen Daten ihrer Beschäftigten weitere personenbezogene Daten von Kindern bzw. Daten zu sehr persönlichen Umständen erheben, speichern und DS-GVO-konform verarbeiten. Hierbei handelt es sich um eine rechtliche Verpflichtung, der Arbeitgeber*innen gemäß § 55 Abs. 3 a SGB XI unterliegen. Datenschutzrechtlich können Arbeitgeber*innen die zur Erfüllung dieser Verpflichtung erforderliche Verarbeitung auf Art. 6 Abs. 1 Unterabsatz 1 Buchstabe c DS-GVO stützen.

Arbeitgeber*innen als beitragsabführende Stellen stehen somit vor der Herausforderung, den Nachweis der Elterneigenschaft, Anzahl der Kinder usw. datenschutzkonform zu erheben und zu führen.

Derzeit wird unter Federführung des Bundesministeriums für Gesundheit an einem digitalen Verwaltungsverfahren zur Erhebung und zum Nachweis der Kinderzahl gearbeitet. Die Arbeit soll bis zum 31. März 2025 abgeschlossen sein.

Für den Zeitraum vom 1. Juli 2023 bis zum 30. Juni 2025 sieht das Gesetz ein sog. „vereinfachtes Nachweisverfahren“ vor. Danach gilt der erforderliche Nachweis in diesem Zeitraum auch dann als erbracht, wenn die beschäftigten Eltern auf Anforderung den Arbeitgeber*innen die erforderlichen Angaben zu den berücksichtigungsfähigen Kindern mitteilen (vgl. § 55 Abs. 3d Satz 2 SGB XI). Die bloße Mitteilung der Angaben ist ausreichend und kann ohne weitere Prüfung verwendet werden. Die Vorlage konkreter Nachweise (zum Beispiel der Geburtsurkunde) ist nicht erforderlich. Die Arbeitgeber*innen haben somit die Möglichkeit, die erforderlichen Daten zum Beispiel durch ein Formular abzufragen, das die Beschäftigten ausfüllen. Dabei muss sich der Umfang der Datenerhebung jedoch auf die erforderlichen Informationen beschränken (Grundsatz der Datenminimierung). Im Ergebnis sollte sich die Datenerhebung daher auf die Namen und die Geburtsdaten der Kinder beschränken.

Außerhalb des vereinfachten Nachweisverfahrens dürfen Arbeitgeber*innen die Nachweise auch nach Empfehlungen des Bundes der Pflegekassen führen. Dazu können sie ihre Beschäftigten auffordern, analoge Nachweise (etwa eine

Kopie der Geburtsurkunde) vorzulegen. Aus datenschutzrechtlicher Sicht ist zu beachten, dass von dem Bund der Pflegekassen empfohlene Dokumente zum Teil (sensible) personenbezogene Daten enthalten, die für den Nachweis der Elterneigenschaft und der Anzahl der Kinder nicht erforderlich sind. So geht beispielsweise aus den Geburtsurkunden die Religionszugehörigkeit der Eltern hervor. Die datensparsamere Möglichkeit, die Unterlagen den Arbeitgeber*innen im Original vorzulegen und einen Bestätigungsvermerk anzufertigen, wird vom Spitzenverband in seinen Empfehlungen allerdings als nicht ausreichend angesehen.

Bei der Nachweisführung ist die DS-GVO zu beachten und deswegen sind für den Nachweis nicht benötigte Informationen auch nicht zu übermitteln. Arbeitgeber*innen sollten ihre Beschäftigten daher auf die Möglichkeit hinweisen, die nicht erforderlichen Angaben vor der Übersendung der Dokumente zu schwärzen. Erhalten Arbeitgeber*innen Dokumente mit nicht erforderlichen Angaben, sollten sie diese Angaben selbst schwärzen.

Bei der Abfrage und Einholung der entsprechenden Nachweise müssen Arbeitgeber*innen auch die weiteren datenschutzrechtlichen Pflichten beachten. Hierzu gehören zunächst die Informationspflichten aus Art. 13 und 14 DS-GVO. Wenn später der Zweck der Datenverarbeitung entfallen ist, müssen sie die personenbezogenen Daten löschen (Art. 17 Abs. 1 Buchstabe a DS-GVO).

Beschäftigte sollten Dokumente ihren Arbeitgeber*innen am besten persönlich vorlegen. Ist dies nicht möglich, sollten die Nachweise per Post oder als verschlüsselter E-Mail-Anhang versendet werden, um unbefugte Zugriffe zu verhindern.

Für die Übergangszeit, bis das digitale Verfahren vorhanden ist, können Arbeitgeber*innen das vereinfachte Nachweisverfahren (Meldung durch Selbsterklärung) oder die analoge Meldemöglichkeit (Übermittlung eines Papiers zum Nachweis) wählen. Die Nutzung des vereinfachten Nachweisverfahrens ist allerdings nur bis zum 30. Juni 2025 möglich. Danach müssen die Arbeitgeber*innen die Informationen entweder nach den Empfehlungen des Spitzenverbandes erheben und übermitteln oder das dann zur Verfügung stehende digitale Verfahren nutzen.

Fazit

Das bis zum Ende der Übergangsfrist am 30. Juni 2025 mögliche Verfahren ist datenschutzfreundlich und Arbeitgeber*innen zu empfehlen. Das in Bearbeitung befindliche und zukünftig anzuwendende digitale Verfahren wird hoffentlich dafür Sorge tragen, dass nicht benötigte Daten, die sich in Nachweisdokumenten befinden, nicht erhoben werden.

13. Zertifizierungen

13.1. Zertifizierungskriterien: EDSA-Dokument beschleunigt Genehmigungsverfahren

Die DS-GVO fördert Zertifizierungen von Datenverarbeitungsvorgängen. Durch Zertifizierungen sollen diejenigen, die Daten verarbeiten, die Sicherheit erhalten, dass sie dabei den Datenschutz einhalten. Der Aufbau von Zertifizierungsverfahren seit dem Inkrafttreten der DS-GVO im Jahr 2018 war anspruchsvoll und nimmt erst seit zwei Jahren deutlich an Fahrt auf. Ein Beschluss des Europäischen Datenschutzausschusses (EDSA) gibt jetzt noch etwas Rückenwind, um Zertifizierungen den Weg zu bereiten.

Im Februar 2023 beschloss der EDSA ein „Dokument über das Verfahren zur Verabschiedung seiner Stellungnahmen zu nationalen Zertifizierungskriterien und zu den europäischen Datenschutzsiegeln“. Der EDSA legt in diesem Dokument seine Verfahren sowohl für national gültige Zertifikate als auch für europäische Datenschutzsiegel fest, die zur europaweiten Anerkennung führen. Zertifikate dokumentieren, dass sich zum Beispiel Unternehmen datenschutzgerecht verhalten. Solche Zertifikate werden von akkreditierten Zertifizierungsstellen nach bestimmten Kriterien vergeben, die von Datenschutzbehörden genehmigt wurden. Das Dokument soll für Klarheit und Transparenz bei allen Beteiligten sorgen, wie die Verfahren ablaufen, um Zertifizierung marktfähig zu machen.

Der EDSA prüft die Kriterien in zwei Phasen: In der ersten, informellen Phase prüfen zunächst drei Aufsichtsbehörden und beziehen anschließend alle Aufsichtsbehörden im EDSA mit ein. Auch die Fachuntergruppen des EDSA können bei Bedarf mit einbezogen werden. Antragstellende erhalten detaillierte Rückmeldungen, sie können auf Kritik und Verbesserungsvorschläge reagieren und ihre Zertifizierungskriterien noch anpassen. So sollen die nötige Abstimmung zwischen den Aufsichtsbehörden und Verbesserungen an

den Zertifizierungsverfahren erzielt werden. Wie die zweite, formelle Phase auszusehen hat (wenn es zum Beispiel um konkrete Fristen für Stellungnahmen geht), ist in der DS-GVO geregelt. Wenn alles in Ordnung ist, steht am Ende die Genehmigung. Geht es um nationale Zertifizierungskriterien, erteilt die zuständige Aufsichtsbehörde die Genehmigung und berücksichtigt dabei die Stellungnahme des EDSA. Wenn es um ein europäisches Siegel geht, entscheidet der EDSA über die Genehmigung.

Der EDSA hat das Dokument in einer Fachuntergruppe erstellt (Compliance, E-Government & Health Expert Subgroup). Die LDI NRW stellt in dieser Fachuntergruppe die Ländervertreterin und hat an der Erstellung des Dokuments mitgewirkt. Dabei konnte sie ihre Erfahrungen aus noch laufenden und bereits abgeschlossenen Verfahren einbringen.

Fazit

Das Dokument des EDSA ist ein wichtiger Schritt, um ein einheitliches Qualitätsniveau von Zertifizierungsverfahren sicherzustellen. Weitere Vereinheitlichungen und Verschlankungen der Prozesse sind geplant oder laufen bereits. Unternehmen, die den Datenschutz nachweislich einhalten, genießen Vertrauen und haben damit einen Wettbewerbsvorteil. Das lässt die Nachfrage nach Zertifizierungen und den Bedarf an Zertifizierungsstellen steigen. Der EDSA ist mit dem Dokument nun noch besser auf die gemeinsame Bewertung von Zertifizierungsverfahren vorbereitet. Genehmigungsverfahren können zügiger durchgeführt werden.

13.2. Erste Zertifizierungsstelle in Deutschland akkreditiert

Was lange währt, wird endlich gut! Seit Dezember 2023 ist mit der EuroPriSe Cert GmbH die erste deutsche Zertifizierungsstelle akkreditiert. 2024 können Auftragsverarbeiter mit Sitz in Deutschland ihre Datenverarbeitungsprozesse hier nach der DS-GVO zertifizieren lassen. Damit hat die LDI NRW als erste Datenschutzbehörde in Deutschland ein Verfahren für die Zulassung einer Zertifizierungsstelle abgeschlossen.

Zertifikate, die von einer solchen Stelle vergeben werden, dokumentieren, dass bei einer Datenverarbeitung die Datenschutzanforderungen eingehalten werden. Private Zertifizierungsstellen müssen dazu staatlich genehmigte Kriterien verwenden und selbst staatlich akkreditiert, also geprüft und zugelassen sein.

Bereits Ende 2022 hat die LDI NRW die Zertifizierungskriterien für Auftragsverarbeitung genehmigt, die die Grundlage für die Tätigkeit der Zertifizierungsstelle sind. Daran schloss sich das Akkreditierungsverfahren an, das die Deutsche Akkreditierungsstelle GmbH (DAkkS) gemeinsam mit der LDI NRW durchgeführt hat. Das Akkreditierungsverfahren erfolgte in mehreren Phasen. DAkkS und Aufsichtsbehörde bildeten ein Begutachtungsteam und prüften die eingereichten Dokumente und die Zertifizierungsstelle vor Ort. Grundsätzlich entscheidend für die Akkreditierung war das Votum des Akkreditierungsausschusses, der zu einem Drittel mit Mitgliedern der DAkkS und zu zwei Dritteln mit Mitgliedern der LDI NRW besetzt war. Eine positive Entscheidung muss einstimmig erfolgen. Im Anschluss daran hat die DAkkS den Akkreditierungsbescheid erteilt, die Akkreditierungsurkunde ausgestellt und die Stelle im DAkkS-Register („Verzeichnis der akkreditierten Stellen“) gelistet. Mit der Befugniserteilung durch die LDI NRW wurde das Verfahren abgeschlossen und konnte die Zertifizierungsstelle ihre Arbeit aufnehmen.

Die Akkreditierung wurde zeitlich befristet für fünf Jahre erteilt. Eine Re-Akkreditierung ist möglich. Die Arbeit der Zertifizierungsstelle wird zu Anfang und in regelmäßigen Abständen durch die DAkkS und die LDI NRW überwacht. Werden dabei Abweichungen festgestellt, kann dies zur Einschränkung, Aussetzung oder Aufhebung der Akkreditierung führen – mit Auswirkungen auf bereits erteilte Zertifizierungen.

Interessierte Unternehmen, die Zertifikate erhalten möchten, sollten vor der Beauftragung einer Zertifizierungsstelle einen Blick in das DAkkS-Verzeichnis werfen, abrufbar unter www.dakks.de/de/akkreditierte-stellen-suche.html. So können sie sicher sein, dass sie eine ordnungsgemäß akkreditierte Stelle beauftragen.

Zertifikate, die jetzt vergeben werden, können sich auszahlen: Unternehmen finden Kundschaft für die zertifizierte Dienstleistung. Kundschaft auf der Suche nach datenschutzgerechten Dienstleistungen, findet leichter die passenden Unternehmen. Datenschutzbeauftragte, die die Einhaltung des Datenschutzes bei Auftragnehmer prüfen, können die Zertifikate dabei heranziehen. Datenschutzaufsichtsbehörden werden entlastet. Und nicht zuletzt: Alle, deren Daten in zertifizierten Verfahren verarbeitet werden, können sich darauf verlassen, dass dabei die Datenschutzregeln eingehalten werden.

Fazit

Die LDI NRW hat maßgeblichen Anteil daran, dass ein wichtiges Instrument der DS-GVO für einen guten Datenschutz erstmalig in Deutschland Marktreife erlangt. Interessierte Auftragsverarbeiter können jetzt Zertifizierungen nutzen. Verantwortliche können später zertifizierte Auftragsverarbeiter beauftragen.

14. Wirtschaft

14.1. Datenübermittlung in die USA: Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework

Eine Datenübermittlung in Drittländer ist unter anderem dann zulässig, wenn die EU-Kommission beschlossen hat, dass dort ein angemessenes Datenschutzniveau besteht. Im Juli 2023 hat sie den Angemessenheitsbeschluss für das EU-U.S. Data Privacy Framework angenommen.

Seitdem kann der Beschluss für die Übermittlung personenbezogener Daten an bestimmte Unternehmen in den USA genutzt werden. Das sind solche Unternehmen, die sich selbst dazu verpflichtet haben, bestimmte Datenschutzregeln einzuhalten, und die insoweit der Kontrolle durch Behörden der USA unterliegen. Der Angemessenheitsbeschluss folgt früheren Angemessenheitsbeschlüssen für die USA nach, die der Europäische Gerichtshof für nichtig erklärt hatte (EU-US Privacy Shield und Safe Harbor).

Die DSK hat Anwendungshinweise zum Angemessenheitsbeschluss zum EU-U.S. Data Privacy Framework veröffentlicht, abrufbar unter www.datenschutzkonferenz-online.de. Sie enthalten einerseits Informationen für die Datenexporteure, also die Verantwortlichen und Auftragsverarbeiter, die Daten in die USA übermitteln. Andererseits erfahren betroffene Personen, welche Rechtsschutz- und Beschwerdemöglichkeiten sie haben. Die LDI NRW hat an den Anwendungshinweisen der DSK mitgearbeitet.

Zu beachten ist: Es besteht nicht generell ein angemessenes Datenschutzniveau für Übermittlungen an Organisationen in den USA. Datenexporteure aus der EU müssen deshalb zunächst vorab prüfen, ob die Organisation, an die übermittelt werden soll, unter dem EU-U.S. Data Privacy Framework zertifiziert ist. Erst dann sind keine weiteren Übermittlungsinstrumente oder zusätzlichen Maßnahmen zur Absicherung des Datenexports erforderlich.

Das U.S. Department of Commerce veröffentlicht eine Liste mit den zertifizierten Organisationen, mit der die Voraussetzungen geprüft werden können. Der Europäische Datenschutzausschuss hatte eine kritische Stellungnahme zum Entwurf des Angemessenheitsbeschlusses abgegeben.

Ob der Angemessenheitsbeschluss dauerhaft Bestand haben wird, ist offen. Es ist mit einer gerichtlichen Kontrolle durch den Europäischen Gerichtshof zu rechnen.

Fazit

Der Angemessenheitsbeschluss schafft für bestimmte Datenübermittlungen in die USA vorerst Rechtssicherheit. Vor einer Übermittlung ist im Einzelfall zu prüfen, ob die Daten empfangende Organisation gemäß den Regelungen des Angemessenheitsbeschlusses zertifiziert ist.

14.2. Hinweisgeberschutzgesetz: Bei internen Meldestellen müssen Datenschutz-Folgen geprüft werden

Seit 2023 gibt es das Hinweisgeberschutzgesetz zum Schutz hinweisgebender Personen (Whistleblower). Im Gesetz ist eine Pflicht zur Einrichtung interner Meldestellen für Arbeitgeber*innen mit jeweils in der Regel mindestens 50 Beschäftigten vorgesehen. Wer eine interne Meldestelle braucht, benötigt auch eine*n Datenschutzbeauftragte*n.

Meldestellen im Sinne des Hinweisgeberschutzgesetzes (HinSchG) verarbeiten Daten, deren Bekanntwerden ein besonders hohes Risiko für die Rechte und Freiheiten von Beschäftigten und sonstigen Personen erzeugen würde. Deswegen ist dort der Schutz der Daten bei den Meldestellen besonders wichtig. Diese erhalten von den meldenden Personen Informationen über Regelverstöße. Daraus darf für die meldenden Personen kein Nachteil entstehen, insbesondere wenn sie dort arbeiten, wo gegen die Regeln verstoßen wurde; Repressalien sind vom Gesetz ausdrücklich verboten (§ 36 Abs. 1 HinSchG). Die interne Meldestelle hat die datenschutzrechtlichen Bestimmungen bei der Verarbeitung personenbezogener Daten einzuhalten.

Wer eine interne Meldestelle mit eigenen Beschäftigten einrichtet, bleibt für deren Datenverarbeitung Verantwortlicher. Er muss mit den Beschäftigten, die die Aufgabe der Meldestelle wahrnehmen, konkrete Verfahren zum Umgang mit den anfallenden Daten und zum Schutz dieser Daten treffen. Dabei ist die unabhängige Aufgabenwahrnehmung der Stelle zu achten und zugleich der Schutz der hinweisgebenden Personen – auch gegenüber dem Verantwortlichen selbst – sicherzustellen.

Mit den Aufgaben der internen Meldestelle kann auch ein Dritter betraut werden (§ 14 Abs. 1 HinSchG). Insbesondere die Beauftragung externer Anwält*innen oder sonstiger externer Berater*innen kann in Betracht kommen. Wird ein Dritter mit den Aufgaben betraut, ist dieser Verantwortlicher, da interne Meldestellen selbstständig und unabhängig über den Umgang mit den erhaltenen Informationen einschließlich der dazu gehörenden personenbezogenen Daten entscheiden. Eine gemeinsame Verantwortlichkeit (Art. 26 DS-GVO) ist dabei nicht anzunehmen. Die durch Externe wahrgenommene interne Meldestelle ist kein Auftragsverarbeiter. Dritte können aber auch nur mit einzelnen Hilfstätigkeiten zum Betrieb der Meldestelle beauftragt werden, beispielsweise um die dort eingesetzte IT zu betreuen. In diesen Fällen sind die Vorgaben für Auftragsverarbeitungen zu beachten (Art. 28 DS-GVO). Auftraggeber sind die Verantwortlichen, die die interne Meldestelle betreiben, weil sie selbst dazu verpflichtet sind oder weil sie die Aufgabe übernommen haben.

Vor der Einrichtung einer internen Meldestelle – und damit vor Eröffnung eines Meldekanals – ist eine Datenschutz-Folgenabschätzung durchzuführen, weil ein besonders hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Art. 35 DS-GVO). Dies gilt auch bei einer externen Beauftragung. Die Verarbeitung der Daten von Hinweisgebenden ist besonders risikoreich, da teilweise schwerwiegende Vorwürfe mitgeteilt werden, die dazu führen können, dass Hinweisgebende Repressalien oder Sanktionen ausgesetzt werden.

Aus der Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung vor Einrichtung der internen Meldestelle folgt, dass ein*e Datenschutzbeauftragte*r zu benennen ist, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen (§ 38 Abs. 1 Satz 2 BDSG).

Fazit

Es ist zulässig, einen Dritten mit der Einrichtung und dem Betrieb der Meldestelle zu betrauen. Wird eine interne Meldestelle nach dem HinSchG eingerichtet, so ist zwingend eine Datenschutz-Folgenabschätzung durchzuführen. Wer eine interne Meldestelle braucht, muss auch eine*n Datenschutzbeauftragte*n benennen.

14.3. Empfehlung an Bundesregierung: Scoring-Regelung verbessern

Bonitäts-Scoring steht regelmäßig in der Kritik. Wie und nach welchen Kriterien ein Scoring für Kreditnehmer*innen zustande kommt, ist oft intransparent. Die DSK hat der Bundesregierung deswegen Maßnahmen empfohlen, um die Transparenz und damit den Verbraucher- und Datenschutz zu verbessern. Zusätzliche Anforderungen an den Einsatz von Scores ergeben sich aus der jüngsten Rechtsprechung des EuGH.

Beim Scoring wird ein Wahrscheinlichkeitswert gebildet, der eine Vorhersage über das Verhalten einer Person ausdrückt. Der Wert wird für die Entscheidung über ein Vertragsverhältnis mit dieser Person verwendet – also beispielsweise darüber, ob die Person einen Kredit erhält und zu welchen Bedingungen. Unter Bonitätsscoring ist das Scoring nicht nur durch die Kreditwirtschaft zu verstehen, sondern auch durch Verantwortliche weiterer Branchen, die damit Risiken absichern, die durch ausfallende Zahlungen entstehen können. Dies ist beispielsweise bei Warenbestellungen auf Rechnung oder bei Telekommunikationsverträgen mit einem vertraglich bereitgestellten Smartphone eine verbreitete Praxis.

Anlass für die Empfehlungen der DSK war der Koalitionsvertrag der Regierungsparteien im Bund. Daraus ergibt sich, dass die Bundesregierung prüfen will, wie die Transparenz beim Kreditscoring zugunsten der Betroffenen erhöht werden kann. Sie will dazu Handlungsempfehlungen umsetzen. Die von der DSK formulierten „Vorschläge für Handlungsempfehlungen an die Bundesregierung zur Verbesserung des Datenschutzes bei Scoringverfahren“ vom Mai 2023, abrufbar unter www.datenschutzkonferenz-online.de, könnten bereits im aktuellen Gesetzgebungsverfahren zur Novellierung des BDSG berücksichtigt werden. Die Empfehlungen wurden im DSK-Arbeitskreis Kreditwirtschaft unter der Leitung der LDI NRW mit Beteiligung des DSK-Arbeitskreises Auskunfteien und Inkasso erarbeitet.

Die Handlungsempfehlungen zielen auf eine bessere Transparenz hinsichtlich des Einsatzes und der Aussagekraft von Scorewerten unter anderem durch eine verbesserte Unterrichtung, Information und Erteilung von Auskünften über den Einsatz von Scoringverfahren sowie über die Aussagekraft und Prognosegenauigkeit der verwendeten Scores und darüber, in welchem Umfang ein Scorewert gegebenenfalls Einfluss auf eine nicht ausschließlich automatisierte Entscheidungsfindung hat,

- durch unabhängige Zertifizierung des Scoreverfahrens,
- durch Speicherung übermittelter Scorewerte, um Auskünfte zu ermöglichen, sowie
- durch Daten-Cockpits und Score-Simulatoren.
- Weiter empfiehlt die Konferenz,
- für einzelne Kriterien, die nur eine geringe Bedeutung für die Score-Berechnung haben, eine Negativliste zu erstellen oder die Verwendung solcher Kriterien zu verbieten,
- Verfahren vorzusehen, die sicherstellen, dass nur richtige und aktuelle Daten für das Scoring verwendet werden.

Darüber hinaus schafft die DSK mit dem Papier Klarheit in Bezug auf die Transparenzanforderungen, die die für das Scoring Verantwortlichen einhalten müssen.

Das Scoring wird auch kritisiert, weil es vielfach ein typischer Anwendungsfall eines automatisierten Bewertungsverfahrens nach Art. 22 DS-GVO ist. Die DS-GVO verbietet automatisierte Entscheidungen im Einzelfall. Zur Reichweite dieses Verbots hat der EuGH entschieden (Urteil vom 7. Dezember 2023, Az. C-634/21 (Schufa/Scoring) und ausgeführt, dass das Scoring eine von der DS-GVO grundsätzlich verbotene automatisierte Entscheidung im Einzelfall ist, falls die Kundschaft von Wirtschaftsauskunfteien (zum Beispiel Banken, Online-Händler*innen oder Telekommunikationsunternehmen) ihm eine „maßgebliche“ Rolle im Rahmen der Kreditgewährung beimisst.

Zwar kann der nationale Gesetzgeber unter bestimmten Umständen, die sich aus Art. 22 DS-GVO ergeben, eine automatisierte Einzelentscheidung erlauben. Die bisher für Scoringverfahren wesentliche Vorschrift, nämlich § 31 BDSG, genügt diesen Anforderungen allerdings nicht. In der Praxis können Scoringverfahren in Folge der Entscheidung des EuGH daher aktuell nur zum Einsatz kommen, wenn sie keinen maßgeblichen Einfluss auf eine für Betroffene nachteilige Entscheidung haben. Was dies in der Praxis bedeutet, prüfen die Datenschutzaufsichtsbehörden derzeit.

Fazit

Eine rechtmäßige Datenverarbeitung erfordert Transparenz, auch und gerade bei Scoringverfahren. Hier gibt es im Interesse der Rechtssicherheit einen hohen Verbesserungsbedarf.

14.4. Wenn der digitale Euro kommt...

Digitalisierung und neue Technologien prägen zunehmend den Handel und die europäische Wirtschaft. Banknoten und Münzen werden immer seltener als Zahlungsmittel eingesetzt. Online-Einkäufe nehmen zu, aber auch im stationären Handel kommen private digitale Zahlungsmittel vermehrt zum Einsatz – meist von US-Anbietern wie Visa, Mastercard, Apple und PayPal. Die LDI NRW vertritt die Datenschutzaufsichtsbehörden der Bundesländer in der Financial Matters Subroup des Europäischen Datenschutzausschusses und setzt sich dort dafür ein, dass anonyme Zahlungen weiter möglich bleiben werden.

Zentralbanken arbeiten schon seit einigen Jahren an digitalen Varianten ihrer jeweiligen Währung, so auch die Europäische Zentralbank (EZB). Nach einer grundlegenden Analyse hat der EZB-Rat im Oktober 2023 entschieden, in die zweijährige Vorbereitungsphase für die Einführung des Digitalen Euros einzutreten. Dafür muss vorab über den rechtlichen Rahmen entschieden werden. Einen Gesetzentwurf hat die EU-Kommission bereits vorgelegt (COM/2023/369 final). Dieser ist für den Schutz personenbezogener Daten von besonderer Bedeutung. Daher hat sie den Europäischen Datenschutzausschuss (EDSA) konsultiert. Dieser hat zusammen mit dem Europäischen Datenschutzbeauftragten (EDSB) eine gemeinsame Stellungnahme veröffentlicht, abrufbar unter www.edps.europa.eu. Die LDI NRW hat als Vertretung der Bundesländer in der zuständigen Arbeitsgruppe des EDSA an der Vorbereitung der Stellungnahme mitgewirkt.

Der Gesetzentwurf zum Digitalen Euro will das Zentralbankgeld mit dem Status eines gesetzlichen Zahlungsmittels der breiten Öffentlichkeit zur Verfügung stellen. Es soll nach der Zielsetzung des Entwurfs ein modernes und kosteneffizientes Zahlungsmittel sein, das ein hohes Maß an Privatsphäre bei digitalen Zahlungen gewährleistet, die Finanzstabilität aufrechterhält und die Zugänglichkeit und finanzielle Inklusion fördert. Die EU-Kommission betont, dass der Digitale Euro das Bargeld nicht ersetzen, sondern ergänzen wird.

Dies wird vom EDSA und dem EDSB begrüßt. Beide fordern die europäischen Gesetzgebungsorgane zudem auf, weiterhin dafür Sorge zu tragen, dass der Digitale Euro kein „programmierbares Geld" sein wird. Ansonsten ließe sich ableiten, wofür die Nutzer*innen des Digitalen Euros ihr Geld einsetzen. EDSA und EDSB weisen in ihrer gemeinsamen Stellungnahme auf eine Reihe von Bedenken hin:

- So verlangen sie ein hohes Maß an Schutz der Privatsphäre. Für Online-Zahlungsvorgänge fordern sie eine „Datenschutzschwelle", bis zu der keine Rückverfolgung der Transaktionen möglich ist. Auf diese Weise würde das Vertrauen der Bürger*innen in den Digitalen Euro gestärkt und dem Risiko von Geldwäsche oder Terrorismusfinanzierung angemessen Rechnung getragen. Keine Rückverfolgung bedeutet in diesem Fall, dass Transaktionen mit geringem Wert keiner Kontrolle unterliegen und auch nicht von Zahlungsdienstleistern zwischen EZB und Bürger*innen erfasst werden.

- EDSA und EDSB bemängeln, dass der Gesetzentwurf hinsichtlich der zu verarbeitenden Daten und der Verantwortlichkeit für die jeweiligen Verarbeitungsschritte noch unklar ist. So sind die Daten bislang nicht hinreichend konkret bestimmt, die die verschiedenen Dienstleister für Zahlungstransaktionen für den Digitalen Euro verarbeiten sollen. Auch die Verantwortlichkeiten zwischen der EZB, den nationalen Zentralbanken und den beteiligten Zahlungsdienstleistern verbleiben noch im Vagen. Mehr Klarheit bedarf es außerdem bezüglich der personenbezogenen Daten, die die EZB für die Kontrolle der Zahlungsdienstleister benötigt.

- In Bezug auf die Infrastruktur, die die EZB bereitstellen und verwalten soll, fordern EDSA und EDSB, dass der Gesetzentwurf eine Pseudonymisierung aller Transaktionsdaten gegenüber der EZB und den nationalen Zentralbanken vorsieht.

- Die Verhältnismäßigkeit der Bestimmungen zu den Betrugserkennungs- und Präventionsmechanismen ist nach Auffassung von EDSA und EDSB noch nicht hinreichend klar herausgearbeitet und die Rolle der EZB und der anderen Zentralbanken noch nicht ausreichend konkretisiert. Zudem halten EDSA und EDSB weitere Garantien zum Schutz der Privatsphäre der Bürger*innen für notwendig, wie zum Beispiel eine angemessene Speicherbegrenzung für personenbezogene Daten. Darüber hinaus weisen der EDSA und der EDSB auf die potenziellen Risiken hin, denen der Digitale Euro aus IT- und Cybersicherheitssicht ausgesetzt sein könnte.

Fazit

Das Bargeld wird durch digitale Zahlungsmethoden zunehmend in Frage gestellt. Menschen in der EU legen bei einer digitalen Währung nicht nur Wert auf Geschwindigkeit, sondern auch auf Anonymität. Sicherheit und Datenschutz müssen für das Vertrauen in die digitale Währung gewährleistet sein. Dafür setzen sich die deutschen Datenschutzaufsichtsbehörden zusammen mit ihren Kolleg*innen in den anderen europäischen Ländern ein.

14.5. Bezahlen Kund*innen im kassenlosen Supermarkt mit ihren Daten?

Die Digitalisierung hat auch den Supermarkt erreicht. Der kassenlose Supermarkt wird durch Kameras und Sensoren zunehmend zur Realität. Er soll den Einkauf erleichtern, indem Wartezeiten an der Kasse entfallen. Das wirft Fragen zum Umgang mit den Daten der Kundschaft auf.

In den USA gibt es kassenlose Supermärkte seit 2018. In Deutschland werden solche Märkte seit 2021 durch ein in NRW ansässiges Einzelhandelsunternehmen in Köln, Berlin und München im Rahmen eines Pilotprojektes erprobt. Das Unternehmen beabsichtigt, den kassenlosen Einkauf möglicherweise flächendeckend und dauerhaft einzuführen. Es wandte sich an die LDI NRW und bat um Beratung zu der datenschutzrechtlichen Zulässigkeit des kassenlosen Einkaufs. Die Umsetzung dieses Pilotprojekts wird von der LDI NRW begleitet.

Der kassenlose Supermarkt verspricht, das Einkaufen zu vereinfachen, indem das Bezahlen an der Kasse entfällt. Die Ware wird aus dem Regal genommen und sogleich in die Tasche gesteckt. Dieser Vorgang wird von einer großen Zahl von Kameras und Sensoren erfasst. Dabei verfolgen die

Kameras Kund*innen auf ihrem Weg durch den Supermarkt. Sie registrieren dabei auch, wenn bereits entnommene Waren wieder zurückgelegt werden. Die Sensoren sind an den Verkaufsständen angebracht. In hybrid ausgestatteten Märkten, in denen sowohl kassenloses Einkaufen als auch Bezahlen an der Kasse möglich ist, werden alle Kund*innen aufgenommen – selbst die, die den neuen Service nicht nutzen. Dies geschieht, damit Einkäufe von konventionell bezahlenden Kund*innen nicht fälschlicherweise Nutzern*innen des kassenlosen Supermarktes zugeordnet werden.

Nutzer*innen des kassenlosen Einkaufens melden sich beim Betreten des Supermarktes mit Hilfe eines in einer App generierten QR-Codes an. Hierzu muss eine Schranke durchschritten werden. Für den Einkauf wird dann jeweils eine zufällig generierte Einkaufs-ID vergeben. So kann der Einkauf einer bestimmten Person zugeordnet und mit ihr abgerechnet werden. Will eine Begleitperson gemeinsam mit den Nutzer*innen des kassenlosen Einkaufens einkaufen, wird diese ebenfalls registriert und diese Einkaufs-ID der Person zugeordnet, die sie begleitet.

Gegenüber der Kundschaft, die kassenlos einkaufen möchte, kann das Unternehmen die Datenverarbeitung und hier insbesondere die Nachverfolgung der Einkaufsvorgänge mittels Videokameras auf den Vertrag stützen, den Nutzer*innen des kassenlosen Einkaufens mit dem Unternehmen abschließen (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe b DS-GVO). Bei Kund*innen, die das System nicht nutzen wollen, oder bei Begleitpersonen kommt eine Datenverarbeitung aus berechtigtem wirtschaftlichem Interesse des Unternehmens nach Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO in Betracht, wenn technisch-organisatorisch sichergestellt werden kann, dass die Grundrechte und -freiheiten der betroffenen Personen ausreichend geschützt sind.

Hierzu soll unter anderem durch die Ausrichtung und Auswahl der Kameras sichergestellt werden, dass Gesichter nicht erkannt werden können. Das der LDI NRW vorgelegte Konzept beinhaltet weitere technische und organisatorische Maßnahmen zur Datenminimierung, etwa zur Pseudonymisierung/Anonymisierung, um die Verarbeitung auf das für den Zweck erforderliche Maß zu beschränken.

Das Unternehmen hat auch Überlegungen zur datenschutzfreundlichen Ausgestaltung des Systems angestellt (Data Protection by Design). Auf Initiative der LDI NRW wurden weitere Verbesserungen durch eine Änderung der Technik zur Anonymisierung/Pseudonymisierung der Bilddaten umgesetzt. Zum Beispiel werden für einen Verarbeitungsschritt notwendige Bilddaten unwiederbringlich überschrieben, bevor sie in die Cloud des Auftragsverarbeiters gelangen. Die LDI NRW hat außerdem besonders darauf geachtet, dass eine Verarbeitung der personenbezogenen Daten zum Zweck des Profilings ausgeschlossen ist.

Durch Hinweisbeschilderungen bzw. Datenschutzerklärungen für alle Nutzer*innengruppen konnte im Rahmen der Beratung die Transparenz der Datenverarbeitung verbessert werden. Aufgrund der komplexen Datenverarbeitungsvorgänge, die bei den einzelnen Personengruppen unterschiedlich ausgestaltet sind, haben wir hierzu Empfehlungen ausgesprochen, die das Unternehmen aufgegriffen hat. So können Kunden*innen, die den kassenlosen Supermarkt mit der App nutzen, aber auch deren Begleitpersonen bzw. Personen, die an der Kasse bezahlen, noch besser nachvollziehen, welche personenbezogenen Daten für welche Zwecke und auf welche Art und Weise verarbeitet werden. Dies versetzt sie in die Lage zu entscheiden, ob sie in einem kassenlosen Supermarkt einkaufen möchten oder nicht.

Bei derartig komplexen Datenverarbeitungen findet regelmäßig eine Speicherung von Daten in einer Cloud statt. Falls es dabei Übermittlungen in Länder außerhalb des Europäischen Wirtschaftsraums gibt, sind weitere datenschutzrechtliche Anforderungen umzusetzen (Kapitel V der DS-GVO). Der Austausch mit dem verantwortlichen Unternehmen hierzu ist noch nicht abgeschlossen, sodass eine abschließende Bewertung noch nicht getroffen werden kann.

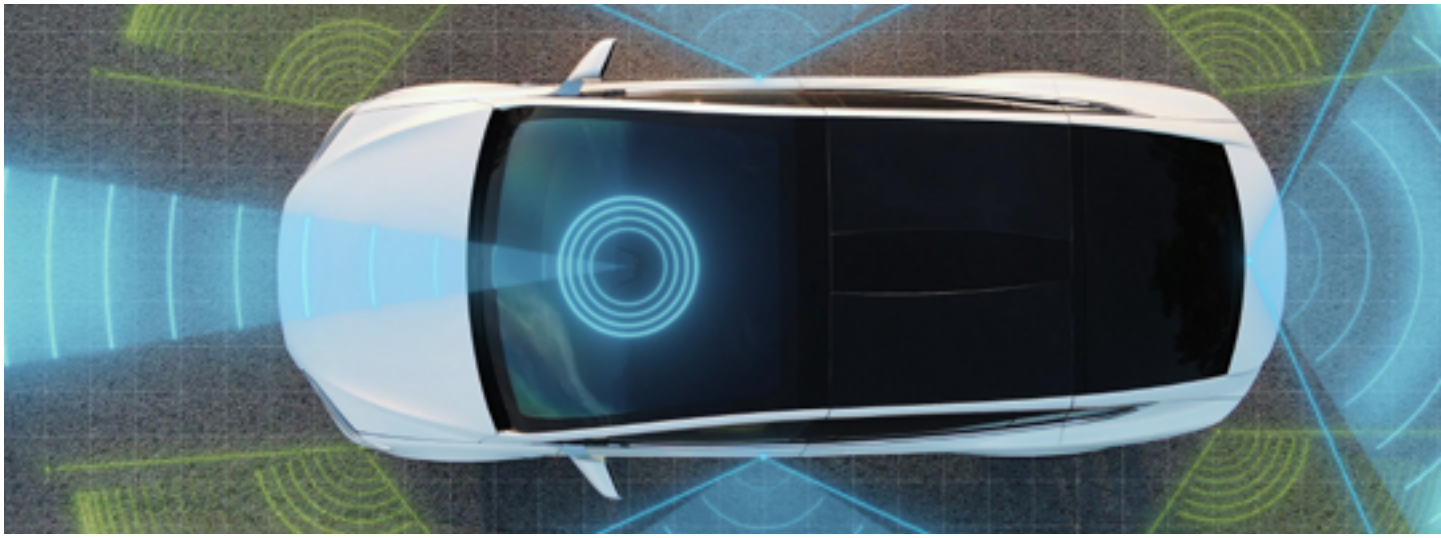
Der kassenlose Supermarkt ist ein Baustein auf dem weiten Feld der zunehmenden Digitalisierung von Prozessen, die bisher analog stattfanden. Das bedeutet, dass alle Beteiligten Erfahrungen zu rechtlichen und technischen Aspekten sammeln müssen. Implementierte Systeme werden in den kommenden Jahren zunehmend verbessert und fortentwickelt.

Das Unternehmen beabsichtigt die Ausweitung des kassenlosen Supermarktes auf weitere Standorte nach Ende der Pilotphase. Es hat angekündigt unsere Beratung auch zu weiteren Fragen, wie dem Schutz der Beschäftigtendaten, zu suchen. Dies begrüßt die LDI NRW ausdrücklich. Sie hat hierzu bereits Empfehlungen ausgesprochen. Wir werden über weitere interessante Entwicklungen in diesem Kontext berichten.

Fazit

Digitalisierung kann Prozesse beschleunigen und verbessern. Damit dabei die Datenschutzrechte nicht auf der Strecke bleiben, beraten wir bei großen Digitalisierungsvorhaben Unternehmen gern, wenn sie dazu frühzeitig auf uns zukommen und uns die notwendigen Informationen zur Verfügung stellen. Privacy by Design ist der richtige Weg, um Datenschutzverletzungen von vornherein zu vermeiden.

14.6. Autonomes Fahren: Grenzen für Datensammeln bei der Entwicklung



Die DSK hat ein „Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten“ beschlossen (Abdruck im Anhang). Dieses Papier entstand in Kooperation mehrerer Datenschutzaufsichtsbehörden und im Austausch mit dem Verband der Automobilindustrie e. V. Die LDI NRW war als Aufsichtsbehörde für die in NRW ansässigen Automobilhersteller und Zulieferer beteiligt.

Die audiovisuelle Umgebungserfassung – also die Aufnahme von Bild und Ton – dient dazu, aussagekräftige reale Verkehrsdaten zu sammeln, um Techniken für autonomes Fahren zu entwickeln und zu testen. Dabei werden Algorithmen der KI eingesetzt und auf das Fahren in realistischen Verkehrssituationen trainiert. Diese Datensammlung dient unter anderem dazu, bestehende oder neu zu entwickelnde Assistenzsysteme zu optimieren und das automatisierte und autonome Fahren weiterzuentwickeln. Moderne Ansätze für maschinelles Lernen benötigen in der Regel große Mengen an Daten. Je mehr Daten für das Training vorliegen, desto besser und zuverlässiger funktioniert der Algorithmus.

In dem DSK-Papier werden die datenschutzrechtlichen Aspekte für die Durchführung von Entwicklungs- und Erprobungsfahrten behandelt. Im Fokus steht dabei die Umgebungserfassung durch Videokameras und Mikrofone, die in Testfahrzeugen verbaut sind. Bei den Entwicklungs- und Erprobungsfahrten werden Bilder von der Umgebung aufgenommen, unter anderem mit Gesichtern von Personen und Kennzeichen von Fahrzeugen auf der Straße, aber auch von Personen, die sich zum Beispiel im Vorgarten aufhalten oder auf einem Spielplatz. Zwar sind die Personen für das maschinelle Lernen nicht relevant, ihre Erfassung durch die Kameras lässt sich technikbedingt allerdings nicht vermeiden.

Für den Testbetrieb kann die entsprechende Datenverarbeitung auf die berechtigten Interessen der Automobilhersteller gestützt werden (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO). Die Interessen der verantwortlichen Stelle sind mit denen der betroffenen Personen abzuwägen. Die Hersteller und Entwickler haben zum Beispiel ein berechtigtes Interesse an der (Weiter-)Entwicklung der Fahrerassistenzsysteme des automatisierten und des autonomen Fahrens. Diese Entwicklungen können auch der Verbesserung der Verkehrssicherheit und damit dem allgemeinen öffentlichen Interesse dienen. Dagegen abzuwägen ist das Interesse der betroffenen Personen, sich unbeobachtet im öffentlichen Raum bewegen zu können.

Zudem werden im Papier der Datenschutz durch Technikgestaltung und die zwingende Durchführung einer Datenschutz-Folgenabschätzung beleuchtet. Ein weiteres Thema des Papiers ist die Umsetzung der Informationspflichten sowie der Betroffenenrechte, zum Beispiel der Rechte auf Auskunft und Löschung.

Es kann noch nicht abschließend beurteilt werden, ob die Daten pseudonymisiert oder anonymisiert verarbeitet werden können. Die Hersteller geben an, dass eine Pseudonymisierung oder Anonymisierung der erhobenen Daten im Rahmen der Entwicklungsfahrten derzeit nicht realisierbar sei. Eine Verfälschung von Bildern mit dem Ziel, Gesichter oder Kennzeichen unkenntlich zu machen, würde das Risiko erhöhen, dass reale Situationen im Straßenverkehr dann nicht eindeutig erkannt werden können. Auch wenn diese Einschätzung nach derzeitigem Stand der Technik zutreffen sollte, müssen die Hersteller und Entwickler in regelmäßigen Abständen überprüfen, ob der Eingriff in die Rechte betroffener Personen durch fortgeschrittene technische Mittel ausgeschlossen oder abgemildert werden kann.

Auch noch nicht geklärt sind die datenschutzrechtlichen Anforderungen an den späteren Regelbetrieb autonom fahrender Fahrzeuge. Die DSK wird sich mit der Frage beschäftigten, ob hierzu ein besonderer gesetzlicher Regelungsbedarf besteht. Hieran wird sich die LDI NRW ebenfalls beteiligen.

Fazit

Die Entwicklung des autonomen Fahrens ist und bleibt ein wichtiges Thema für die Autohersteller und Autozulieferer und kann langfristig zur Sicherheit im Straßenverkehr beitragen. Bei der Erhebung der dafür erforderlichen Daten muss sowohl im Testbetrieb als auch später im regulären Betrieb der Datenschutz gewährleistet sein. Dafür setzt sich die LDI NRW zusammen mit den Datenschutzaufsichtsbehörden aller Länder und des Bundes ein.

14.7. Datenweitergabe an Subunternehmen – auch ohne Einwilligung

Es ist Alltagsgeschäft, dass Unternehmen zum Beispiel bei Auftragsspitzen Daten an Subunternehmen weitergeben. Sowohl die Unternehmen als auch deren Kundschaft sind oft unsicher, ob auch die Weitergabe von personenbezogenen Daten der Kundschaft an die Subnehmen zulässig ist, und fragen bei der LDI NRW nach.

Der Einsatz von Subunternehmen im Handwerk ist nach dem Bürgerlichen Gesetzbuch (BGB) grundsätzlich zulässig (§ 267 BGB), wenn er nicht vertraglich ausgeschlossen wurde. Wenn ein Handwerksbetrieb mehr Aufträge hat, als er mit den eigenen Beschäftigten bewältigen kann (Auftragsspitzen), oder ein Auftrag Leistungen umfasst, auf die der eigene Betrieb nicht eingerichtet ist, kann die Einbindung eines Subunternehmens erforderlich sein. Ein Beispiel sind Küchenbauunternehmen (Generalunternehmen), die für Starkstromarbeiten in der Küche Elektroinstallationsbetriebe (dann Subunternehmen) beauftragen. Ein Konflikt droht, wenn die Kundschaft bestimmte Erwartungen mit ihrem Auftrag verbindet. Wird zum Beispiel eine bestimmte Goldschmiede beauftragt, weil diese für ihre filigranen und ausgefallenen Ringe bekannt ist, so wird erwartet, dass nur der beauftragte Betrieb die Ringe anfertigt. Im Zweifel sollte sich die Kundschaft dies im Vertrag bestätigen lassen. Für den Bereich der Dienstleistungen nimmt der Gesetzgeber diesen Gedanken auf: Der zur Dienstleistung Verpflichtete hat die Dienste im Zweifel selbst zu leisten (§ 613 BGB). Deshalb können zum Beispiel Arbeitnehmer*innen ihre Arbeit nicht durch betriebsfremde Personen ausführen lassen.

Doch selbst wenn der Einsatz eines Subunternehmens zivilrechtlich gestattet sein sollte, müssen Auftragnehmer*innen noch prüfen, ob die personenbezogenen Daten der Kundschaft weitergegeben werden dürfen. Datenschutzrechtlich kommt es darauf an, ob die Verarbeitung der Daten für die Vertragserfüllung notwendig ist (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe b DS-GVO). Dass eine gewisse Datenverarbeitung durch einen Vertrag abgedeckt ist, bedeutet nicht schon, dass die Verarbeitung für die Erfüllung auch erforderlich ist. Nur wenn das der Fall ist, dürfen Subunternehmen personenbezogene Daten der Kundschaft mitgeteilt werden. Das kann zum Beispiel Name, Adresse und bestellte Leistung betreffen. Der anfangs erwähnte Elektroinstallationsbetrieb muss natürlich Adresse und Name der Kundschaft erfahren, um die notwendigen Installationen für den Kücheneinbau vornehmen zu können. Die Datenübermittlung ist in diesem Fall erforderlich.

Wenn hingegen eine vom Goldschmiedebetrieb mit der Anfertigung eines Ringes beauftragte dritte Person nur Informationen zum vereinbarten Design und zu dem Maß des anzufertigenden Ringes benötigt, wäre eine Übermittlung von darüberhinausgehenden personenbezogenen Daten der Kundschaft nicht erforderlich und datenschutzrechtlich unzulässig.

In jedem Fall ist es wichtig, dass das Unternehmen seine Kund*innen über die geplante Datenweitergabe an Subunternehmen direkt bei der Datenerhebung informiert. Das sorgt für Klarheit und vermeidet Irritationen, wenn ein Unternehmen vor der Tür steht, das eigentlich gar nicht selber beauftragt wurde. Nach Art. 13 DS-GVO sind Unternehmen, die personenbezogene Daten verarbeiten, gesetzlich dazu verpflichtet, Betroffene zum Zeitpunkt der Datenerhebung über Verarbeitungsvorgänge zu informieren. Das Subunternehmen muss grundsätzlich die Kundschaft ebenfalls über seine Datenverarbeitung informieren (Art. 14 DS-GVO). Diese Pflicht entfällt, wenn die Kundschaft diese Information bereits durch das Generalunternehmen selbst erhalten hat.

Fazit

Transparente Information über die Datenverarbeitung ist nicht nur rechtlich geboten, sondern wird auch als Serviceleistung wahrgenommen. Sie nimmt die Bedürfnisse der Kundschaft ernst und fördert ihre Zufriedenheit.

14.8. Versicherungen dürfen Detekteien beauftragen – müssen Betroffene aber informieren

Wenn eine Versicherung Betrug vermutet, dann darf sie unter bestimmten Voraussetzungen verdeckte Ermittler*innen einsetzen, um mutmaßlich Betrügende systematisch und zielgerichtet zu beobachten. Bei der LDI NRW ging dazu eine Beschwerde einer observierten Person ein.

Die Versicherung hatte aufgrund einer Klage im Zusammenhang mit einem Unfallschaden einen Betrugsverdacht. Um diesem Verdacht nachzugehen, beauftragte sie zunächst einen Dienstleister mit einer Vorrecherche. Dazu nutzte er ausschließlich öffentliche Quellen (zum Beispiel Soziale Medien). Erst nachdem sich der Verdacht erhärtete und keine weiteren Möglichkeiten zur Verfügung standen, „Licht ins Dunkle“ zu bringen, gab die Versicherung anschließend eine auf drei Tage begrenzte Observation im öffentlichen Raum in Auftrag. Dabei sollte auf die Weitergabe von sensiblen Daten verzichtet werden.

Die Rechtslage dazu ist komplex: Eine Verarbeitung personenbezogener Daten zur Betrugsabwehr kann grundsätzlich auf die DS-GVO gestützt werden (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO). Zweck der Verarbeitung ist in diesem Falle die Prüfung und Abwehr der Ansprüche, die gegen die Versicherung geltend gemacht werden. Dabei ist zu berücksichtigen, dass Versicherungen zur Betrugsabwehr verpflichtet sind und eine Verhinderung von Versicherungsmissbrauch im Interesse der Versichertengemeinschaft liegt.

Zwar besteht ein hohes Interesse daran, nicht von Ermittler*innen beobachtet zu werden. Doch die Interessen der Versicherungen und der Versichertengemeinschaft, nicht zu Opfern fingierter Schadensfälle zu werden, überwiegen in bestimmten Fällen. Das ist regelmäßig zumindest dann anzunehmen,

- wenn konkrete Anhaltspunkte für ein missbräuchliches Verhalten von Versicherungsnehmer*innen vorliegen,
- die beanspruchte Leistung eine gewisse Höhe erreicht hat und
- kein Grund zur Annahme besteht, dass das schutzwürdige Interesse der beobachteten Person aus besonderen Gründen überwiegt.

Besteht ein konkreter Anfangsverdacht für einen Versicherungsbetrug, kann also ein Eingriff in die Grundrechte von betroffenen Personen durch Observierungsmaßnahmen gerechtfertigt sein. Dabei ist zu beachten: Das Einschalten einer Detektei für die Beobachtung muss geeignet und erforderlich sein, den konkreten Zweck zu erreichen. Konkreter Zweck könnte zum Beispiel sein, den Betrugsverdacht zu erhärten. Dabei ist auf das mildeste Mittel abzustellen, das heißt der Eingriff in die Grundrechte der betroffenen Person muss möglichst gering ausfallen. In keinem Fall darf in den Kernbereich der Privatsphäre oder gar in die Intimsphäre eingegriffen werden.

Versicherungsunternehmen sollten interne Maßstäbe entwickeln, was vor einer Beauftragung der verdeckten Ermittler*innen zu prüfen und zu dokumentieren ist, mit wem die Auftragserteilung innerhalb des Hauses abzustimmen und was zu beachten ist. Dabei helfen Versicherungen bei einem Betrugsverdacht festgelegte Kriterien bei der Auswahl und Beauftragung von Detekteien:

- fachliche und örtliche Eignung
- zeitliche Befristung der Maßnahme
- Art der Ermittlungsmethode
- keine Weitergabe von personenbezogenen Daten an Dritte
- datenschutzgerechte Löschung/Vernichtung von personenbezogenen Daten
- Zugriff und Schutz der personenbezogenen Daten
- datenschutzrechtliche Vereinbarung zwischen Versicherung und Ermittlungsbüro
- Beschränkung der Datenübermittlung auf das für den konkreten Ermittlungszweck erforderliche Maß

Fazit

Der Einsatz von verdeckten Ermittler*innen zur Aufklärung eines begründeten Versicherungsbetrugsverdachts kommt nur in Betracht, wenn mildere Aufklärungsmittel nicht zur Verfügung stehen. In Einzelfällen kann die Überwachung auf das berechtigte Interesse gemäß Art. 6 Abs. 1 Unterabsatz 1 Buchtstabe f DS-GVO gestützt werden, um Fälle von Versicherungsmissbrauch im Sinne der Versichertengemeinschaft zu prüfen. Dabei hat die Versicherung im Vorfeld der Maßnahme interne Maßstäbe zu berücksichtigen und die verdeckten Ermittler*innen anhand festgelegter Kriterien auszuwählen. Auch darf kein Grund zur Annahme bestehen, dass das schutzwürdige Interesse einer betroffenen Person bei Durchführung der Maßnahmen überwiegt.

14.9. Bekämpfung von Geldwäsche und Datenschutz schließen sich nicht aus

Aufgrund einer Beratungsanfrage einer großen Spielbanken-Gruppe hat sich die LDI NRW mit dem Thema Glücksspiel befasst. Hintergrund: Spielbanken wären eigentlich verpflichtet, Spieler*innen auf Antrag eine vollständige schriftliche Auskunft – auch zu Besuchszeiten und Gewinnauszahlungen – zu erteilen (Art. 15 DS-GVO). Das kollidiert aber mit dem landesgesetzlichen Verbot, Gewinnbescheinigungen auszustellen. Es gibt jedoch ein Verfahren, um die Auskunft zu gewährleisten und das Verbot zu beachten.

Vorschriften zur Geldwäschebekämpfung schränken den Auskunftsanspruch von Spieler*innen nach Art. 15 DS-GVO ein. Obwohl Spielbanken Datum und Zeit eines Spielbankbesuchs sowie ausgezahlte Beträge personenbezogen erfassen, dürfen sie über diese Informationen nicht ohne Weiteres eine schriftliche Auskunft erteilen. Eine Auskunft darüber kollidiert grundsätzlich mit dem Verbot der Erteilung von Gewinnbescheinigungen, das verhindern soll, dass kriminell erlangte Gelder mittels Spielbanken reingewaschen werden. In NRW regelt das ein landesgesetzliches Verbot (§ 5 Abs. 6 Spielordnung NRW vom 18. November 2020). Diese nationale Ausnahmevorschrift kann das Auskunftsrecht aus Art. 15 DS-GVO nach Art. 23 DS-GVO wirksam einschränken.

Geldwäsche in Spielbanken funktioniert, indem Kriminelle Bargeld aus Straftaten oder auch Falschgeld in der Spielbank einzahlen, etwas spielen und sich den Rest wieder auszahlen lassen. Diese Auszahlung wird als „Gewinn“ deklariert, selbst wenn in Wirklichkeit kein Gewinn erzielt wurde oder vielleicht sogar Verluste entstanden sind. Eine andere Methode besteht darin, illegal erhaltenes Geld in der Spielbank von kleiner Stückelung in eine große Stückelung zu wechseln (Geldwechselfälle). Oder es wird mit Geld aus Straftaten (inkriminiertes Geld) und/oder Falschgeld am Glücksspiel teilgenommen, um tatsächliche Gewinne zu erzielen. In allen drei Fällen könnten die Gewinne anschließend mit Hilfe der Gewinnbescheinigung einer Spielbank legal auf ein Konto eingezahlt und damit in den legalen Geldkreislauf gebracht wer-

den. Deshalb haben sich Spielbanken bundesweit selbst verpflichtet, auf der Grundlage von § 6 Geldwäschegesetz keine Gewinnbescheinigungen auszustellen.

Das Verfahren zur Auskunft nach Art. 15 DS-GVO wurde auf Anregung der LDI NRW im Ergebnis so gestaltet, dass Betroffene die Informationen über die eigenen Daten im vollen Umfang erhalten können. Die schriftliche Auskunft enthält allerdings keine Daten zu Besuchszeiten und Auszahlungen, so dass diese nicht zur Entlastung vom Geldwäscheverdacht bei den Banken vorgelegt werden können. Betroffene können aber zur Überprüfung der Richtigkeit ihrer von der Spielbank gespeicherten Daten diese vor Ort (in der Spielbank) einsehen oder eine mündliche Auskunft erhalten. Sofern die Auskunftsersuchenden auch die anderen Daten schriftlich benötigen (zum Beispiel für einen Versicherungsfall, weil das Geld auf dem Nachhauseweg abhandengekommen ist), bedarf es dafür eines begründeten Antrages an die Bezirksregierung als Glücksspielaufsicht.

Fazit

Datenschutz behindert nicht die Bekämpfung von Geldwäsche. Durch Verfahrensgestaltung kann auch dem Auskunftsanspruch nach der DS-GVO hinreichend Rechnung getragen werden.

14.10. Ein Name im Briefkopf eröffnet nicht automatisch einen Auskunftsanspruch auf eine Kopie des gesamten Briefs

Die LDI NRW war mit einem Fall befasst, in dem sich ein Rechtsanwalt auf sein Auskunftsrecht nach Art. 15 DS-GVO gegenüber einer Versicherung berief. Er verlangte Kopien des gesamten Schriftverkehrs zwischen der Versicherung und einer Kanzlei, in der er Partner war. Der Anwalt begründete seinen Auskunftsanspruch damit, dass sein Name, wie es das Berufsrecht vorschreibt, als Partner auf dem Briefbogen der Kanzlei genannt ist.

Der Anwalt hatte mehrfach Mandant*innen gegenüber der Versicherung vertreten. Er beschränkte seinen Auskunftsanspruch aber nicht auf seine Mandatsverhältnisse, sondern wollte ausdrücklich auch Kopien des Schriftverkehrs mit der Versicherung aus Mandaten anderer Anwält*innen der Kanzlei. Er berief sich dabei unter anderem auf ein Urteil des Europäischen Gerichtshofs (EuGH zur Rechtssache C-487/21, Urteil vom 4. März 2023 zu Art. 15 Abs. 3 DS-GVO).

In den Anwendungsbereich des Auskunftsrechts nach Art. 15 DS-GVO fallen alle personenbezogenen Daten, die die Person betreffen, die die Auskunft verlangt. Die Nennung des Namens des Anwalts auf den Schreiben der

Rechtsanwaltskanzlei an die Versicherung ist ein personenbezogenes Datum. Dieses personenbezogene Datum enthalten auch die Schreiben, die nicht die Mandate des Anwalts betreffen.

Der Auskunftsanspruch erstreckt sich aber deswegen nicht automatisch auf alle Inhalte einer umfassenden Korrespondenz. Zumindest in Fällen, in denen der Anwalt nicht im eigenen Mandatsverhältnis tätig geworden ist, stößt das Auskunftsrecht nach Art. 15 an Grenzen, sofern Rechte und Freiheiten anderer Personen betroffen sind (Art. 15 Abs. 4 DS-GVO) und Art. 23 Abs. 1 DS-GVO in Verbindung mit § 29 Abs. 1 BDSG (Mandatsgeheimnis). Die Interessen des Anwalts werden dabei regelmäßig hinter den Interessen der Personen aus dem fremden Mandatsverhältnis zurückstehen.

Ohnehin musste die Versicherung bei fremden Mandaten nicht sämtliche Geschäftsbriefe in Kopie zur Verfügung stellen, obwohl der Name des Anwalts im Briefkopf stand. Das Recht auf Kopie nach Art. 15 Abs. 3 DS-GVO richtet sich nicht auf Dokumente, sondern auf die vom Verantwortlichen zu einer Person verarbeiteten personenbezogenen Daten.

In diesem Sinne ist das anfangs erwähnte EuGH-Urteil vom 4. März 2023 in der Rechtssache C-487/21 zu verstehen: Der EuGH verlangt eine originalgetreue und verständliche Reproduktion aller personenbezogener Daten. Eine Kopie von Auszügen aus Dokumenten oder gar von ganzen Dokumenten oder Datenbanken ist aber nur dann erforderlich, wenn die Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung ihrer Datenschutzrechte zu ermöglichen. Eine solche Kopie von Dokumenten ist bei Schreiben, in denen der Anwalt nur im Kopfbogen steht, nicht unerlässlich für das Verständnis und damit nicht erforderlich.
Im geprüften Fall hat die Versicherung die Herausgabe von Kopien von Schreiben, die nicht die Mandate des Anwalts betrafen, zu Recht abgelehnt.

Fazit

Der Begriff des personenbezogenen Datums ist von der DS-GVO eigentlich weit gefasst. Allerdings wird die Herausgabe von Kopien von ganzen Dokumenten durch Rechte Dritter eingeschränkt. Die Herausgabe reicht nur so weit, wie die Information für die Wahrung eigener Datenschutzrechte notwendig ist.

14.11. Auskunftsrecht – Betroffene haben die Wahl

Das Recht auf Auskunft ist ein zentrales Element der DS-GVO, das die Betroffenen in die Lage versetzt, das Ausmaß der sie betreffenden Datenverarbeitungen zu erkennen. Verantwortliche dürfen den Weg, auf dem Betroffene dieses Recht geltend machen, nicht durch einseitige Formvorgaben einschränken.

Uns erreichte eine Beschwerde gegen ein verantwortliches Unternehmen, das im Internet eine Buchungsplattform betreibt. Auf der Plattform können Hotels, Ferienwohnungen und andere Unterkünfte ausschließlich elektronisch gebucht werden. Kund*innen suchen auf der Plattform nach der passenden Unterkunft, sie buchen und erhalten anschließend eine Bestätigung – per E-Mail. Eine Buchung auf postalischem Weg ist nicht möglich.

Wenn Kund*innen ihre Rechte als Betroffene – also zum Beispiel das Recht auf Auskunft oder Löschung – geltend machen, sieht das Unternehmen auch hierfür nur die Kommunikation via E-Mail vor. Für das Unternehmen hat das den Vorteil, die Bearbeitung effizient organisieren zu können: Anhand der E-Mail-Adresse werden vom Unternehmen die betroffenen Kund*innen identifiziert und authentifiziert. Anschließend werden die personenbezogenen Daten, die der Mailadresse zugeordnet werden (Name/Vorname Telefonnummer, E-Mail-Adresse, ggf. freiwillig erteilte weitere Angaben), dem geltend gemachten Recht entsprechend verarbeitet, sie werden also zum Beispiel gelöscht oder die Betroffenen erhalt die gewünschte Auskunft.

Im konkreten Fall wollte die betroffene Person ihr Auskunftsrecht allerdings per Post geltend machen. Sie erhielt die gewünschte Auskunft zunächst nicht, sondern wurde darauf verwiesen, ihr Anliegen elektronisch geltend zu machen.
Eine solche Beschränkung auf die elektronische Kontaktaufnahme beschneidet die Betroffenen in der Wahrnehmung ihrer Datenschutzrechte. Betroffene haben die Wahl, über welchen Kommunikationskanal sie mit dem Verantwortlichen in Kontakt treten. Auch wenn das Unternehmen eine elektronische Kommunikation vorzugswürdig findet, kann es einen ausschließlich postalisch eingegangenen Auskunftsanspruch nicht ignorieren:

- Die DS-GVO macht keine Vorgaben zur Form des Antrags für Betroffenenrechte. Verantwortliche können zwar bestimmte Kommunikationskanäle vorrangig anbieten und bewerben, über die Betroffene ihre Rechte geltend machen können. Sie dürfen aber betroffenen Personen die Möglichkeit nicht verwehren, auch auf einem anderen Weg ihre Rechte geltend zu machen. Denn Verantwortliche haben der betroffenen Person die Ausübung ihrer Rechte zu erleichtern (Art. 12 Abs. 2 DS-GVO). Betroffene können mit der Wahl eines Kommunikationskanals zu erkennen geben, dass beispielsweise die Auskunft auf diese Weise für sie „leicht zugänglich ist“ (Art. 12 Abs. 1 DS-GVO).

- Verantwortliche können einen anderen Weg nur dann ablehnen, wenn sie Daten so nicht sicher übermitteln können.

- Verantwortliche können zusätzliche Informationen zur Authentifizierung und Identifizierung fordern, wenn auf dem Weg, auf dem die Betroffenen ihre Rechte geltend machen, ansonsten nicht sichergestellt werden kann, dass die Person als berechtigt identifiziert werden kann.

Im von uns geprüften Fall musste der Verantwortliche auch aufgrund des postalisch geltend gemachten Auskunftsrechts tätig werden. Es gab keinen Grund zu der Annahme, dass eine Übermittlung per Post ein unsicherer Weg ist.

Fazit

Die DS-GVO will Betroffenen die Geltendmachung ihrer Rechte möglichst leicht machen. Dabei was leicht ist, kommt es auf die Perspektive der Betroffenen an. Selbst wenn die ganze Kund*innen-Kommunikation elektronisch läuft, müssen Verantwortliche auch einen postalisch geltend gemachten Auskunftsanspruch erfüllen. Dies gilt entsprechend auch für andere Betroffenenrechte, wie etwa Löschungs- oder Berichtigungsansprüche.

14.12. EuGH: Konkretes Handeln von Personen aus der Unternehmensleitung muss bei Bußgeldern nicht mehr nachgewiesen werden

Der Europäische Gerichtshof (EuGH) stellt fest, dass bei Verstößen von Unternehmen gegen die DS-GVO, die mit einem Bußgeld geahndet wurden, kein konkretes Handeln oder Unterlassen einer (individualisierten) Leitungsperson erforderlich ist, um das Unternehmen zur Verantwortung ziehen zu können. Ein schuldhaftes Handeln in Form von Vorsatz oder Fahrlässigkeit bleibt jedoch notwendige Voraussetzung zur Einleitung eines datenschutzrechtlichen Bußgeldverfahrens.

In Deutschland gilt grundsätzlich das Rechtsträgerprinzip (§§ 30, 130 Ordnungswidrigkeitengesetz, OWiG). Danach können Unternehmen bzw. juristische Personen im Allgemeinen nur dann mit einem Bußgeld belegt werden, wenn die Tat durch eine verantwortliche Person begangen wurde bzw. dieser

zumindest mittelbar zuzurechnen ist. Verantwortliche Personen sind in diesem Zusammenhang Beschäftigte, die regelmäßig strategische Entscheidungen treffen, wie beispielsweise Geschäftsführer*innen und leitende Angestellte. Dem Europäischen Recht – und damit auch der DS-GVO – ist eine solche Zurechnung fremd. Zwar ist die DS-GVO als europäische Verordnung unmittelbar in den Mitgliedstaaten anwendbar. Das Bußgeldverfahren konnte allerdings national konkretisiert werden. Dazu legt § 41 Bundesdatenschutzgesetz (BDSG) fest, dass für Bußgeldverfahren nach der DS-GVO das OWiG grundsätzlich entsprechend gelten soll. Rechtlich umstritten war dann jedoch, ob hinsichtlich der Zurechnung von Datenschutzverstößen zu Unternehmen, die dem Europarecht fremden, engeren Regelungen des OWiG (§§ 30, 130) gelten.

Gerade bei großen, international tätigen Unternehmen war es in Bußgeldverfahren aufgrund der Anwendung der §§ 30, 130 OWiG bisher regelmäßig problematisch, einen konkreten Nachweis für die Verantwortlichkeit eines Mitglieds der Geschäftsführung oder des Vorstands zu erbringen. Folge dieser deutschen Sonderregelungen war eine uneinheitliche Sanktionspraxis innerhalb der EU. Auch in Deutschland gab es dazu eine uneinheitliche Rechtsprechung, die im vorherigen Bericht dargestellt wurde.

Genau um diese Frage ging es in einem Bußgeldverfahren der Berliner Beauftragten für Datenschutz und Informationsfreiheit (BInBDI) gegen die Deutsche Wohnen SE. Nachdem das Landegericht Berlin dieses Verfahren aufgrund der vermeintlich fehlenden Zurechnung über die §§ 30, 130 des OWiG eingestellt hatte, legte die Staatsanwaltschaft dagegen Beschwerde ein. Das Verfahren wurde an das Kammergericht Berlin abgegeben, welches dem EuGH zwei relevante Rechtsfragen, insbesondere die Europarechtskonformität der §§ 30, 130 OWiG, zur Vorabentscheidung vorlegte: Hängt die Rechtmäßigkeit einer Geldbuße von der vorherigen Feststellung eines Verstoßes durch individualisierte Leitungspersonen, die im Dienst dieser juristischen Person stehen, ab? Ist die Feststellung eines schuldhaften Handelns in Form von Vorsatz oder Fahrlässigkeit unabdingbare Voraussetzung für die Sanktionierung einer Tat?

Der EuGH entschied nun, dass die Zurechnungsvoraussetzungen der §§ 30, 130 OWiG im Rahmen einer Sanktion nach der DS-GVO nicht anwendbar sind (Urteil vom 5. Dezember 2023, Az. C-807/21). Unternehmen können (als juristische Personen) nach Ansicht des EuGH auf Grundlage der DS-GVO direkt für einen Verstoß mit einem Bußgeld sanktioniert werden, sofern sie Verantwortliche im datenschutzrechtlichen Sinne sind. Es ist somit nicht erforderlich, dass der Datenschutzverstoß der Geschäftsleitung zugerechnet werden kann. Es ist darüber hinaus noch nicht einmal erforderlich, dass der Verstoß überhaupt einer identifizierten natürlichen Person zugeordnet werden kann. Es liefe dem Zweck der DS-GVO zuwider, wenn es den Mitgliedstaaten gestattet wäre, einseitig engere Anforderungen für die Verhängung von Bußgeldern festzulegen, als die DS-GVO. Dies könne letztlich die Wirksamkeit und die abschreckende Wirkung von Geldbußen schwächen.

Schuldhaftes Handeln in Form von Vorsatz oder Fahrlässigkeit bleibt allerdings Voraussetzung zur Sanktionierung eines datenschutzrechtlichen Verstoßes – und muss insofern im Rahmen des Bußgeldverfahrens festgestellt werden. Ein rein objektiver Pflichtverstoß ohne Verschulden der Beteiligten ist dagegen nicht bußgeldbewährt. Entscheidend für ein Verschulden ist, „ob sich der Verantwortliche über die Rechtswidrigkeit seines Verhaltens nicht im Unklaren sein konnte“.

Fazit

Mit seiner Entscheidung schafft der EuGH Klarheit und stärkt damit insbesondere die Handlungsmöglichkeiten der Datenschutzaufsichtsbehörden. Dies gilt in besonderem Maße auch für die LDI NRW, die im gerichtlichen Verfahren wegen der Anwendung des Rechtsträgerprinzips bisher bei der Durchsetzung von Bußgeldern auf Grenzen gestoßen ist. Wie die Hinweise des EuGH nun in der deutschen Datenschutzaufsichts- und Gerichtspraxis im Einzelfall angewendet werden, bleibt aber ein spannender Prozess.

15. Datensicherheit

15.1. Leitfaden bietet Hilfe beim Cyberangriff

2023 sind nach Schätzungen rund 58 Prozent der deutschen Unternehmen Ziel eines Cyberangriffs geworden. Die LDI NRW hat einen Leitfaden zum Umgang mit solchen Attacken erstellt.

Fließen bei einem Cyberangriff personenbezogene Daten ab oder sind anderweitig gefährdet, ist das auch ein Fall für die LDI NRW. Beispiele aus der Praxis:

- Der Geschäftsführer eines Handwerksunternehmens erhielt von seiner beruflichen E-Mail-Adresse eine Nachricht auf sein privates E-Mail-Konto. Eine unbekannte Person drohte in der E-Mail mit der Veröffentlichung von Daten und Chatverläufen und forderte den Geschäftsführer zur Zahlung von 400 Dollar in Bitcoin auf.

- Eine Steuerberaterin fand zum Arbeitsbeginn eine Nachricht auf ihrem Computer: „Your data is stolen and encrypted, if you don't pay the ransom, the data will be published on our TOR darknet sites". Alle Daten auf dem Computer waren verschlüsselt und damit unbrauchbar.

- Die „Qualitäts- und Unterstützungs Agentur – Landesinstitut für Schule" (Qualis) wurde durch einen „ethischen Hacker" über eine unsichere Schnittstelle in einem Verzeichnisdienst informiert. Es war möglich, eine große Anzahl von Kontaktdaten von Lehrer*innen und Beschäftigten der Agentur abzurufen. Auch die Presse berichtete über diesen Vorfall. Glück gehabt: Ethische Hacker verfolgen in der Regel keine Schädigungsabsichten, sondern informieren die betroffenen Stellen über gefundene Sicherheitslücken, um auf eine Verbesserung der IT-Sicherheit hinzuwirken und die betroffenen Personen vor Hackern mit bösartigen Absichten zu schüt-

zen. Nach einer Prüfung konnten keine Hinweise darauf gefunden werden, dass bereits vor dem ethischen Hacker Unbefugte die Sicherheitslücke bei Qualis ausgenutzt haben und die Kontaktdaten missbräuchlich verwenden.

Die Beispiele zeigen, dass auch kleine und mittelständische Verantwortliche mit der wachsenden Bedrohung durch Cyberangriffe konfrontiert sind. Sie sind – nach Erfahrungen der LDI NRW – in der Regel damit überfordert, eigenständig auf einen Cyberangriff zu reagieren. Bereits die Prüfung, ob überhaupt ein Cyberangriff vorliegt, ist für sie schwierig. Daher benötigen die betroffenen Stellen häufig externe Unterstützung. Dies betrifft auch die Stärkung der Cybersicherheit und die Vorsorge vor Cyberangriffen.

Die LDI NRW hat dazu einen Leitfaden zum Umgang mit Cyberangriffen und den damit verbundenen datenschutzrechtlichen Pflichten erstellt, abrufbar unter www.ldi.nrw.de/cyberangriff. Der Leitfaden umfasst fünf Schritte:

1. Cyberangriffe stoppen oder zumindest eingrenzen
2. Untersuchung des Vorfalls
3. Auswirkungen auf die betroffenen Personen bestimmen
4. Nachteile für die betroffenen Personen abmildern
5. Schutzniveau der Systeme der Gefahr anpassen

Verantwortliche können den Leitfaden bereits vor einem Vorfall heranziehen, um den Schutz vor Cyberangriffen zu bewerten und einen Notfallplan zu entwickeln. Es ist empfehlenswert, bereits vor einem Vorfall den Kontakt zu einem Dienstleister im IT-Sicherheitsbereich aufzunehmen, an den man sich im Falle eines Cyberangriffs wenden kann.

Fazit

Vorsicht ist besser als Nachsicht! Verantwortliche Stellen sollten nicht erst warten, bis sie Ziel eines Cyberangriffs werden. Sie sollten sich bereits frühzeitig mit der Möglichkeit auseinandersetzen. Denn tatsächlich ist inzwischen nicht die Frage, ob man Opfer eines solchen Angriffes wird, sondern nur noch, wann es passiert. Und um dann den Schaden möglichst gering zu halten oder den Angriff sogar abzuwehren, bedarf es der Vorbereitung.

15.2. E-Mails werden in der Regel verschlüsselt versandt

Bürger*innen, deren Daten per E-Mail übermittelt werden, befürchten mitunter, dass ihre Daten dabei nicht richtig geschützt sind und wenden sich an die LDI NRW. Vielfach besteht aber gar kein Anlass zur Sorge.

E-Mail-Empfänger*innen vermuten, dass beim Versand keine technischen Maßnahmen zum Schutz der Vertraulichkeit der in der Nachricht enthaltenen Daten getroffen wurden. Diese Vermutung beruht meistens auf der Schwierigkeit, dass es nicht unmittelbar erkennbar ist, ob und welche Verschlüsselung beim Versand der E-Mail angewendet wurde. Tatsächlich werden E-Mails in der Regel mit einer Transportverschlüsselung versandt. Oft ist diese Verschlüsselung ausreichend.

Eine E-Mail kann zwischen dem Versand und dem endgültigen Empfang mehrere Zwischenstationen durchlaufen. Die Transportverschlüsselung sorgt dabei für den Aufbau einer verschlüsselten Verbindung zwischen diesen Kommunikationspunkten und reduziert das Risiko einer passiven Abhörmaßnahme durch Dritte auf dem Transportweg. Eine Transportverschlüsselung ist vollkommen ausreichend, wenn es sich um allgemeine, personenbezogene Daten handelt, für die kein erhöhter Schutzbedarf besteht. Die Transportverschlüsselung bietet dann einen Basis-Schutz und ist die Mindestmaßnahme zur Erfüllung der gesetzlichen Anforderungen.

Anders sieht es bei E-Mails aus, die personenbezogene Daten enthalten, deren Bekanntwerden ein hohes Risiko für die Rechte und Freiheiten von natürlichen Personen darstellen würde. Das gilt beispielsweise für Gesundheitsdaten aber auch andere besonders sensible Informationen. Sie müssen regelmäßig durch eine Ende-zu-Ende-Verschlüsselung und eine qualifizierte Transportverschlüsselung geschützt werden.

Da Transportverschlüsselungen vom E-Mail-Dienst der Empfänger*innen beim Eingang der Nachricht sofort wieder aufgelöst werden und die E-Mail dann im Klartext vorliegt, ist für die Empfänger*innen nicht erkennbar, ob eine Verschlüsselung stattgefunden hat. Dadurch kann dort der Eindruck entstehen, dass beim Versand der E-Mail gar keine Sicherheitsmaßnahmen getroffen wurden.

Die Anwendung einer Transportverschlüsselung entspricht dem aktuellen Stand der Technik. Je nach Konfiguration des verwendeten E-Mail-Dienstes wird bereits der Versand von Nachrichten unterbunden, falls kein gesicherter Kommunikationskanal zwischen den Diensten aufgebaut werden kann.

Bei Beschwerden informiert die LDI NRW die Beschwerdeführer*innen über die technischen Grundlagen und prüft den Einzelfall. In der Regel ergeben sich dabei allerdings keine Anhaltspunkte für einen unverschlüsselten Versand. In wenigen Ausnahmefällen lag 2023 ein tatsächlicher technischer

Mangel vor, der von der LDI NRW aufgegriffen wurde, um eine Korrektur zu erwirken. In der Praxis ist somit kein relevantes Defizit bei der Umsetzung der Transportverschlüsselung im E-Mail-Verkehr festzustellen.

Die konkreten technischen Anforderungen an den E-Mail-Versand werden in der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ der DSK vom 27. Mai 2021 im Detail erklärt, abrufbar unter www.datenschutzkonferenz-online.de.

Fazit

Ein gänzlich unverschlüsselter Versand von E-Mail-Nachrichten ist aufgrund des allgemein etablierten Standes der Technik nur in seltenen Ausnahmen zu beobachten. Die LDI NRW informiert bei Beschwerden regelmäßig über die technischen Grundlagen des Verfahrens, um Missverständnisse auszuräumen.

15.3. Wann ist eine „Souveräne Cloud“ tatsächlich souverän?

Der Begriff „Souveräne Cloud“ suggeriert, dass man die volle Bestimmungshoheit über die Datenverarbeitung in der Cloud behält. Die Lösungen, die am Markt angeboten werden, sind vielfältig. Allein das Label „Souveräne Cloud“ gewährleistet noch nicht, dass sie für eine datenschutzgerechte Datenverarbeitung geeignet ist. Hier will die DSK mit einem Positionspapier weiterhelfen. Es soll Verantwortlichen als bei der Entscheidung helfen, ob eine souveräne Cloud datenschutzkonform genutzt werden kann.

Auf dem Markt gibt es bereits seit geraumer Zeit diverse Cloud-Angebote, die damit werben, den Anwendenden die Ausübung ihrer „Digitalen Souveränität“ zu ermöglichen. Dieser Begriff wird in der öffentlichen Debatte allerdings unterschiedlich verstanden. Eine allgemeingültige Definition gibt es bislang nicht. Je nach Sichtweise – etwa aus Perspektive der Ökonomie, der Forschung, der inneren und äußeren Sicherheit sowie der IT-Sicherheit – werden unterschiedliche Schwerpunkte der technologischen Unabhängigkeit betont. Das Kompetenzzentrum Öffentliche IT versteht darunter „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“. Danach verdient das Angebot einer „Souveränen Cloud“ diesen Namen nur, wenn es den verantwortlichen Stellen (als Anwendende einer solchen Cloud) ermöglicht, ihren datenschutzrechtlichen Pflichten effektiv, nachprüfbar und dauerhaft nachzukommen.

Das unter der Mitwirkung der LDI NRW entstandene Positionspapier „Kriterien für Souveräne Clouds“ vom 11. Mai 2023 nennt nun Kriterien, die von einem Cloud-Angebot mindestens erfüllt sein müssen (Mindestkriterien), wenn in der Cloud personenbezogene Daten verarbeitet werden sollen. Darüber hinaus gibt es weitergehende Empfehlungen, die eine besonders datenschutzfreundliche und langfristig datenschutzkonforme Cloud auszeichnen. Eine souveräne Cloud muss dabei mindestens alle Bestimmungen des Datenschutzrechts – insbesondere der DS-GVO – einhalten, um aus Sicht der DSK als souverän zu gelten.

Mithilfe dieser Kriterien können Verantwortliche in Wirtschaft und Verwaltung beurteilen, ob ein als souverän bezeichnetes Cloud-Angebot zur datenschutzkonformen Verarbeitung personenbezogener Daten grundsätzlich geeignet ist und auch auf lange Sicht geeignet bleibt. Die Rechte und Freiheiten natürlicher Personen stehen dabei im Fokus. Thematisch lassen sich die aufgestellten Kriterien in folgende Bereiche einteilen:

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

Angesprochen werden sowohl Anbietende von Cloud-Diensten, als auch deren Anwendende. Die konkrete Umsetzung der aufgezeigten Kriterien obliegt in der Praxis regelmäßig den Anbietenden, weil diese wesentlich die technische Ausgestaltung des Dienstes beeinflussen. Aus diesem Grund enthält das Positionspapier keine konkreten Hinweise auf die Umsetzung der Kriterien.

Das Papier verfolgt das Ziel, die Sicht der DSK auf den Begriff einer „Souveränen Cloud“ darzulegen und so die Grundlage für ein allgemeines Verständnis zu schaffen. Die Kriterien unterstützen bei der Bewertung und Auswahl passender Angebote auf dem Markt, bedeuten aber ausdrücklich keine abschließende Bewertung einzelner Angebote. Das Papier ist unter www.datenschutzkonferenz-online.de abrufbar.

Fazit

Das Positionspapier informiert über die Erwartungen der DSK hinsichtlich der „Souveränität“ im Zusammenhang mit datenschutzgerechten Cloud-Diensten. Die aufgestellten Kriterien erlauben einen Vergleich der auf dem Markt bereits erhältlichen und zukünftig angebotenen souveränen Cloud-Lösungen.

15.4. Was man bei einer Datenpanne tun kann

Wenn Bürger*innen erfahren, dass sie von einer Datenpanne betroffen sind, sind sie schockiert oder zumindest verunsichert. Wie sollen sie sich nun verhalten? Und welche Schritte können oder sollten sie veranlassen? Um Betroffenen eine erste Orientierung zu geben, hat die LDI NRW Antworten auf häufig gestellte Fragen zusammengetragen.

Bürger*innen können auf verschiedenen Wegen von Datenpannen erfahren. Bei einem voraussichtlich hohen Risiko für sie müssen die Betroffenen aktiv von der datenverarbeitenden Stelle informiert werden. Manchmal lesen Betroffene in der Zeitung davon, dass ein Unternehmen, mit dem sie in Kontakt stehen, von einer Datenpanne betroffen ist. Schließlich kann mit sog. „Leak-Checkern“ geprüft werden, ob die eigenen Kontaktdaten in veröffentlichten Datensammlungen aus Angriffen enthalten sind. Dies alles führt regelmäßig zu Nachfragen Betroffener bei der LDI NRW. Antworten auf die meisten Fragen haben wir auf unserer Internetseite www.ldi.nrw.de/faq-datenpannen veröffentlicht.

Datenpanne ist umgangssprachlich das, was juristisch „Verletzung des Schutzes personenbezogener Daten“ heißt. Die „Verletzung des Schutzes personenbezogener Daten“ liegt nach der DS-GVO vor, wenn ein

Ereignis, „unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“. Eine Datenpanne kann zum Beispiel sein,

- wenn ein Datenträger mit Daten von Kund*innen oder Geschäftspartner*innen verloren geht,
- wenn personenbezogene Daten von Kund*innen oder Beschäftigten aus Versehen gelöscht werden oder
- wenn sich „Hacker“ Zugriff auf die Daten verschafft haben.
- Datenpannen können also verschiedene Ursachen haben und in verschiedenen Bereichen auftreten.

Mit der Datenpanne sind Pflichten verbunden: Gehen zum Beispiel in einem Unternehmen Kund*innendaten verloren oder tauchen ungewollt im Internet auf, dann besteht in der Regel eine gesetzliche Meldepflicht bei der Aufsichtsbehörde – in Nordrhein-Westfalen bei der LDI NRW. Wenn aufgrund der Datenpanne für die betroffenen Personen ein voraussichtlich hohes Risiko für ihre Rechte und Freiheiten besteht, müssen diese zudem von der verantwortlichen Stelle benachrichtigt werden.

Auf Basis der Erfahrung als Aufsichtsbehörde gibt die LDI NRW Antworten zu häufig gestellten Fragen rund um die Datenpanne – von Informationsrechten bis zu Meldepflichten. Zudem stellt die LDI NRW vor, welche Möglichkeiten sie hat, im Falle einer Datenpanne tätig zu werden und zu helfen. Dabei geht es um Ursachenforschung wie um Betroffenenschutz gleichermaßen. So prüft die Aufsichtsbehörde, ob die verantwortliche Stelle angemessene und geeignete Maßnahmen zur Behebung und Abmilderung der Datenpanne getroffen hat, ob der Vorfall ausreichend untersucht wurde und ob für die Zukunft ein angemessenes Schutzniveau gewährleistet wird. Bei der zivilrechtlichen Beurteilung zum Beispiel eines Anspruchs auf Schadenersatz kann die LDI NRW allerdings nicht unterstützen.

Es werden auch Empfehlungen für Selbstschutzmaßnahmen ausgesprochen, mit denen Betroffene einem möglichen Schaden vorbeugen bzw. diesen minimieren können. Hierzu gehören das Ändern von Passwörtern, die Wachsamkeit hinsichtlich Kontobewegungen, E-Mails und Anrufen sowie die Berücksichtigung allgemeiner IT-Sicherheitsmaßnahmen.

Fazit

Die LDI NRW prüft Ursache und Auswirkung einer Datenpanne. Ein besonderes Augenmerk liegt dabei darauf, dass der Schaden für die Betroffenen minimiert wird. Mit den FAQ kann die LDI NRW Betroffene effektiv beraten und unterstützen.

16. Anhang

16.1. Positionspapier der Datenschutzaufsichtsbehörden der Länder zur nationalen Umsetzung der Europäischen Datenstrategie vom 06.12.2023

Leitgedanken

(1) Die nationale Umsetzung der Europäischen Datenstrategie erfordert ein stringentes nationales Gesamtkonzept. Darin müssen sich Bund und Länder zu den Chancen und Risiken der Europäischen Datenstrategie positionieren und insbesondere die Wahrnehmung der Aufsicht über die europäischen Rechtsakte in den Strukturen eines föderalen Staates vorbereiten. Dies gilt umso mehr als die Digitale Transformation in Unternehmen und Behörden bereits in vollem Gange ist und den Alltag der Bürgerinnen und Bürger erreicht.

(2) Die Verarbeitung personenbezogener Daten durch Technologien auf Grundlage Künstlicher Intelligenz führt genauso wie eine Ökonomie des Datenteilens zu neuen Gefährdungen für die Grundrechte der Betroffenen. Deren Schutz erfordert Aufklärung, risikoadäquate Schutzmechanismen und wirksame Kontrolle durch unabhängige Aufsichtsbehörden. Handlungsfähige Aufsichtsstrukturen sind deshalb Grundbedingungen für Vertrauen und Akzeptanz, mithin für den Erfolg der Digitalen Transformation im Alltag der Bürgerinnen und Bürger.

(3) Nur mit klar abgegrenzten Kontrollaufgaben betraute, adäquat ausgestattete Institutionen können der Dynamik der technologischen und wirtschaftlichen Entwicklung gerecht werden, verlässliche Rahmenbedingungen für Betroffene und Unternehmen bieten und in den europäischen und globalen Debatten frühzeitig und klar wahrnehmbar für Deutschland Positionierungen ermöglichen.

(4) Der institutionellen Ordnungsrahmen einer nationalen Digitalstrategie sollte sich an vorhandenen Strukturen ausrichten und die Möglichkeiten ihrer Fortentwicklung ausschöpfen, statt neue Verwaltungsstrukturen zu entwickeln und langwierige Aufbauprozesse anzustoßen.

(5) Soweit die neuen EU-Rechtsakte eine national koordinierende Behörde als zentrale Kontaktstelle für die europäische Koordinierung vorsehen, bedeutet dies nicht, dass dazu innerstaatliche Zuständigkeiten zwangsläufig zentralisiert werden müssten. Weder eröffnet die verfassungsrechtliche Aufgabenverteilung von Bund und Ländern hierzu unbeschränkte Spielräume, noch bestehen hinreichende, rechtspolitisch überzeugende sachliche Gründe, die seit Jahrzehnten eingeübte Koordination und Kooperation von Bundes- und Landesbehörden durch eine vermeintlich effektivere Zentralisierung

von Aufgaben beim Bund zu ersetzen. Jedenfalls dort, wo eine Aufgabenzentralisierung in ihrer praktischen Umsetzung eine Vielzahl von Abstimmungserfordernissen mit den Datenschutzaufsichtsbehörden der Länder zwangsweise und einzelfallbezogen erzeugen würde, sollte sie schon im Interesse von Effizienz und Bürokratievermeidung unterbleiben.

(6) Eine der Schlüsselaufgaben bei der Entwicklung des institutionellen Ordnungsrahmens für die nationale Datenstrategie liegt in der effizienten Ausgestaltung der Kooperationsbeziehungen der jeweils zuständigen Behörden.

(7) Die Datenschutzaufsichtsbehörden der Länder haben Expertise und Vollzugs- wie Beratungskompetenz in allen Fragen des Datenschutzes, der ein wesentlicher Bestandteil der Europäischen Datenstrategie ist. Sie halten ihre frühzeitige und stärkere Beteiligung in der europäischen und nationalen Datenschutz- und Digitalgesetzgebung für erforderlich, um die Praxistauglichkeit künftiger Digitalregulierung zu sichern.

(8) Bund und Länder sollten umgehend einen Diskurs über den institutionellen Ordnungsrahmen der EU-Digitalgesetzgebung aufnehmen. Klare Zuständigkeiten, handlungsfähige Aufsichtsstrukturen und effektive Abstimmungsprozesse sind eine notwendige Voraussetzung für eine zukunftsfähige und zukunftsorientierte Wirtschaft und Verwaltung.

(9) Die Entwicklung eines handlungsfähigen und effizienten institutionellen Ordnungsrahmen der EU-Digitalgesetzgebung fordert die für Digitalpolitik Verantwortlichen ebenso, wie diejenigen für Daten- und Verbraucherschutz, aber auch für Wirtschaft und nicht zuletzt Finanzen zuständigen Stellen und Gremien von Bund und Ländern. Bei der Einrichtung von Datenräumen etwa für Gesundheits- oder Mobilitätsdaten wird zusätzliche Expertise von Fachressorts und -gremien einzubeziehen sein. Insgesamt ist daher eine übergeordnete Koordinierung der nationalen Umsetzungsstrategie in Bund und Ländern geboten.

A. Datenökonomie und Künstliche Intelligenz als Taktgeber der Digitalen Transformation

Am 19. Februar 2020 hat die Europäische Kommission eine **Europäische Datenstrategie veröffentlicht**. Danach will sie die Menschen und ihre Grundrechte in den Mittelpunkt ihrer Strategie stellen und zugleich das wirtschaftliche

Potential von Daten und deren Nutzen für die Allgemeinheit schöpfen. Dies bezieht sich sowohl auf nicht personenbezogene als auch auf personenbezogene Daten. Ziel ist ein Binnenmarkt für Daten, der der Wirtschaft und dem Allgemeinwohl gleichermaßen dient. Die Kommission ist der Auffassung, dass ein europäischer Datenmarkt den Wohlstand in der Europäischen Union mehren könne. Zugleich sieht sie in Daten ein wichtiges Instrument für die politische Steuerung.

Im Unionsrecht sind mit dem Gesetz über Digitale Dienste, dem Gesetz über digitale Märkte und dem Data-Governance-Act wichtige legislative Ecksteine dieser Strategie bereits in Kraft getreten und verlangen heute nationale Umsetzungsschritte. Für andere ebenso zentrale Rechtsakte wie zum Datengesetz oder zur KI-Verordnung sind politische Einigungen bereits erzielt oder sollen alsbald erreicht werden. Zusammen mit weiteren wichtigen Bausteinen wie dem Verordnungsentwurf für einen Datenraum im Gesundheitswesen entsteht damit mittlerweile ein sehr deutliches Bild der künftigen europäischen Rahmenbedingungen für Datennutzung und Zukunftstechnologien auf Grundlage von Künstlicher Intelligenz.

All diese Regulierungskonzepte verbindet die klare Anforderung an die durch die Mitgliedstaaten zu bestimmenden Vollzugsbehörden, koordiniert und kooperativ für die kohärente Anwendung des neuen europäischen Datenrechtsrahmens Sorge zu tragen. Sämtliche bislang vorliegenden Rechtsakte oder Entwürfe erklären die mit der DS-GVO seit 25. Mai 2018 bestehenden Bestimmungen zum Schutz personenbezogener Daten für unberührt und enthalten Regelungen, die Schnittstellen der DS-GVO für nationale oder unionsrechtliche Spezifizierungen z. B. durch konkretisierte Rechtsgrundlagen nutzen. Entsprechendes gilt im Übrigen auch für die Anforderungen der e-Privacy-Richtlinie zum Schutz der Vertraulichkeit elektronischer Kommunikation.

Parallel zur europäischen und nationalen Rechtssetzung vollzieht sich tatsächlich bereits die Transformation zu einer Datenökonomie, zu datengetriebenen und auf der Nutzung Künstlicher Intelligenz aufbauenden Prozessen und Produkten in Unternehmen und Behörden und erreicht den Alltag der Bürgerinnen und Bürger.

Im Mittelpunkt dieser Transformationsprozesse muss der Schutz von Würde und Freiheit des Einzelnen stehen. Dies haben das Europäische Parlament, der Rat und die Kommission in ihrer gemeinsamen Erklärung vom 26. Januar 2022 zu den digitalen Rechten und Grundsätzen für die digitale Dekade bekräftigt (KOM (2022) 28 endg.). Den Datenschutzaufsichtsbehörden des Bundes und der Länder kommt bereits im Rahmen ihrer jeweiligen Zuständigkeiten die durch die EU-Grundrechtecharta vorgegebene Aufgabe zu, in der Digitalisierung und damit auch bei der Umsetzung der europäischen Datenstrategie den grundrechtlichen Schutz personenbezogener Daten zu überwachen.

B. Nationale Digitalstrategie – Umsetzung schon in Verzug

Die Datenschutzaufsichtsbehörden der Länder stellen fest, dass eine nachhaltige und umfassende Debatte über die nationale Umsetzung der EU-Datenstrategie und der mit ihr verknüpften Rechtsakte bislang weder im Bund noch in den Ländern eingeleitet wurde[1]. Obwohl der rasche Fortschritt der europäischen Gesetzgebungsverfahren und die dort im Interesse zukunftsfähiger Rahmenbedingungen richtigerweise vorgesehenen knappen Umsetzungsfristen für alle Adressaten – egal, ob Verantwortliche, nationale Gesetzgeber oder künftige Aufsichtsbehörden – Handlungsbedarf erzeugen, sind bisher zur Umsetzung der EU-Datenstrategie im nationalen Recht allenfalls punktuelle, reaktive Vorschläge vorgelegt worden. Um diese Gesetzesvorhaben in einem Bundesstaat von der Größe der Bundesrepublik, für Wirtschaft, Staat und Bürgerinnen und Bürger gewinnbringend und reibungslos umzusetzen, bedarf es indessen eines Gesamtkonzepts, das klug und vorausschauend sein sollte. Es sollte auf den bundesstaatlichen Verwaltungsstrukturen aufsetzen und nah an den Bedarfen dieser Akteure insbesondere Rechtssicherheit vermitteln. Soweit dabei personenbezogene Daten betroffen sind, tragen die Datenschutzaufsichtsbehörden der Länder ihre Expertise bei und legen dazu nachfolgend erste Vorschläge für ein Gesamtkonzept vor.

C. Handlungsfähige institutionelle Strukturen als Grundbedingung von Rechtssicherheit und Innovation, Akzeptanz und Vertrauen

Weder in der Daten- noch in der Digitalstrategie der Bundesregierung noch in den entsprechenden Programmen und Projekten der Länder finden sich bislang Zielsetzungen oder Maßnahmen, die die Bedeutung handlungsfähiger Behördenstrukturen für das Gelingen der EU-Digitalstrategie widerspiegeln. Ein klares Verständnis von Umfang und Zielen der Nutzung von Datenpotenzialen ist Grundvoraussetzung einer gelingenden Datenstrategie. Sie muss die Interessen von Bürgerinnen und Bürgern, Staat und Wirtschaft klar benennen und miteinander in Einklang bringen. Handlungsfähige institutionelle Strukturen sorgen dabei für eine erfolgreiche Umsetzung. Versäumnisse in der Vorbereitung der administrativen und organisatorischen Beratungs- und Kontrollstrukturen bedeuten absehbar, dass die Ausgestaltung neuer Datennutzungsprozesse oder der Einsatz Künstlicher Intelligenz in Behörden und Unternehmen ohne beratende Begleitung mit Rechtsunsicherheiten beginnen werden, die sich so nachhaltig zulasten von Innovation und Stärkung der europäischen Digitalwirtschaft auswirken können.

Besonders der Schutz der Grundrechte der Betroffenen, für die die Verarbeitung ihrer personenbezogenen Daten in einer Ökonomie des Datenteilens und vielfältiger Datennutzungsinteressen neue Risiken schafft, verlangt de-

1 solchen Verzug kritisiert etwa auch der Sachverständigenrat zur Begutachtung der gesamtwirtschaftlichen Entwicklung in seinem Jahresgutachten 2023/24 das für die Forschungsdatennutzung nachteilige Fehlen einer öffentlich finanzierten, nicht zugangsbeschränkte Plattform zur Datenübersicht, wie es der Data Governance Act als zentrale Informationsstelle bereits seit September 2023 verlangt; www.sachverstaendigenrat-wirtschaft.de/fileadmin/dateiablage/gutachten/jg202324/JG202324_Gesamtausgabe.pdf

ren Aufklärung, risikoadäquate Schutzmechanismen und wirksame Kontrolle durch unabhängige Aufsichtsbehörden. Handlungsfähige Aufsichtsstrukturen sind deshalb ebenso Grundbedingungen für Vertrauen und Akzeptanz, mithin für den Erfolg des europäischen Datenmarktes im Alltag der Bürgerinnen und Bürger. Dies ist angesichts fortschreitenden Einsatzes Künstlicher Intelligenz in Unternehmen und Behörden längst überfällig.

Anders als etwa bei Verabschiedung der Datenschutz-Grundverordnung bestehen für die Rechtsakte der EU-Digitalstrategie in ihren Kernbereichen - wie etwa der Prüfung und Überwachung von KI-Produkten - bislang keine umfassenden Vollzugsstrukturen, auf denen ein nationales Umsetzungskonzept aufbauen könnte. Auch für die in den europäischen Datennutzungsregelungen festgelegten Aufgaben nationaler Behörden zur Mitwirkung an einer unionsweiten Kooperation und zur Gewährleistung einheitlicher Rechtsdurchsetzung fehlen geeignete Vorbilder und Modelle.

Im Hinblick auf ihre jeweiligen Zuständigkeiten für die Gesetzgebung und den Gesetzesvollzug sind daher Bund und Länder gemeinsam gefordert, unverzüglich Analysen und Bewertungen ihrer mit den EU-Digitalrechtsakten verknüpften Handlungserfordernisse vorzunehmen, um schnellstmöglich ein Gesamtkonzept der künftigen Vollzugsverantwortlichkeiten und dringlichsten Vorbereitungsmaßnahmen zu entwickeln und umzusetzen.

D. Herausforderungen bei der Umsetzung der EU-Digitalstrategie

1) Aus Sicht der Datenschutzaufsichtsbehörden der Länder ergeben sich mit den Rechtsakten zur Umsetzung der EU-Datenstrategie in vielfacher Hinsicht Überschneidungen zu bereits bestehenden Verwaltungsaufgaben, die von den Ländern ausgeführt werden. Soweit die Umsetzung der Datenstrategie auch personenbezogene Daten erfasst, berührt dies zwangsläufig die Aufgaben der Datenschutzaufsichtsbehörden. Aber auch andere Landesbehörden sind in ihren Aufgaben betroffen, etwa die Medienaufsicht, der Verbraucherschutz, die Marktaufsicht und auch die Fachverwaltungen mit Bezug zu den EU-Datenräumen (s. o. aktuell Gesundheitsdatenraum, Mobilitätsdatenraum).

Ungeachtet dessen sind aus Sicht der Datenschutzaufsichtsbehörden der Länder in zahlreichen rechtspolitischen Äußerungen Bestrebungen wahrnehmbar, Aufsichtsstrukturen beim Bund zu zentralisieren. Wenn die neuen EU-Rechtsakte eine national koordinierende Behörde als zentrale Kontaktstelle für die europäische Koordinierung vorsehen, dann bedeutet dies freilich nicht, dass dazu innerstaatliche Zuständigkeiten zwangsläufig zentralisiert werden müssten. Die in der Bundesrepublik Deutschland verfassungsrechtlich determinierte und in der Praxis bewährte Ausführung von Gesetzen durch die Länder bleibt sinnvoll, unabhängig davon, ob Bundesgesetze oder

europäische Verordnungen ausgeführt werden. Weder gibt Art. 87 GG verfassungsrechtliche Spielräume, noch bestehen hinreichende, rechtspolitisch überzeugende sachliche Gründe die seit Jahrzehnten eingeübte Bund-Länder-Koordination durch eine vermeintlich effektivere Zentralisierung von Aufgaben beim Bund zu ersetzen. Jedenfalls dort, wo eine Aufgabenzentralisierung in ihrer praktischen Umsetzung eine Vielzahl von Abstimmungserfordernissen mit den Datenschutzaufsichtsbehörden der Länder zwangsweise und einzelfallbezogen erzeugen würde, sollte sie unterbleiben.

Die wirkliche Stärke des Föderalismus besteht aus Sicht der Datenschutzaufsichtsbehörden der Länder in diesem Zusammenhang darin, dass einzelne Länder etwa mit guten Beispielen vorangehen können. So gefundene und erprobte Lösungen können von anderen genutzt oder gemeinsam fortentwickelt werden. Komplexe und schwierige Aufgaben, die aus der Digitalstrategie erwachsen, können dabei auf mehrere Schultern verteilt sowie wechselseitig qualitätsgesichert werden. Die föderalen Aufsichtsstrukturen zeichnen sich zudem durch Bürger*innennähe aus und antworten damit gerade im Datenschutz, weit besser als zentrale Strukturen, auf das Gebot größtmöglicher Nähe und Effektivität für Betroffene. Föderale Strukturen stellen auch sicher, dass die in der DSGVO genauso wie in den anstehenden Digitalrechtsakten deutlich erweiterten behördlichen Entscheidungs- und Sanktionsbefugnisse in den kleinsten möglichen Einheiten verbleiben, um die Partizipation und Nachvollziehbarkeit zu sichern und gerade in Ansehung der völligen Unabhängigkeit der Datenschutzaufsichtsbehörden unverhältnismäßigen Beschränkungen parlamentarischer Kontrolle entgegenzuwirken. Im Föderalismus kann überdies zielgenauer und agiler auf regionale Besonderheiten der Wirtschaft eingegangen und passgenau reagiert werden.

2) Statt durch den Aufbau neuer zusätzlicher Behördenstrukturen zur Aufsicht und Kontrolle der EU-Digitalrechtsakte sind die unionsrechtlichen Anforderungen an eine umfassende Überwachung und deren einheitliche Anwendung aus Sicht der Datenschutzaufsichtsbehörden der Länder durch effektive und rechtssichere Regelungen der Zusammenarbeit, des Informationsaustauschs und der Abstimmung zu bewältigen. Dies ist notwendig, um das föderale Aufsichtssystem an ein europäisches Koordinierungssystem unabhängiger Aufsichtsbehörden reibungslos anzuschließen. Wie kaum andere verfügen die Datenschutzaufsichtsbehörden bereits jetzt über erprobte Expertise im Dialog mit anderen Regulierungsbehörden. Dies zeigt sich in der direkten Koordinierung mit anderen europäischen Aufsichtsbehörden im Einzelfall, in der Bund-Länder Koordinierung an der Schnittstelle zum Europäischen Datenschutzausschuss sowie auf der Ebene der rein nationalen Koordinierung etwa bei der Mitwirkung in Verfahren des Bundeskartellamts. Diese Erfahrungen und Kompetenzen der Datenschutzaufsichtsbehörden sollten bei der konzeptionellen Ausrichtung der nationalen Zustän-

digkeitsordnung für die Umsetzung der Europäischen Datenstrategie unbedingt genutzt und berücksichtigt werden.

3) Vor diesem Hintergrund sind aus Sicht der Datenschutzaufsichtsbehörden in besonderer Weise die Länder gefordert: Diese sind dringend gehalten, sich konzeptionell zu den Chancen und Risiken der Europäischen Datenstrategie zu positionieren, ihre Verantwortung für deren Umsetzung anzunehmen und haushaltsrechtlich durch klare Priorisierung von Ressourcen zu dokumentieren. Weder eine datenschutzgerechte Datenökonomie noch vertrauenswürdige und beherrschbare Künstliche Intelligenz können ohne leistungsfähige, aufgabengerecht ausgestattete Datenschutzaufsichtsbehörden gelingen. Nichts anderes gilt für eine bürger*innennahe und an den örtlichen Bedürfnissen orientierte problembewusste Verwaltung, die leistungsfähige Beratung ratsuchender Unternehmen oder zielgerichtete Begleitung regionaler Innovationstreiber. Weiteres Abwarten oder Zögern bedeutet daher, die Chancen für Akzeptanz und Vertrauen, Rechtssicherheit und Innovationsfähigkeit, die die Datenökonomie und der Einsatz Künstlicher Intelligenz bietet, auf Spiel zu setzen.

4) Angesichts knapper Umsetzungsfristen und vielschichtiger Aufgabenstellungen der nationalen Gesetzgeber und Regierungen besteht aus Sicht der Datenschutzaufsichtsbehörden der Länder deshalb dringender Abstimmungs- und Entscheidungsbedarf.

E. Vorschläge zur Entwicklung eines institutionellen Ordnungsrahmen in der nationalen Digitalstrategie

Ungeachtet aller neuen Fragestellungen, die die Regulierung der Datenökonomie und erst Recht die Entwicklung und Nutzung Künstlicher Intelligenz mit sich bringen, kann und sollten sich Konzepte für einen institutionellen Rahmen am Ziel schnellstmöglicher Handlungsfähigkeit ausrichten. Handlungsfähige, mit klar abgegrenzten Kontrollaufgaben betraute Institutionen können der Dynamik der technologischen und wirtschaftlichen Entwicklung gerecht werden, verlässliche Rahmenbedingungen für Betroffene und Unternehmen bieten und in den europäischen und globalen Debatten frühzeitig und klar wahrnehmbar für Deutschland Position beziehen.

Für ein gemeinsames Konzept von Bund und Ländern zur Entwicklung eines institutionellen Ordnungsrahmens in der nationalen Digitalstrategie unterbreiten die Datenschutzaufsichtsbehörden der Länder daher folgende Vorschläge:

1) Fortentwicklung statt Umbau nationaler Zuständigkeitsstrukturen

Weder ein grundlegender Umbau bestehender Behördenstrukturen noch der Aufbau neuer, ggf. zentraler Strukturen werden dem vordringlichen Erfordernis handlungsfähiger institutioneller Strukturen als Grundbedingung von Rechtssicherheit und Innovation für Unternehmen sowie von Akzeptanz und Vertrauen der Bürgerinnen und Bürger gerecht. Der institutionelle Ordnungsrahmen einer nationalen Digitalstrategie sollte sich an vorhandenen Strukturen ausrichten und die Möglichkeiten ihrer Fortentwicklung ausschöpfen, statt neue Verwaltungsstrukturen zu entwickeln und langwierige Aufbauprozesse anzustoßen. Dies schließt nicht aus, im Einzelfall dort im Rahmen der verfassungsrechtlichen Kompetenzzuweisungen neue Aufsichtsinstitutionen zu entwickeln, wo die vorhandenen Kompetenzen neuen Aufgaben bei der Regulierung digitalen Transformationsprozesse nur unzureichend gerecht werden.

Beim Schutz personenbezogener Daten ordnet die Grundrechtecharta eine unabhängige Aufsicht an, die besondere Bedingungen verlangt, die heute bereits durch die Datenschutzaufsichtsbehörden gewährleistet werden.

2) Kooperationsregelung als Bindeglied unterschiedlicher Zuständigkeitsbereiche und – ebenen

Aus Sicht der Datenschutzaufsichtsbehörden der Länder besteht eine der Schlüsselaufgaben bei der Entwicklung des institutionellen Ordnungsrahmens für die nationale Datenstrategie in der effizienten Ausgestaltung der Kooperationsbeziehungen der jeweils zuständigen Behörden. Kooperation gewährleistet umfassende Sachkompetenz, die notwendige Sachnähe und sichert die rechtsstaatlich gebotene Abstimmung bei der Beurteilung einheitlicher Lebensvorgänge durch Behörden unterschiedlicher Aufgabenbereiche. Die Effizienz ihrer Aufgabenwahrnehmung wird durch Mehrfachzuständigkeiten oder künstliche Schnittstellen in Frage gestellt.

Im Bereich der Datenschutzaufsicht bestehen hierzu jedenfalls zu einzelnen Bereichen wie den Wettbewerbsbehörden bereits erste, zuletzt durch den EuGH in seinem Urteil vom 4. Juli 2023 bestätigte Erfahrungen. Die vom EuGH auf Grundlage des unionsrechtlichen Grundsatzes der loyalen Zusammenarbeit für grenzüberschreitende Sachverhalte konkretisierten Leitlinien der Kooperation zwischen Datenschutzaufsichtsbehörden und anderen Aufsichtsbehörden können ohne Abstriche auch für die Ausgestaltung der Zusammenarbeit unterschiedlicher Bundes- oder Länderbehörden, etwa zwischen Datenschutzaufsichtsbehörden und anderen Aufsichtsbehörden (bspw. Bundesnetzagentur oder BaFin) in Fragen des Schutzes personenbezogener Daten herangezogen werden.

Eine solche Regelung über Zusammenarbeitsbefugnisse, gegenseitige Informationspflichten bis hin zu Abstimmungs- und Beteiligungserfordernissen,

dient nicht nur der Gewährleistung der Überwachung des Schutzes personenbezogener Daten durch die mit Erfahrung und Expertise ausgestatteten unabhängigen Aufsichtsbehörden, sie sichert auch entsprechend der Zielvorgabe des Art. 51 Abs. 2 DS-GVO die einheitliche Anwendung europäischen Datenschutzrechts. Insoweit kann eine solche Kooperationsregelung daher auch einen Eckpfeiler für die Gewährleistung der künftig geforderten einheitlichen Anwendung der Digitalrechtsakte bilden.

Eine breit ausgestaltete Regelung der Kooperationsbeziehungen entlang dieser unionsrechtlichen Zielsetzungen ist zudem geeignet, Schnittstellen der verschiedenen Rechtsakte zwischen Anforderungen an den Schutz personenbezogener und nicht-personenbezogener Daten oder zwischen Zertifizierung und Marktüberwachung von Innovatoren und Anbietenden von KI-Produkten einerseits und deren Anwendung durch Unternehmen und Behörden andererseits im Interesse effizienter und einheitlicher Rechtsdurchsetzung rechtssicher einzugrenzen. Sie kann gewährleisten, dass im Unionsrecht vorgesehene Verpflichtungen zur Koordinierung mehrerer nach nationalem Recht zuständiger Behörden (etwa Art. 31 Abs. 4 Data Act) im Interesse einheitlicher Ansprechpartner der Mitgliedstaaten ohne Eingriffe in nationale Zuständigkeitsstrukturen gerade bei multi- oder interdisziplinären Vollzugsaufgaben gewahrt werden.

Wesentliche Regelungsgegenstände einer solchen letztlich bereits vom EuGH skizzierten Zusammenarbeit zwischen Datenschutzaufsichtsbehörden und anderen Regulierungsbehörden sind insbesondere

- die Bedingungen für einen unkomplizierten des Daten- und Informationsaustauschs,
- der zu nutzenden informationstechnischen Systeme,
- die Behandlung von Beschwerden, welche verschiedene Überwachungs-zuständigkeiten betreffen,
- schlanke Abstimmungs- und Beteiligungsverfahren.

Eine solche Kooperationsregelung sollte als wesentliche Bestimmung der Aufgabenerfüllung unabhängiger Aufsichtsbehörden und ggf. der Bund-Länder-Zusammenarbeit im Bundesrecht getroffen werden und könnte als horizontale Bestimmung z.B. schon im laufenden Gesetzgebungsverfahren zur Änderung des Bundesdatenschutzgesetzes berücksichtigt werden. Die aus Sicht der Datenschutzaufsichtsbehörden der Länder im Rahmen der gesetzlichen Ausgestaltung der Datenschutzkonferenz zu ergänzende Geschäftsstelle[2] kann als wichtiger Anknüpfungspunkt für die praktische Durchführung solcher Kooperationsverfahren genutzt werden. Sie kann etwa schon

2 Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 6. September 2023 zum Entwurf eines Ersten Gesetzes zur Änderung des Bundesdatenschutzgesetzes mit Stand 9.8.2023

mit geringen Ressourceneinsatz zu einer für alle Kooperationsbeziehungen wichtigen Schnittstelle für den Daten- und Informationsaustausch ausgestaltet oder zu Bereitstellung der dafür zu nutzenden informationstechnischen Systeme befähigt werden, wie sie durch die Rechtsakte der Digitalstrategie zwischen Fachbehörden und Datenschutzaufsicht oder etwa auch in Umsetzung der NIS 2-Richtlinie[3] bei der Bearbeitung von Cybersicherheitsvorfällen erforderlich wird.

3) Expertise der Datenschutzaufsichtsbehörden bei der Umsetzung der Digitalstrategie nutzen

a) europäische und nationale Gesetzgebung

Art. 57 Abs. 1c) DSGVO weist den Datenschutzaufsichtsbehörden die Aufgabe zu, „im Einklang mit dem Recht des Mitgliedsstaats das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung (zu) beraten".

Aus Sicht der Datenschutzaufsichtsbehörden der Länder zeigen insbesondere die Rechtsetzungsverfahren zur EU-Digitalstrategie Defizite und Verbesserungsbedarf bei der nationalen Umsetzung, insbesondere der Ausgestaltung der für die Wahrnehmung dieser Aufgabe bestimmenden Regelungen und Prozesse des Bundes und der Länder auf. Es fehlen für die Wahrnehmung dieser Aufgabe substantielle Grundbedingungen, z. B.

- kontinuierliche Informationen der Aufsichtsbehörden über Beratungsprozesse in den EU-Gremien (z. B. in Form des Zugangs zu Ratsdokumenten),
- die frühzeitige Beteiligung der Aufsichtsbehörden der Länder mit ihrer Vollzugserfahrung durch die Bundesregierung zu Referentenentwürfen der Bundesregierung, die den Schutz personenbezogener Daten betreffen
- und die anschließende Beteiligung durch die Landesregierungen in Bundesratsangelegenheiten.

Die bisher etablierte Beteiligung des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in der europäischen und nationalen Datenschutz- und Digitalgesetzgebung kann und wird diese Defizite nicht in hinreichender Weise kompensieren. Die umfassenden Vollzugserfahrungen und die darauf aufbauende praktische Expertise der Datenschutzaufsichtsbehörden der Länder ist für die Entwicklung einer optimalen Umsetzungsstrategie unverzichtbar.

3 vgl. z.B. Art. 31 Abs. 3 oder Art. 35 RL (EU) 2022/2555;"

Die Datenschutzaufsichtsbehörden der Länder halten daher sowohl gesetzliche als untergesetzliche bzw. organisationsrechtliche Anpassungen des Bundes und der Länder zu ihrer stärkeren Beteiligung in der europäischen und nationalen datenschutz- und Digitalgesetzgebung für erforderlich. So wird die Praxistauglichkeit künftiger Digitalregulierung gesichert. Auf Grundlage besserer Informationen über die künftige Rechtslage können sie ihre Beratung von Unternehmen und Behörden über Anpassungserfordernisse frühzeitiger und zielgenauer ausrichten.

Das Ziel müssen gute Gesetze sein. Gute Gesetze sind praxistaugliche Gesetze, die auf Grundlage von Erfahrungen aus dem Verwaltungsvollzug effizient und rechtssicher angewendet werden können.

b) staatliche Gremien und staatlich geförderte zivilgesellschaftliche Strukturen

Die Datenschutzaufsichtsbehörden der Länder halten es für erforderlich, die Ausrichtung bzw. Zusammensetzung der zur Begleitung der Digitalen Transformation neu geschaffenen Gremien des staatlichen Bereichs und öffentlicher Institutionen wie etwa Räte oder Beiräte zur Förderung und Begleitung des Einsatzes Künstlicher Intelligenz[4] zu überprüfen. Entsprechendes gilt für staatlich geförderte zivilgesellschaftlicher Strukturen[5], die auf verschiedenen Ebenen eingerichtet wurden, um die gesellschaftlichen Debatten über Digitale Transformation, insbesondere die Chancen und Risiken der Nutzung Künstlicher Intelligenz aber auch einer Datenökonomie zu sensibilisieren und zu begleiten.

Bei der Mehrzahl dieser Gremien ist trotz der unabweisbaren Wechselwirkungen ihrer Beratungs- und Förderungsaufgaben mit Fragen des Schutzes personenbezogener Daten eine Einbindung der Datenschutzaufsichtsbehörden weder vorgesehen noch praktiziert. Um Fragen des Schutzes personenbezogener Daten von Anfang an in den solchen Gremien übertragenen Handlungsempfehlungen oder Vermittlungsstrategien zur Umsetzung der Digitalstrategie zu berücksichtigen, sollte die Expertise der Datenschutzaufsichtsbehörden stärker genutzt werden. Dazu sollten künftig Vertreterinnen und Vertreter der Datenschutzaufsichtsbehörden als ständige Mitglieder, jedenfalls aber im Rahmen von Beiräten oder als anlassbezogen einbezogene Sachverständige bei der Schaffung staatlicher oder staatlich geförderter zivilgesellschaftlicher Gremien zur Begleitung und Umsetzung der Digitalstrategie einbezogen werden.

4 Z.B. den Bayerischen KI-Rat, Staatsregierung etabliert hochkarätig besetzten KI-Rat (bayern.de)
5 Z.B. das vom BMV geförderte Zentrum für vertrauenswürdige Künstliche Intelligenz (ZVKI), ZVKI | Über Uns

4) Mehr-Ebenen-Prozess zur Umsetzung und Begleitung der Daten- und Digitalstrategie

Die Datenschutzaufsichtsbehörden der Länder halten es für dringend erforderlich, dass Bund und Länder umgehend einen Diskurs über den institutionellen Ordnungsrahmen der EU-Digitalgesetzgebung aufnehmen. Ziel muss es sein, abgestimmt Anforderungen und Handlungserfordernisse zu analysieren und wechselseitige Aufgaben zu klären, um zeitnah handlungsfähige Strukturen zu schaffen, die praxisnahe Beratung und Rechtssicherheit gewährleisten. Klare Zuständigkeiten und Aufsichtsstrukturen, die abgestimmten Vorgaben führen, sind eine notwendige Voraussetzung für eine zukunftsfähige und zukunftsorientierte Wirtschaft und Verwaltung.

Dieser Prozess der Analyse und Festlegung von Umsetzungsverantwortlichkeiten berührt gleichermaßen die für Digitalpolitik Verantwortlichen wie die für Daten- und Verbraucherschutz Verantwortlichen, aber auch die für Wirtschaft und nicht zuletzt Finanzen zuständigen Stellen und Gremien von Bund und Ländern. Die Datenschutzaufsichtsbehörden der Länder bieten allen an diesem Diskussionsprozess Beteiligten ihre Unterstützung an, um mit ihren tagtäglichen Erfahrungen in der Anwendung und Durchsetzung europäischen Datenschutzrechts im Verhältnis zu Betroffenen, Behörden und Unternehmen die dringend notwendigen Weichenstellungen für einen institutionellen Ordnungsrahmen in der nationalen Digitalstrategie zu begleiten.

16.2. Veröffentlichungen der Datenschutzkonferenz

Alle Veröffentlichungen der Datenschutzkonferenz sind auf der Website der Datenschutzkonferenz www.datenschutzkonferenz-online.de abrufbar

Entschließungen der Datenschutzkonferenz

Mit Entschließungen nimmt die Datenschutzkonferenz zu datenschutzpolitischen Fragen öffentlich Stellung. Entschließungen werden sowohl in den Konferenzen, als auch zwischen den Konferenzen gefasst.

22./23.11.2023 – Rahmenbedingungen und Empfehlungen für die gesetzliche Regulierung medizinischer Register

Das Vorhaben der Bundesregierung, für die ausgesprochen heterogene Vielfalt medizinischer Register einen allgemeinen Rahmen und eine einheitliche Basis zu schaffen, um Daten im öffentlichen Interesse nutzen zu können, ist aus datenschutzrechtlicher Perspektive nachvollziehbar. Allerdings muss sichergestellt sein, dass auch im konkreten Anwendungsfall die datenschutzrechtlichen Vorgaben eingehalten werden und das Grundrecht auf Datenschutz stets gewährleistet ist. Sowohl für die Befüllung der Register als auch für die registerinterne Verarbeitung und die Bereitstellung sowie die mögliche Nutzung der Daten durch Dritte sind die spezifischen datenschutzrechtlichen Voraussetzungen für die Verarbeitung von Gesundheitsdaten, insbesondere aus Art. 9, 25, 32 und ggf. Art. 89 Abs. 1 DSGVO, maßgeblich.

Es gibt eine Vielzahl medizinischer Register in Deutschland in unterschiedlichen Strukturen und Formen. Wenige sind spezialgesetzlich geregelt oder basieren auf allgemeinen gesetzlichen Grundlagen. Die meisten stützen sich zur Datenverarbeitung auf Einwilligungen: verschiedene stammen aus abgeschlossenen Forschungsvorhaben, andere werden auf Patienteninitiative oder von Fachgesellschaften zu bestimmten Erkrankungen betrieben; nicht alle werden noch aktiv genutzt.

Anknüpfend an die Festlegungen im Koalitionsvertrag „Mehr Fortschritt wagen“ vom November 2021 (S. 83), wonach neben einem Gesundheitsdatennutzungsgesetz auch ein Registergesetz im Einklang mit der DSGVO geschaffen werden soll, sieht die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Anlass, ergänzend zu ihren bisherigen Forderungen und Empfehlungen die datenschutzrechtlichen Anforderungen und Bedingungen für die Regulierung einer Datenverarbeitung in medizinischen Registern zu präzisieren. Soweit die Datenverarbeitung den Zwecken wissenschaftlicher Forschung dient, gelten daneben die Hinweise in der „Petersberger Erklärung“ der DSK aus dem November 2022 (Entschließung der DSK „Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung“ vom 24. November 2022).

Die DSK begrüßt, dass durch das vom Bundesministerium für Gesundheit (BMG) beauftragte Gutachten zur Weiterentwicklung medizinischer Register (Gutachten zur Weiterentwicklung medizinischer Register zur Verbesserung der Dateneinspeisung und -anschlussfähigkeit, TMF – Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. und BQS – Institut für Qualität und Patientensicherheit, 29. Oktober 2021) ein nahezu vollständiger Überblick über die vorhandenen Register und die darin enthaltenen Daten vorliegt (Unter dem Link: www.registersuche.bqs.de/search.php sind ca. 400 Register gelistet). Zugleich schließt sich die DSK der darin enthaltenen Empfehlung an, durch die nun geplante Gesetzgebung ein entsprechendes Registerverzeichnis zu verstetigen und dauerhaft öffentlich zugänglich zu gestalten. Die DSK befürwortet insbesondere die Überlegungen zur Schaffung einer Zentralstelle für medizinische Register, die das Registerverzeichnis führen und die eine Auditierung und Zuordnung medizinischer Register je nach vorhandener Qualitätsstufe (im Gutachten als „Reifegrad" bezeichnet) verantworten soll. Aufgrund der Aufgaben der Zentralstelle für medizinische Register, die maßgeblich für die weitere Verarbeitung der in den medizinischen Registern enthaltenen Daten sind, hält es die DSK für geboten, hiermit eine unabhängige Körperschaft des öffentlichen Rechts zu betrauen. Dieser Zentralstelle könnte zudem eine besondere Funktion als Ansprechpartner und Lotse für die betroffenen Personen sowie bei der Erfüllung der Betroffenenrechte zukommen.

Die DSK teilt das aus dem Koalitionsvertrag erkennbare Anliegen, durch die gesetzliche Regelung die bislang heterogene Registerlandschaft zu strukturieren und zum Aufbau fachlich qualitätsgesicherter Register beizutragen. Entsprechend den Ausführungen im Gutachten bietet es sich an, bei der Zuordnung der Register je nach Qualitätsstufe zu verschiedenen Kategorien die Datenqualität, die Datenstruktur und die Standards bei der Verarbeitung zu berücksichtigen.

Insbesondere folgende Rahmenbedingungen sind aus datenschutzrechtlicher Sicht bei der gesetzlichen Regulierung medizinischer Register vorzusehen:

- Werden personenbezogene Daten an die Register übermittelt und von diesen erhoben, die nicht unmittelbar für das Register, sondern zu einem anderen Zweck erhoben worden sind, bedarf es hierfür – soweit dies nicht durch Einwilligungen gedeckt ist – klarer gesetzlicher Festlegungen zu den Voraussetzungen der zweckändernden Datenverarbeitung, die den Anforderungen aus Art. 6 Abs. 4 DSGVO entsprechen.

- Es sind rechtsklare und verhältnismäßige Regelungen über die Aufbewahrungsdauer und Löschfristen der Registerdaten unter der Maßgabe der Grundsätze der Datenminimierung und Speicherbegrenzung zu treffen.

- Eine Befugnis zur Übermittlung von personenbezogenen Gesundheitsdaten an das Register, zu deren Speicherung im Register sowie zu deren Übermittlung an Dritte unter Verzicht auf eine vorherige Einbindung der betroffenen Person bedarf mindestens der medizinisch-fachlichen Erforderlichkeit für einen der in Art. 9 Abs. 2-4 DSGVO genannten Zwecke, der gesetzlichen Definition der zu verarbeitenden personenbezogenen Daten und bei Forschungszwecken dienenden Registern eines allgemeinen, voraussetzungslosen Widerspruchs-rechts.

- Bei der Festlegung von Voraussetzungen für eine datenschutzkonforme Verarbeitung von Registerdaten, insbesondere den Anforderungen für die Übermittlung an und Erhebung durch die Register, die weitere Verarbeitung der Daten in den Registern und deren Bereitstellung für Dritte, sowie einer Definition der zu verarbeitenden Einzelangaben, sind außer den Maßgaben der Öffnungsklauseln nach Art. 9 Abs. 2 DSGVO und ggf. den Garantien nach Art. 89 Abs. 1 DSGVO auch die Vorgaben des Grundrechts auf Datenschutz zu berücksichtigen. Insbesondere müssen sich wesentliche Grundrechtseinschränkungen unmittelbar aus dem Gesetz ergeben.

- Bei den gesetzlichen Regelungen sollte die Rechtmäßigkeit der Datenverarbeitung abhängig von dem jeweiligen Zweck differenziert festgelegt werden. Eine Nutzung zur wissenschaftlichen Forschung erfordert beispielsweise andere Bedingungen als eine Auswertung zu Zwecken einer – gesetzlich jeweils näher zu bezeichnenden – Qualitätssicherung. Dies muss berücksichtigt werden.

- Die DSK hält es für erforderlich, dass mit der gesetzlichen Regulierung der medizinischen Register auch Vorgaben zu technisch-organisatorischen Maßnahmen standardisiert und harmonisiert festgelegt werden. Damit wird das dem Risiko angemessene Schutzniveau für die Verarbeitungen verdeutlicht und eine effektive Datenschutzaufsicht ermöglicht. Insbesondere bei besonderen Risiken, wie zum Beispiel einem Remotezugriff auf Gesundheitsdaten über digitale Portale, wird dem Gesetzgeber empfohlen, im Rahmen einer sog. gesetzlichen Datenschutz-Folgenabschätzung (DSFA) globale Risiken der Registersysteme zu ermitteln und so geeignete technische und organisatorische Maßnahmen zur Minimierung dieser Risiken bereits im Gesetz zu regeln. Dies kann die Verantwortlichen zwar nicht vollständig von einer eigenen DSFA entlasten, trägt aber zur Schaffung einheitlicher Mindeststandards bei.

- Die DSK empfiehlt, durch die gesetzlichen Regelungen digitale Methoden u.a. für das Einwilligungsmanagement und die Ausübung der Betroffenenrechte zu fördern sowie – beispielsweise durch Portale – eine Partizipation der Betroffenen zu ermöglichen.

- Die DSK hält es grundsätzlich für tragfähig, für qualitätsgesicherte Register ein Zulassungsverfahren vorzusehen mit dem Ziel, dass für bestimmte im Registerverzeichnis entsprechend gelistete Register bestehende oder noch zu schaffende gesetzliche Datenverarbeitungsbefugnisse herangezogen werden können. Dabei ist hinsichtlich der einzelnen Verarbeitungsschritte der Übermittlung an das Register, der Erhebung und der Bereitstellung der Daten durch das Register sowie der Verwendung bei der weiteren Nutzung der Registerdaten zu differenzieren.

- Für die Register sollten regelmäßig unabhängige Vertrauensstellen vorgesehen werden. Diese könnten eine zentrale Rolle bei der Anonymisierung und Pseudonymisierung von Gesundheitsdaten vor der Bereitstellung für Forschende und bei der Verwaltung bereichsspezifischer Kennzeichen als einheitliche Identifikatoren spielen.

- Im Zulassungsverfahren sollten relevante Aspekte des Datenschutzes (z. B. die Rechtsgrundlagen und die Gewährleistung der Betroffenenrechte) und der Informationssicherheit geprüft werden. Die DSK empfiehlt, die Festlegung des Zulassungsverfahrens mit ihr abzustimmen, um die technisch-organisatorischen Maßnahmen und die datenschutzrechtlichen Prinzipien – wie Verschlüsselung, Pseudonymisierung, Erforderlichkeitsgrundsatz, Anonymisierung, Nutzung synthetischer Daten – bei der Datenerhebung, bei der Verarbeitung innerhalb des Registers und bei der Bereitstellung der Daten durch das Register zu gewährleisten. Zugleich sollte für die Zulassung ein Verfahren vorgesehen werden, mit dem die Einhaltung der Qualitätsstandards sowie die Angemessenheit des Schutzniveaus in regelmäßigen Abständen wiederholt geprüft und nachgewiesen wird.

- Im Zulassungsverfahren sollten auch das Verfahren, das Schutz- und Vertrauensniveau der Schnittstellen und die Voraussetzungen geprüft werden, mit denen ein Register Daten an Dritte bereitstellt oder übermittelt. Nutzungsanträge und -bewilligungen sollten aus Transparenzgründen vom Register und von der für den Nutzungsantrag zuständigen Stelle veröffentlicht werden.

- Zur Verminderung von Risiken und zur datenschutzkonformen Auswertung von Daten sollte in der gesetzlichen Regelung die Nutzung geeigneter technischer und organisatorischer Methoden einschließlich der dezentralen Speicherung und Verarbeitung gefordert werden.

- Es wird empfohlen, gesetzlich festzulegen, welche datenschutzrechtliche Rolle den beteiligten Stellen für welche Verarbeitungsvorgänge zukommt, d. h. ob eine eigene oder gemeinsame Verantwortlichkeit oder eine Auftragsverarbeitung vorliegt.

- Der datenschutzrechtliche Grundsatz der Zweckbindung nach Art. 5 Abs. 1 lit. b DSGVO steht der Verknüpfung von Datensätzen grundsätzlich entgegen. Sofern für Zwecke der wissenschaftlichen Forschung Datensätze verknüpft werden sollen, bedarf es im Hinblick auf das Grundrecht auf Datenschutz einer besonderen Rechtfertigung, die sich in der Regel aus einem öffentlichen Interesse und einem gesellschaftlichen Nutzen ergeben soll. Wegen der sich aus einer Verknüpfung ergebenden Risiken sollte sie nur anlassbezogen und temporär zulässig sein.

- Bei der Verwendung einheitlicher Identifikatoren sollten bereichsspezifische Kennzeichen eingesetzt werden. Im Bereich der Datenverarbeitung durch medizinische Register wäre ein spezifisches datenschutzfreundliches Identifikationssystem für den Gesundheitsbereich denkbar: So könnten beispielsweise aus einer bereits vorhandenen Krankenversichertennummer nicht rückrechenbare, bereichsspezifische Pseudonyme für die Register jeweils gesondert durch geschützte Verfahren gebildet und gespeichert werden, die sich nur über eine zentrale Vertrauensstelle zuordnen ließen. Soweit die Zentralstelle für medizinische Register auch datenschutzrechtliche Aspekte prüft, sollte das Verhältnis zu den Datenschutzaufsichtsbehörden unter Beachtung der Vorgaben der DSGVO gesetzlich geklärt werden.

23.11.2023 – Datenschutz in der Forschung durch einheitliche Maßstäbe stärken

Medizinische Forschungsprojekte werden in Deutschland häufig nicht nur in einem Bundesland durchgeführt. Vielmehr sind zunehmend verschiedene Forschungseinrichtungen aus unterschiedlichen Ländern daran beteiligt (z. B. länderübergreifende Verbundforschung, multizentrische Studien). Je nach Forschungsstandort sind unterschiedliche datenschutzrechtliche Anforderungen zu beachten. Dies erschwert nicht nur die Forschung, sondern wirkt sich auch nachteilig auf den Datenschutz für die betroffenen Personen aus. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Bundesgesetzgeber und die Landesgesetzgeber daher auf, durch aufeinander abgestimmte gesetzliche Regelungen auf hohem Datenschutzniveau den Datenschutz in der länderübergreifenden Forschung zu stärken. Hierfür hat sie Eckpunkte erarbeitet. Im Einzelnen:

In vielen Ländern enthalten verschiedene Landesgesetze, die beispielsweise die Datenverarbeitungen durch Krankenhäuser und Behörden des öffentlichen Gesundheitsdienstes betreffen, konkrete Befugnisse der jeweiligen Stellen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken, die den allgemeinen Vorgaben vorgehen. Diese gesetzlichen Regelungen stellen unterschiedliche datenschutzrechtliche Anforderungen. Bei länderübergrei-

fender Forschung müssen von den Verantwortlichen die jeweils für sie geltenden Gesetze angewandt werden. Unterschiede bestehen insbesondere in Bezug auf die Zulässigkeit der Datenverarbeitung (gesetzliche Grundlage oder Einwilligung mit jeweils unterschiedlichen Anforderungen), die Definition von Schutzbereichen (u. a. Patientinnen und Patienten, Angehörige) und zulässige Zwecke der Verarbeitung. Die rechtliche Bewertung und Umsetzung der jeweils geltenden Rechtsgrundlage führte in der Vergangenheit zu einem gesteigerten Beratungsbedarf und zu Unsicherheiten bei den Forschenden und Rechtsanwendern. Auch ergeben sich aus unterschiedlichen Regelungen Herausforderungen für eine transparente und verständliche Informationserteilung nach Artikel 13 und 14 der Datenschutz-Grundverordnung (DSGVO).

Das Bundesgesundheitsministerium hat mit dem Gesetzentwurf eines Gesundheitsdatennutzungsgesetzes (GDNG) eine Vereinheitlichung der forschungsrelevanten Rechtsgrundlagen vorgeschlagen. Geplant ist insoweit eine Rechtsgrundlage für die „Weiterverarbeitung von Versorgungsdaten zur Qualitätssicherung, zur Förderung der Patientensicherheit und zu Forschungszwecken“ durch eine Gesundheitseinrichtung für die bei ihr rechtmäßig gespeicherten Daten.

Das Verhältnis dieser geplanten Neuregelungen zu den Landeskrankenhausgesetzen ist jedoch unklar. Mit der Gesetzgebungskompetenz der Länder für den Bereich der Krankenhäuser hat sich der Gesetzentwurf nicht auseinandergesetzt. Daher bestehen erhebliche Zweifel, dass mit diesem Gesetzentwurf eine rechtssichere und tragfähige Neuregelung erreicht wird, die die länderübergreifende Forschung erleichtert.

Die DSK hat in ihrer Stellungnahme zum GDNG-Gesetzentwurf vom 14.08.2023 hierauf hingewiesen und weiteren Korrekturbedarf aufgezeigt (Die Stellungnahme der DSK vom 14.08.2023 zum Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz – GDNG – Stand 03.07.2023) ist abrufbar unter www.datenschutzkonferenz-online.de/media/st/23_08_14_DSK_Stellungnahme_GDNG-E.pdf).

In dieser Stellungnahme und in der „Petersberger Erklärung“ vom 24.11.2022 hat die DSK wichtige Hinweise für gesetzliche Neuregelungen formuliert (Die Entschließung der DSK vom 24.11.2022 (Petersberger Erklärung) ist abrufbar unter www.datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf). Sie beschreiben wesentliche Anforderungen zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung, insbesondere zu den Rechtsgrundlagen und den besonderen Einwirkungsmöglichkeiten für betroffene Personen.

Um eine weitgehende Nutzung von Gesundheitsdaten zu Forschungszwecken im Einklang mit den Grundrechten zu normieren, sind konkrete Garantien und Maßnahmen gesetzlich festzulegen. Es gilt der Grundsatz: Je höher der

Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten zu Forschungszwecken genutzt werden (Vgl. Empfehlung Nr. 2 der Petersberger Erklärung). Abhängig von den jeweils verarbeiteten Datenarten – z. B. personenbezogenen Daten (Art. 4 Nr. 1 DSGVO), Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) oder genetische Daten (Art. 4 Nr. 13 DSGVO) – bedarf es eines angemessenen Schutz- und Vertrauensniveaus und spezifischer Regelungen für die Verarbeitungen in den jeweiligen Bereichen der Forschung.

Für besondere Forschungsgegenstände, bei denen eine ausreichende Anonymisierung nicht immer gewährleistet werden kann (etwa für radiologische Bilddaten), sollten spezifische Regelungen getroffen werden, um einen angemessenen Schutz der Grundrechte der betroffenen Personen sicherzustellen, z. B. durch zusätzliche technische und organisatorische Maßnahmen.

Darüber hinaus sind die Regelungen des Art. 9 Abs. 2 lit. j in Verbindung mit Art. 89 Abs. 1 DSGVO zu beachten. Insbesondere müssen im Gesetz selbst angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person festgelegt werden. Diese Festlegung der spezifischen Anforderungen darf nicht an die Verantwortlichen delegiert werden. Die Umsetzung darf sich auch nicht in generalklauselartigen oder in solchen Regelungen erschöpfen, die die DSGVO ohnehin für die Datenverarbeitung vorsieht, wie etwa die Betroffenenrechte nach Art. 15 ff. DSGVO oder Maßnahmen nach Art. 32 DSGVO. Stattdessen müssen konkrete Maßnahmen benannt werden.

Angemessene und spezifische Maßnahmen in diesem Sinne können etwa sein:

- Vorgaben für die Datenschutz-Folgenabschätzung (z. B. Betrachtungstiefe, Aufgabenzuweisungen für die Durchführung),
- die Schaffung weiterer, über die in Art. 15 ff. DSGVO hinausgehender Betroffenenrechte (z. B. spezifische Widerspruchsrechte, Vernichtung von Bioproben),
- die Festlegung angemessener Sperrfristen, die den betroffenen Personen ermöglichen, ihre Rechte auszuüben, bevor mit ihren Daten geforscht werden darf (z. B. bei einem Widerspruchsrecht),
- die Einbindung einer unabhängigen Treuhandstelle insbesondere zur Verschlüsselung, Anonymisierung oder Pseudonymisierung der Daten,
- die Einrichtung von Datenintegrationszentren oder Forschungsplattformen, soweit konkrete, der DSGVO entsprechende Anforderungen an deren Ausgestaltung formuliert werden,
- die Verpflichtung beteiligter Stellen zur Verschwiegenheit und die Schaffung korrespondierender Prozessrechte wie ein Beschlagnahmeverbot und Zeugnisverweigerungsrechte,

- konkrete Festlegungen zur Ausgestaltung und Gewährleistung der Datenminimierung.

Diese Aufzählung ist nicht abschließend. Es ist die Aufgabe des Gesetzgebers, die Risiken zu erkennen, die mit einer Verarbeitung von Gesundheitsdaten verbunden sind, sie zu benennen und ihnen angemessene Schutzmaßnahmen für die Rechte und Interessen der betroffenen Personen gegenüberzustellen.

Die DSK weist darauf hin, dass medizinische personenbezogene Daten in bestimmten Fallkonstellationen dem absoluten Schutz des Kernbereichs privater Lebensgestaltung unterliegen.

Die Verarbeitung solcher menschenwürderelevanter Daten kann selbst zu Forschungszwecken nicht auf Grundlage einer gesetzlichen Regelung legitimiert werden.

Schließlich ist eine uneingeschränkte Datenschutzaufsicht in dem sensiblen Bereich der Verarbeitung von Gesundheitsdaten zu garantieren. Diese bietet Schutz für die betroffenen Personen. Etwaig bestehende Einschränkungen der Befugnisse der Datenschutzaufsichtsbehörden hinsichtlich der Verhängung von Bußgeldern und des Vollzugs gegenüber öffentlichen Stellen sind zumindest im Anwendungsbereich entsprechender Regelungen aufzuheben.

Die DSK setzt sich für die Schaffung eines hohen Datenschutzniveaus in der medizinischen Forschung durch eine aufeinander abgestimmte zeitnahe rechtsklare und systematische Neustrukturierung der entsprechenden rechtlichen Regelungen ein. Sie appelliert an die Gesetzgeber des Bundes und der Länder, durch klarstellende Regelungen einen wirksamen Kernbereichsschutz sicherzustellen.

Die Datenschutzaufsichtsbehörden bieten an, in Wahrnehmung ihrer Beratungsfunktion die Gesetzgeber vor und bei entsprechenden Gesetzesvorhaben zu unterstützen.

17.10.2023 – Geplante Chatkontrolle führt zu einer unverhältnismäßigen, anlasslosen Massenüberwachung!

Die EU-Kommission beabsichtigt, technische Verfahren zur Überwachung der elektronischen Kommunikation zu ermöglichen, deren erklärtes Ziel es ist, Darstellungen von Kindesmissbrauch im Internet vorzubeugen bzw. aufzudecken. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (Datenschutzkonferenz) weist darauf hin, dass die von der EU-Kommission vorgesehene Wahl der Mittel äußerst zweifelhaft ist, denn hierdurch wären massenweise zum Teil sehr sensible Informationen sämtlicher Nutzender, die E-Mails oder andere Nachrichten in Online-Diensten austauschen, unterschiedslos und verdachtsunabhängig von einer Überwachung betroffen.

Im Mai 2022 hat die Kommission einen Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vorgelegt. Der Vorschlag sieht unter anderem vor, dass Anbieter von E-Mail-oder Online-Diensten zur Nachrichtenübermittlung dazu verpflichtet werden, sexuellen Kindesmissbrauch im Internet aufzudecken. Dazu müssen die Anbieter Maßnahmen ergreifen, um die Verbreitung von bekannten oder neuen Dar-stellungen sexuellen Kindesmissbrauchs oder die Kontaktaufnahme zu Kindern anhand bestimmter Indikatoren zu erkennen.

Ohne Zweifel besteht die Notwendigkeit, Kinder vor sexuellem Missbrauch zu schützen und entsprechende Straftaten aufzudecken. Die Ziele der geplanten Verordnung an sich stehen also nicht infrage. Gleichwohl sind die staatlich angeordnete Kontrolle und Überwachung von Kommunikation in der umfassenden Form, die in dem Verordnungsentwurf vorgesehen ist, von unverhältnismäßigem Ausmaß. Es wird eine Vielzahl von Nutzenden mit einer erheblichen Menge sehr persönlicher Informationen aus sämtlichen Lebensbereichen von den Überwachungsmaßnahmen betroffen sein – und zwar unabhängig davon, ob überhaupt der Verdacht einer Straftat besteht. Der gewählte Ansatz bedeutet, dass die Anbieter sämtliche über bzw. mit ihren Diensten verarbeiteten Daten auf die genannten Inhalte hin überprüfen müssen. Je nachdem, um welche Art von Diensten es sich handelt, werden dabei Verkehrs-, Inhalts- und Standortdaten sowie sämtliche Inhalte der über einen Dienst abgewickelten zwischenmenschlichen Kommunikation überwacht – auch komplette Inhalte von E-Mails und Chats.

Die Verpflichtung soll auch dann gelten, wenn die Dienste eine Ende-zu-Ende verschlüsselte Kommunikation anbieten. De facto bedeutet dies eine Abkehr von der Ende-zu-Ende-Verschlüsselung, die sich in den letzten Jahren als notwendige Vorbedingung privater Kommunikation weitgehend etabliert hat. Damit die Maßnahmen gemäß dem Verordnungsentwurf umgesetzt werden können, müsste nämlich die Ende-zu-Ende-Verschlüsselung aufgebrochen werden.

Daraus folgt, dass Technologien wie Ende-zu-Ende-Verschlüsselung nicht mehr zuverlässig zur Verfügung stehen werden, sondern nur noch unter dem Vorbehalt, dass der anbietende Dienst die Verschlüsselung umgehen kann. Das läuft dem Ziel der Verschlüsselung zuwider, die ausdrücklich die Sicherheit und die Vertraulichkeit der Kommunikation von Nutzenden, einschließlich Kindern, wie der Verordnungsentwurf selbst feststellt, gewährleisten soll. Es ist ein Bruch der Vertraulichkeit elektronischer Kommunikation mit nicht absehbaren Folgen für die Kommunikationsfreiheit als eines der demokratiesichernden Grundrechte schlechthin. Damit wird diese Vertraulichkeitsmaßnahme nicht nur gegenüber den Anbietern nutzlos, sondern es erhöht sich auch generell das Risiko von Schwachstellen, die missbräuchlichen Zugriffen Tür und Tor öffnen. In einer Zeit, in der Sicherheitslücken in IT-Systemen

vermehrt und in großem Stil für illegale Zwecke ausgenutzt werden, sollten Schwächungen des Schutzes vermieden werden, statt absichtlich Bruchstellen in den technischen Infrastrukturen einzubauen.

Die vorgesehene anlasslose Massenüberwachung greift fundamental in die Grundrechte auf Achtung des Privat- und Familienlebens, der Vertraulichkeit der Kommunikation und zum Schutz personenbezogener Daten ein. Vor dem Hintergrund der anstehenden Beratungen im Rat der Europäischen Union warnt die Datenschutzkonferenz davor, den Wesensgehalt dieser Grundrechte anzutasten, und appelliert an den EU-Gesetzgeber, bei der Regulierung von Maßnahmen zur Bekämpfung schwerster Kriminalität die Grenzen der Rechtsstaatlichkeit einzuhalten und insbesondere Erforderlichkeit und Verhältnismäßigkeit zu wahren.

11.05.2023 – Verfassungsrechtliche Anforderungen bei automatisierter Daten-analyse durch Polizei und Nachrichtendienste beachten!

Mit Urteil vom 16. Februar 2023 hat das Bundesverfassungsgericht verfassungsrechtliche Weichen für den behördlichen Einsatz von automatisierten Datenanalysen/-auswertungen gestellt (-1BvR 1547/19 - und -1BvR 2634/20 -). 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. Das trifft beispielsweise auf Datenbestände aus Funkzellenabfragen und aus der Vorgangsbearbeitung 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 Opfern und Zeugen. 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 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) sieht ihre Forderungen aus ihrer Entschließung vom 3. April 2019 „Hambacher Erklärung zur Künstlichen Intelligenz“ in dem Urteil bestätigt.

Die DSK, deren Mitglieder in dem Verfahren angehört wurden, betont, dass die im Bereich der Polizei und Nachrichtendienste vorhandenen allgemeinen Vorschriften den Besonderheiten komplexer Analysemethoden nicht ausreichend Rechnung tragen. Dies gilt jedenfalls für solche Analysemethoden, die mit intensiven Eingriffen in die Grundrechte der betroffenen Personen verbunden sein können. Hierfür bedürfte es eigener verhältnismäßig ausge-

stalteter Rechtsgrundlagen. Der Gesetzgeber wäre dann in der Pflicht, die wesentlichen Grundlagen selbst durch spezifische gesetzliche Vorschriften vorzugeben, um insbesondere Art und Umfang der Daten und die Verarbeitungsmethoden zu begrenzen.

Aufsichtsbehördlichen Erfahrungen entsprechend werden im Bereich der Strafverfolgung und der Gefahrenabwehr auch komplexe Formen der Datenanalyse eingesetzt, mitunter Systeme und Komponenten, die auf maschinellem Lernen basieren. Gerade polizeiliche Ermittlungen und nachrichtendienstliche Beobachtung können mit intensiven Grundrechtseingriffen verbunden sein. Daher ist die Beachtung verfassungsrechtlicher Anforderungen an das Handeln von Polizei und Nachrichtendiensten besonders dringlich.

Die Konferenz appelliert an die in Bund und Ländern politisch Verantwortlichen, den sich aus dem Urteil ergebenden gesetzgeberischen Handlungsbedarf zu prüfen. Erachten sie den Einsatz komplexer Datenanalysemethoden für erforderlich, müssen hierfür klare Rechtsgrundlagen und geeignete Rahmenbedingungen geschaffen werden, mittels derer der Grundrechtsschutz betroffener Personen sichergestellt wird. Die vorhandenen gesetzlichen Bestimmungen sind in der Praxis in verfassungskonformer Weise anzuwenden.

11.05.2023 – Notwendigkeit spezifischer Regelungen zum Beschäftigtendatenschutz! Rechtsprechung des Europäischen Gerichtshofs hat Auswirkungen auf zahlreiche deutsche Vorschriften im Beschäftigungskontext

Der Europäische Gerichtshof (EuGH) hat am 30. März 2023 in der Rechtssache C-34/21 über die Anforderungen an eine europarechtskonforme Umsetzung des Beschäftigtendatenschutzrechts in Hessen entschieden. In seinem Urteil formuliert der EuGH hohe Anforderungen an nationale Vorschriften, die auf der Grundlage der Öffnungsklausel des Artikels 88 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) erlassen werden. Die Entscheidungsgründe legen nahe, dass die Vorschrift des § 23 Absatz 1 Satz 1 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes und § 86 Absatz 4 des Hessischen Beamtengesetzes diese Anforderungen nicht erfüllen.

Die Entscheidung des EuGH ist bundesweit von großer Bedeutung, weil Gesetzgeber aufgrund der Feststellungen des EuGH, soweit noch nicht geschehen, prüfen müssen, ob bestehende Regelungen zum Beschäftigtendatenschutz in Deutschland den Vorgaben von Artikel 88 DS-GVO entsprechen.

Zum einen dürfen diese Regelungen nicht nur die Bestimmungen der DS-GVO wiederholen, sondern es muss sich bei ihnen um spezifischere Vorschriften

der Mitgliedstaaten handeln (siehe Artikel 88 Absatz 1 DS-GVO). Zum anderen müssen diese inhaltlich den Vorgaben des Artikels 88 Absatz 2 DS-GVO entsprechen. Danach müssen die mitgliedstaatlichen Vorschriften selbst Maßgaben zum Schutz der Rechte und Freiheiten der Beschäftigten sowie geeignete und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person enthalten.

Nationale Regelungen im Beschäftigtenkontext, die nicht den Vorgaben der DS-GVO entsprechen, müssen unangewendet bleiben – so der EuGH. In diesen Fällen gelten aufgrund des Anwendungsvorrangs des Unionrechts unmittelbar die Bestimmungen der DS-GVO.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hatte bereits in ihrer Entschließung vom 29. April 2022, **„Die Zeit für ein Beschäftigtendatenschutzgesetz ist ‚Jetzt'!"**, festgestellt, dass die bestehende bundesrechtliche Regelung im Beschäftigtenkontext nicht hinreichend praktikabel, normenklar und sachgerecht ist und als Generalklausel weite Interpretationsspielräume eröffnet. Auch der vom Bundesministerium für Arbeit und Soziales (BMAS) eingesetzte unabhängige, interdisziplinäre Beirat zum Beschäftigtendatenschutz ist in seinem Bericht aus Januar 2022 zu dem Schluss gelangt, dass neben weiteren Maßnahmen ein eigenständiges Beschäftigtendatenschutzgesetz notwendig ist.

Anlässlich der EuGH-Entscheidung hält es die DSK für notwendig, über die vorgenannte Entschließung hinaus, den Gesetzgeber auf die daraus resultierenden inhaltlichen Anforderungen an datenschutzrechtliche Regelungen ausdrücklich hinzuweisen.

Die DSK fordert daher den Gesetzgeber erneut auf, ein Beschäftigtendatenschutzgesetz zu schaffen. Sie begrüßt, dass das Bundesministerium für Arbeit und Soziales (BMAS) und das Bundesministerium des Innern und für Heimat (BMI) mit den Arbeiten für ein Beschäftigtendatenschutzgesetz begonnen haben.

Beschlüsse der Datenschutzkonferenz

Beschlüsse der Datenschutzkonferenz sind Positionen, die die Auslegung datenschutzrechtlicher Regelungen bzw. entsprechende Empfehlungen betreffen.

6.11.2023 – Positionspapier zu cloudbasierten digitalen Gesundheitsanwendungen

Einleitung

Seit 2020 ist für die erstattungsfähigen digitalen Gesundheitsanwendungen gemäß § 33a SGB V die Digitale Gesundheitsanwendungen-Verordnung (DiGAV) in Kraft. Sie regelt, dass digitale Gesundheitsanwendungen die gesetzlichen Vorgaben des Datenschutzes und die Anforderungen an die Datensicherheit nach dem Stand der Technik unter Berücksichtigung der Art der verarbeiteten Daten und der damit verbundenen Schutzstufen sowie des Schutzbedarfs gewährleisten (§ 4 Abs. 1 DiGAV) müssen.

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) führt gemäß § 139e Abs. 1 SGB V ein Verzeichnis erstattungsfähiger digitaler Gesundheitsanwendungen (DiGA) nach § 33a SGB V und entscheidet auch über die Anträge der DiGA-Hersteller zur Aufnahme in das Verzeichnis.

Dabei weisen die Hersteller digitaler Gesundheitsanwendungen die Erfüllung der datenschutzrechtlichen Anforderungen gemäß § 139e Abs. 2 Satz 2 Nummer 2 SGB V derzeit unter Verwendung der Erklärung nach Anlage 1 zur Digitale Gesundheitsanwendungen-Verordnung (DiGAV) nach. Die Herstellererklärung (Selbsterklärung) ist jedoch kein sicheres Mittel, um die Einhaltung der datenschutzrechtlichen Anforderungen nachzuweisen. Daher wurden diesbezüglich die gesetzlichen Anforderungen angepasst:

- Ab dem 1. Januar 2025 müssen digitale Gesundheitsanwendungen abweichend von den Anforderungen an die Datensicherheit nach § 4 Abs. 6 DiGAV die von dem Bundesamt für Sicherheit in der Informationstechnik nach § 139e Abs. 10 SGB V festgelegten Anforderungen an die Datensicherheit erfüllen (§ 4 Abs. 7 DiGAV).

- Gemäß der derzeit geltenden rechtlichen Regelung müssen ab dem 1. August 2024 digitale Gesundheitsanwendungen, abweichend von den Anforderungen an den Datenschutz nach Absatz 6, die von dem Bundesinstitut für Arzneimittel und Medizinprodukte nach § 139e Abs. 11 SGB V festgelegten Prüfkriterien für die von digitalen Gesundheitsanwendungen nachzuweisenden Anforderungen an den Datenschutz umsetzen (§ 4 Abs. 8 DiGAV).

Neben diesen gesetzlich geregelten DiGA gibt es jedoch eine Vielzahl weiterer Gesundheitsanwendungen, die nicht von diesen Regelungen erfasst sind. Für den Einsatz dieser Vielzahl der weiteren Anwendungen ist aus Sicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) Folgendes zu bedenken:

I. Verantwortlichkeiten

Die Feststellung der datenschutzrechtlichen Verantwortlichkeit ist für die nicht unter § 139e SGB V fallenden digitalen Gesundheitsanwendungen ausgesprochen komplex, insbesondere da sich daran verschiedene Aufgaben und Pflichten ausrichten. Grundsätzlich kommen verschiedene Konstellationen der datenschutzrechtlichen Verantwortlichkeit in Betracht.

Die DS-GVO verpflichtet Verantwortliche und Auftragsverarbeiter, Art. 4 Nrn. 7 und 8 DS-GVO. Hersteller nehmen die Rolle eines Verantwortlichen ein, wenn sie neben der Herstellung der digitalen Gesundheitsanwendung zugleich über die Zwecke und Mittel der Datenverarbeitung entscheiden. Sie kommen abweichend hiervon als Auftragsverarbeiter in Betracht, wenn sie für einen Verantwortlichen personenbezogene Daten nach Maßgabe von Artikel 28 und 29 DS-GVO weisungsgebunden verarbeiten. Erschöpft sich die Beteiligung dagegen in der Herstellung der Gesundheitsanwendung, sodass die Hersteller keine personenbezogenen Daten der Nutzer verarbeiten, sind die Hersteller weder Verantwortliche noch Auftragsverarbeiter.

Neben den Herstellern kommen hinsichtlich der Verarbeitung personenbezogener Daten der digitalen Gesundheitsanwendungen weitere Beteiligte in Betracht, wie etwa Ärztinnen und Ärzte und andere medizinische Leistungserbringer sowie Anbieter von Cloud-Diensten. Dabei ist im Einzelfall zu prüfen, welche Rolle diese Beteiligten aus Datenschutzsicht wahrnehmen. Hierfür sind ggf. Formen der alleinigen oder gemeinsamen Verantwortlichkeit oder eine Auftragsverarbeitung von Bedeutung.

Nähere Erläuterungen enthalten die Leitlinien 07/2020 des Europäischen Datenschutzausschusses (EDSA) zu den Begriffen „Verantwortlicher“ und „Auftragsverarbeiter“ in der DSGVO, z. B. in Rn. 26:

„Die Notwendigkeit einer Beurteilung der Faktenlage bedeutet auch, dass sich die Rolle des Verantwortlichen nicht aus der Art der Organisation ergibt, die Daten verarbeitet, sondern aus ihren konkreten Tätigkeiten in einem bestimmten Kontext. Anders ausgedrückt kann ein und dieselbe Organisation gleichzeitig hinsichtlich bestimmter Verarbeitungen als Verantwortlicher und hinsichtlich anderer Verarbeitungen als Auftragsverarbeiter handeln; die Einstufung als Verantwortlicher oder als Auftragsverarbeiter muss jeweils im Hinblick auf den konkreten Datenverarbeitungsvorgang bewertet werden.“

Bei dieser Beurteilung sollte auch berücksichtigt werden, ob es sich um einen einheitlichen Lebenssachverhalt handelt, in dem die verschiedenen Aspekte der Verarbeitung nur als Ganzes einen Sinn ergeben Siehe Beschluss der DSK vom 12.05.2020 zu Google Analytics unter www.datenschutzkonferenz-online.de/media/dskb/20200526_beschluss_hinweise_zum_einsatz_von_google_analytics.pdf).

Entsprechend dem Transparenzgrundsatz der DS-GVO ist zudem der Zweck der Verarbeitung personenbezogener Daten und der jeweilige Verantwortliche in der Datenschutzerklärung kenntlich zu machen.

II. Verwendung der Gesundheitsanwendung ohne Nutzung der Cloudfunktionen

Die Verwendung der Gesundheitsanwendung (z. B. einer App zum Auslesen und Speichern der Glukosewerte) muss nach dem Grundsatz „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ nach Art. 25 Abs. 1 DS-GVO auch ohne Nutzung der Cloudfunktionen und ohne Verknüpfung mit einem Benutzerkonto möglich sein, es sei denn, die Cloudfunktion ist unbedingt für die Erreichung eines therapeutischen Nutzens erforderlich und die Funktion wird von der betroffenen Person ausdrücklich gewünscht.

Die betroffene Person muss hierzu eine entsprechende Auswahlmöglichkeit erhalten (z. B. im Registrierungsprozess) und über etwaige bestehende Vorteile und Risiken, die mit der Cloudanwendung verbunden sind, informiert werden. Die Daten dürfen im Falle der Entscheidung gegen eine cloudbasierte Verarbeitung allenfalls lokal auf dem Endgerät gespeichert werden.

III. Nutzung personenbezogener Daten zu Forschungszwecken und zur Qualitätssicherung

Für die Nutzung personenbezogener Daten zu Forschungszwecken ist eine datenschutzrechtliche Rechtsgrundlage erforderlich. Hier kommt regelmäßig die ausdrückliche Einwilligung nach Art. 9 Abs. 2 Buchst. a DS-GVO i. V. m. Art. 6 Abs. 1 Buchst. a DS-GVO in Betracht.

Für die Verarbeitung anonymisierter Daten ist keine Rechtsgrundlage erforderlich. Nur Informationen, die sich nicht auf identifizierte oder identifizierbare natürliche Personen beziehen, sind keine personenbezogenen Daten im Sinne von Art. 4 Nr. 1 DS-GVO. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind (Erwägungsgrund 26 Satz 3, 4 DS-GVO). Soll eine digitale Gesundheitsanwendung unter Nutzung solch anonymisierter Daten erfolgen, wäre in einer Datenschutz-Folgenabschätzung (DSFA) darzulegen, wie die Anonymisierung durchgeführt wird, und nachzuweisen, dass die Aufhebung des Personenbezugs tatsächlich gewährleistet wird (Derzeit werden vom EDSA Leitlinien zu Anonymisierung erstellt. Nach Veröffentlichung wären diese Leitlinien von den Verantwortlichen bei der Beurteilung der Anonymisierung zu berücksichtigen).

Hersteller von Medizinprodukten sind nach der EU-Medizinprodukte-Verordnung 2017/745 (MPV) zur Qualitätssicherung und zum Risikomanagement verpflichtet. Eine Verarbeitung personenbezogener Daten zu Zwecken der danach vorgeschriebenen Qualitätssicherung kann auf Grundlage des Art. 6 Abs. 1 Buchst. c i. V. m. Art. 9 Abs. 2 Buchst. i DS-GVO und § 22 Abs. 1 Nr. 1 Buchst. c BDSG erfolgen.

Hierbei ist die Verarbeitung der Daten auf das erforderliche Maß zu beschränken. Es sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen (§ 22 Abs. 2 BDSG). Hierzu gehört beispielweise eine zeitlich begrenzte Speicherung und eine Löschung der zum alleinigen Zweck der Qualitätssicherung verarbeiteten Daten nach Abschluss der durchgeführten Qualitätssicherung.

Die häufig implementierten Mechanismen der Reichweitenanalyse und Software-Fehlerverfolgungsmechanismen, die typischerweise in Software-Entwicklungs-Umgebungen integriert sind und zusammen mit Apps und

Webanwendungen ausgeliefert werden, überprüfen das Installationsverhalten und allgemeine Funktionalitätsaspekte der Software (Telemetrie). Diese Datenverarbeitung ist grundsätzlich nicht mit dem Zweck der Anwendung vereinbar.

IV. Betroffenenrechte

Die Hersteller bzw. Betreiber von cloudbasierten Gesundheitsanwendungen müssen Prozesse zur effektiven und unverzüglichen Erfüllung der Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Datenübertragbarkeit etablieren.

Da hierbei besonders sensible Gesundheitsdaten betroffen sind, muss zunächst eine sichere Authentifizierung der Antragsteller erfolgen.

V. Sicherheit der Verarbeitung

Weil eine Verarbeitung personenbezogener Daten immer mit Risiken für die davon betroffenen Personen einhergeht, müssen der Verantwortliche und Auftragsverarbeiter durch die wirksame Umsetzung technischer und organisatorischer Maßnahmen (TOM) ein dem Risiko angemessenes Schutzniveau gewährleisten und den Nachweis dafür erbringen können.

Die Verantwortlichen müssen stets prüfen, ob sie eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchführen müssen. Dies ist regelmäßig der Fall, wenn eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DS-GVO vorliegt. Eine Datenschutz-Folgenabschätzung ist vor Aufnahme der Verarbeitungsvorgänge durchzuführen.

Im Einzelfall können beispielsweise (hier nur auszugsweise genannt) folgende TOM dazu beitragen, die gesetzlichen Anforderungen (vgl. Artikel 5, 24, 25, 32 DS-GVO und § 22 Abs. 2 BDSG) zu erfüllen:

- Berücksichtigung von Technischen Richtlinien des BSI zur Informationssicherheit (vgl. folgender Absatz) und Best-Practice-Guidelines zur sicheren Implementierung von Anwendungen (z. B. OWASP7);
- sichere Authentifizierungsverfahren (in der Regel Multi-Faktor-Authentifizierung);
- Zugriffskontrolle mit „least privilege policy“ und regelmäßiger Überprüfung von Benutzerkonten und Zugriffsrechten;
- automatische zeitbasierte Sperrung von Benutzeranwendungen (u. a. bei Nichtverwendung oder Verschiebung der Anwendung in den Hintergrund einer Oberfläche);

- wirksame Verschlüsselungsmechanismen, insbesondere bei der Speicherung auf Mobilgeräten;
- Richtlinien und Weisungen an Beschäftigte zur datenschutzrechtlichen Sensibilisierung;
- Protokollierungen von Zugriffen mit anlasslosen Prüfungen;
- Schaffung einer Redundanz von Infrastrukturkomponenten und Hintergrundsystemen bei technischen Betreibern;
- Überprüfung von Sicherheitsmaßnahmen in Anwendungsprogrammen und Hintergrundsystemen durch Sicherheits- und Penetrationstests.

Auch sollte die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Technische Richtlinie (TR) „Sicherheitsanforderungen an digitale Gesundheitsanwendungen“ (BSI TR-03161) für alle mobilen Anwendungen, die sensible Daten verarbeiten und speichern, herangezogen werden. Grundsätzlich fordert das BSI, Sicherheitsanforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit von Anfang an bei der Software-Entwicklung mit zu betrachten. Diese Technische Richtlinie soll als Leitfaden dienen, um Entwickler von Anwendungen bei der Erstellung sicherer Lösungen zu unterstützen. Sie gliedert sich in drei Teile:

- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 1: Mobile Anwendungen
- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 2: Web-Anwendungen
- BSI TR-03161 Anforderungen an Anwendungen im Gesundheitswesen – Teil 3: Hintergrundsysteme

Die getroffenen technischen und organisatorischen Maßnahmen sind gemäß Art. 5 Abs. 2 i. V. m. Art. 32 Abs. 1 Buchst. d DS-GVO regelmäßig und anlassbezogen zu überprüfen, zu bewerten sowie zu evaluieren.

VI. Internationaler Datentransfer

Bei Datenübermittlungen an Verantwortliche und Auftragsverarbeiter in Drittländern sind die Maßgaben des Kapitel V der DS-GVO zu berücksichtigen. Falls eine Übermittlung auf Grundlage des Art. 46 DS-GVO erfolgt, müssen zusätzliche Maßnahmen ergriffen werden, die geeignet sind, bei dieser Übermittlung ein Schutzniveau herzustellen, das mit dem bei einer Verarbeitung innerhalb der EU/des EWR vergleichbar ist. Die entsprechenden Anforderungen an solche Maßnahmen sind in den EDSA-Empfehlungen 01/2020 und 02/2020 konkretisiert.

27.11.2023 – Positionspapier zur audiovisuellen Umgebungserfassung im Rahmen von Entwicklungsfahrten

1. Vorbemerkung

Dieses Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder[6] (DSK) behandelt Aspekte des Datenschutzes der Verarbeitung audiovisuell erfasster Umgebungsdaten zu Entwicklungs- und Testzwecken im Zusammenhang mit der Entwicklung des autonomen Fahrens. Die Automobilhersteller und Zulieferer (im Folgenden als Hersteller bezeichnet) äußern zunehmend den Bedarf, Entwicklungs- und Erprobungsfahrten (im Folgenden kurz als „Entwicklungsfahrten“ bezeichnet) unter realen Fahr- und Verkehrsbedingungen durchführen zu können. Das dient dazu, sowohl den Nutzungsgrad bestehender oder neu zu entwickelnder Assistenzsysteme, Fahrfunktionen und damit in Kontext stehende Dienste als auch ihre Verwendung zum automatisierten Fahren bis hin zur autonomen Mobilität zu entwickeln und zu verbessern.

Bei der audiovisuellen Umgebungserfassung werden personenbezogene Daten, u. a. Kfz-Kennzeichen, von Verkehrsteilnehmenden und weiteren Personen (z. B. Insassen anderer Fahrzeuge oder Personen, die zu Fuß, mit einem Fahrrad oder Motorrad am Verkehr teilnehmen) in räumlicher Umgebung der Fahrzeuge verarbeitet. Es ist bekannt, dass die Funktions- und Fahrzeugentwicklung in diesem Bereich oft in Zusammenarbeit mit Forschungseinrichtungen, Technologiepartnern und anderen Unternehmen der Automobilindustrie erfolgt und damit eine Weitergabe dieser Daten an Dritte verbunden ist.

2. Entwicklungsfahrten

Entwicklungsfahrten im Bereich der audiovisuellen Umgebungserfassung, sei es auf einem nicht öffentlichen Testgelände oder unter realen Bedingungen, zielen darauf ab, Systeme für die aktive und passive Sicherheit und für automatisiertes und autonomes Fahren zu entwickeln oder zu verbessern. Nach Angaben der Hersteller werden dazu speziell ausgerüstete und entsprechend gekennzeichnete (vgl. Abschnitt 3.4 weiter unten) Testfahrzeuge eingesetzt, die keine Privatfahrzeuge sind.

6 Dieses Positionspapier basiert auf einem Austausch der Datenschutzaufsichtsbehörden des Bundes und der Länder mit dem Verband der Automobilindustrie (VDA).

2.1. Datenerfassung unter realen Verkehrsbedingungen

Gemäß den Informationen der Hersteller verarbeiten die Testfahrzeuge bei der (Weiter-)Entwicklung von Fahrerassistenzsystemen sowie der Erprobung des automatisierten und autonomen Fahrens die Video- und Audiodaten der Fahrzeugumgebung insbesondere, um damit Lern- und Testdaten für die Entwicklung selbstlernender Systeme zu erhalten. Für den bestmöglichen „Lernerfolg“ dieser Systeme bedürfe es der Erfassung und Verarbeitung einer Vielzahl unterschiedlichster Verkehrssituationen als Abbild der Realität. Die Hersteller betonen, dass diese Echtdaten, zu denen zwangsläufig auch personenbezogene Daten gehören, für diesen bestmöglichen Lernerfolg unerlässlich sind.

Die DSK weist darauf hin, dass die Aufzeichnungen im öffentlichen Raum nur in dem Umfang zulässig sind, wie Aufzeichnungen auf einem nichtöffentlichen Testgelände nicht ausreichend sind. Die genauen Zwecke der jeweils geplanten Datenverarbeitungen müssen für jedes Projekt festgelegt werden. Soweit die o. g. personenbezogenen Daten für die Weiterentwicklung der Algorithmen für Simulationen und Verifikationen z. B. für Folge-Generationen benötigt werden, ist für diese Verarbeitung ebenfalls der Grundsatz der Zweckbindung zu beachten.

2.2. Art und Umfang der verarbeiteten Daten

Folgende audiovisuelle Datenkategorien und dazugehörige Metadaten (GPS-Position des Erprobungsfahrzeugs mitsamt Zeitstempel, Geschwindigkeit des Testfahrzeugs usw.) werden nach Aussage der Hersteller bei der audiovisuellen Umgebungserfassung zu den oben beschriebenen Zwecken verarbeitet[7]:

- Optische Umgebungserfassung durch Bild- und Videoaufnahmen oder andere bildgebende Sensorik (bis zu 360°),
- Akustische Signale der Umgebung zwecks Erkennung von akustischen Warnsignalen.

Zur Gewährleistung einer hinreichenden funktionalen Sicherheit selbstlernender Systeme könne es je nach Zweck der Entwicklung erforderlich sein, große Datenmengen zu erfassen und dazu bis zu mehreren Millionen Testkilometer zu absolvieren. Die Verarbeitung der aufgezeichneten Daten erfolge nicht nur in den Testfahrzeugen, sondern in der Regel auch in den Entwicklungszentren der Hersteller und Entwickler.

7 Zur Klarstellung: Nicht in der Liste enthalten sind die Datenkategorien, die im Rahmen der Erprobung verarbeitet werden, aber keinen unmittelbaren Bezug zur Umgebungserfassung haben und somit nicht Gegenstand dieser Erklärung sind.

3. Rechtmäßigkeit der Datenverarbeitung

3.1. Rechtsgrundlage

Da die Einholung von Einwilligungen aller betroffenen Personen nicht möglich erscheint, kommt als Rechtsgrundlage für die Zulässigkeit der Datenverarbeitung im Regelfall Art. 6 Abs. 1 Buchst. f DS-GVO in Betracht. Danach ist die Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Die DSK erkennt grundsätzlich an, dass Hersteller und Entwickler ein berechtigtes Interesse an der (Weiter-)Entwicklung von Fahrerassistenzsystemen, des automatisierten und autonomen Fahrens sowie der Entwicklung von Fahrfunktionen und damit in Kontext stehenden Diensten haben können. Diese Entwicklungen können der Verbesserung der Verkehrssicherheit und damit auch dem allgemeinen öffentlichen Interesse dienen.

Die Hersteller haben dargestellt, dass für die Wahrung dieses Interesses die Verwendung von Material aus dem realen Straßenverkehr unter Echtbedingungen erforderlich ist, da lediglich hierdurch ein hinreichend breites Spektrum an Fahrsituationen erlernt und getestet werden könne. Nach Aussagen der Hersteller ist zur Gewährleistung einer hinreichenden Zuverlässigkeit und Sicherheit des automatisierten und autonomen Fahrens eine hohe Quantität und Qualität der Daten erforderlich und damit die Erfassung einer möglichst großen Anzahl unterschiedlicher Verkehrssituationen.

Bei der Erzeugung von Audio- und Videodateien haben die Verantwortlichen den Anwendungsbereich von § 201 und des § 201a StGB zu beachten. Die DSK betont, dass an strafbaren Datenverarbeitungsvorgängen bereits kein berechtigtes Interesse im Sinne des Datenschutzrechts bestehen kann.

Die Datenverarbeitung ist zur Verwirklichung der festgelegten Entwicklungs- und Testzwecke nicht erforderlich, wenn diese in zumutbarer Weise ebenso wirksam mit anderen Mitteln erreicht werden können, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen, insbesondere die durch die Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union garantierten Rechte auf Achtung des Privatlebens und auf Schutz personenbezogener Daten, eingreifen. Die Verantwortlichen haben daher in regelmäßigen Abständen unter Berücksichtigung des Stands der Technik zu überprüfen, ob der Eingriff in die Rechte betroffener Personen etwa durch technische Mittel ausgeschlossen oder abgemildert werden kann, beispielsweise durch die Nutzung technischer Anonymisierungsverfahren (Schwärzen, Verpixeln o. Ä.) oder eine während oder unmittelbar nach der Aufzeichnung erfolgende automatisierte Löschung von Daten, die für die festgelegten Zwecke unerheblich sind. Das Ergebnis der Prüfung ist zu dokumentieren.

Die nach Art. 6 Abs. 1 Buchst. f DS-GVO erforderliche Abwägung der berechtigten Interessen des Verantwortlichen mit den Interessen oder Grundrechten und Grundfreiheiten der betroffenen Personen, insbesondere dem grundrechtlich geschützten Interesse, sich frei und unbeobachtet im öffentlichen Raum bewegen zu können, muss im Einzelfall erfolgen. Im Erwägungsgrund 47 der DS-GVO finden sich insbesondere die folgenden Kriterien, die im Einzelfall im Rahmen der Interessenabwägung anzuwenden sind[8]:

a) Vernünftige Erwartung der betroffenen Personen und Vorhersehbarkeit der Datenverarbeitung / Transparenz,
b) Interventionsmöglichkeiten der betroffenen Personen,
c) Verkettung von Daten,
d) Beteiligte Akteure,
e) Dauer der Erfassung,
f) Kreis der betroffenen Personen (beispielsweise besonders schutzbedürftige Personen),
g) Datenkategorien,
h) Umfang der Datenverarbeitung.

Nachstehend sind, bezogen auf diese Kriterien, beispielhaft Aspekte aufgeführt, die im Rahmen der im Einzelfall durchzuführenden Interessenabwägung zugunsten der Interessen der Hersteller und Entwickler berücksichtigt werden können. Ob die Abwägung dann zugunsten der Hersteller und Entwickler ausfällt, muss anhand der Gesamtumstände des konkreten Einzelfalls entschieden werden.

- Die zu entwickelnden Fahrfunktionen dienen überwiegend der Verbesserung der Verkehrssicherheit und insoweit auch dem Gemeinwohl.
- Die Erfassung zielt nicht auf eine Identifizierung von individuellen Personen oder Personengruppen ab. Es sollen vielmehr Kategorien (z. B. Fahrzeuge, Fahrradfahrer oder Fußgänger) erkannt und klassifiziert werden. Dem entsprechend werden die einzelnen Personen nicht identifiziert.
- Die Datenerhebungen beschränken sich auf eine Erfassung realer Zustände und Abläufe im öffentlichen Verkehrsraum, wobei nur kurzzeitig, momenthaft und als Nebeneffekt auch personenbezogene Daten erhoben werden können.

Zugunsten der betroffenen Personen können im Rahmen einer Abwägung nach Art. 6 Abs. 1 Buchst. f DS-GVO insbesondere folgende Erwägungen zu berücksichtigen sein:

8 Siehe „Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien“ (S. 16 ff.), Beschluss der DSK vom 29.03.2019 (www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf), und „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021“, Beschluss der DSK vom 20.12.2021 (www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf).

- Werden Daten offensichtlich nicht am Straßenverkehr beteiligter Personen erhoben, die regelmäßig nicht damit rechnen müssen, zu den festgelegten Entwicklungs- und Testzwecken aufgenommen zu werden, wiegt der Eingriff in die Rechte auf Datenschutz und Achtung des Privatlebens besonders schwer. Offensichtlich nicht am Straßenverkehr beteiligt sind grundsätzlich Personen, die sich in von der Fahrbahn aus einsehbaren Räumlichkeiten oder anderen befriedeten Bereichen, wie beispielsweise auf der Terrasse eines Gastronomiebetriebs, auf eingezäunten Schulhöfen oder Spielplätzen, aufhalten.

- Infolge einer Mehrfacherfassung bereits abgebildeter Straßenabschnitte kann es zu einer Wiederholung oder Vertiefung des Eingriffs in die Rechte betroffener Personen kommen. Dies gereicht dem Verantwortlichen zum Nachteil, es sei denn, eine weitere Abbildung des Verkehrsgeschehens auf dem jeweiligen Straßenabschnitt war im Hinblick auf die festgelegten Zwecke objektiv geboten, da sie etwa wesentliche neue Erkenntnisse versprach, und der Verantwortliche hat dies vor Durchführung der Entwicklungsfahrt dokumentiert.

- Die Verarbeitung besonderer Kategorien personenbezogener Daten ist regelmäßig von hoher Eingriffsintensität und grundsätzlich gemäß Art. 9 Abs. 1 DS-GVO untersagt. Soweit das aufgezeichnete Material nicht verarbeitet wird, um besondere Datenkategorien abzuleiten, ist Art. 9 DS-GVO jedoch nicht anzuwenden (vgl. EDSA-Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte, Rn. 62 ff.). Allerdings stellt die Verarbeitung von anderen besonders schützenswerten sensiblen Daten auch in Fällen, in denen Art. 9 Abs. 1 DS-GVO keine Anwendung findet, einen intensiven Eingriff dar, der in der gemäß Art. 6 Abs. 1 Buchst. f DS-GVO durchzuführenden Interessenabwägung umso schwerer wiegt, wenn die Verarbeitung solcher Daten durch den Verantwortlichen objektiv zu erwarten und technisch oder organisatorisch vermeidbar war. Die Erhebung solcher Daten ist insbesondere dann objektiv zu erwarten, wenn Einrichtungen oder Veranstaltungen erfasst werden, die regelmäßig dazu bestimmt sind, durch besonders schutzbedürftige Personengruppen, wie beispielsweise Kinder, aufgesucht zu werden. Die Verantwortlichen müssen vor Durchführung der Entwicklungsfahrt begründen und entsprechend der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO dokumentieren, aus welchem Grund sich eine audiovisuelle Erfassung entsprechender Einrichtungen oder Veranstaltungen wie z. B. Spielplätze, Kindergärten, Schulen, Krankenhäuser und Einrichtungen zur Glaubensausübung als unvermeidbar darstellt. Ein möglicher Grund könnte in besonderen Ausnahmefällen etwa die Gewährleistung der hinreichenden funktionalen Sicherheit auch in Gegenwart vulnerabler Personen im Straßenverkehr und damit deren Schutz sein.

3.2. Datenschutz durch Technikgestaltung

Die Hersteller und Entwickler müssen nach Art. 25 Abs. 1 DS-GVO sowie nach Art. 32 Abs. 1 DS-GVO sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen treffen, die die Einhaltung der Datenschutzgrundsätze nach Art. 5 DS-GVO wirksam gewährleisten. Diese Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind.

Die Hersteller geben an, dass eine Pseudonymisierung oder Anonymisierung der erhobenen Daten im Rahmen der Entwicklungsfahrten nicht realisierbar ist, da eine Verfälschung von Bildern mit dem Ziel, Gesichter oder Kennzeichen beispielsweise durch Unschärfe oder Schwärzen unkenntlich zu machen, das Risiko erhöhen würde, dass reale Situationen im Straßenverkehr von diesen Systemen nicht eindeutig erkannt werden können. Auch wenn diese Einschätzung nach derzeitigem Stand der Technik zutreffen sollte, müssen die Hersteller und Entwickler in regelmäßigen Abständen überprüfen, ob der Eingriff in die Rechte betroffener Personen durch andere, fortgeschrittene technische Mittel, wie etwa die Nutzung von synthetischen Daten oder durch Fahrten auf einem Testgelände, ausgeschlossen oder abgemildert werden kann.

Darüber hinaus sind in den Fahrzeugen wie auch bei der Übermittlung in die sowie der Verarbeitung in den Entwicklungszentren geeignete technische und organisatorische Maßnahmen zur Unterbindung einer zweckfremden Verwendung der Daten zu ergreifen. Dies gilt besonders, wenn Daten nicht anonymisiert oder pseudonymisiert werden konnten. Die Wirksamkeit der technischen und organisatorischen Maßnahmen muss durch Einhaltung der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nachgewiesen werden. Dabei sind bestehende Standards, Methoden und Best Practices gebührend zu berücksichtigen[9].

3.3. Durchführung einer Datenschutz-Folgenabschätzung

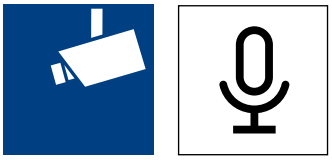
Im Rahmen von Entwicklungsfahrten werden in großem Umfang personenbezogene Daten verarbeitet und beim Verantwortlichen gespeichert. Aus diesem Grund muss eine Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO durchgeführt werden.

9 Z. B. „Positionspapier der DSK zu empfohlenen technischen und organisatorischen Maßnahmen bei der Entwicklung und dem Betrieb von KI-Systemen", Beschluss der DSK vom 06.11.2019 (www.datenschutzkonferenz-online.de/media/en/20191106_positionspapier_kuenstliche_intelligenz.pdf), Positionspapier „Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar" im Rahmen der 36. Konferenz der Informationsfreiheitsbeauftragten vom 16.10.2018 (www.informationsfreiheit.bremen.de/sixcms/media.php/13/IFK-Positionspapier_Algorithmen_16.pdf), IT-Grundschutz-Kompendium des BSI, Standard-Datenschutzmodell (SDM, www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V30a.pdf) oder einschlägige ISO-Normen wie z. B. 27701

3.4. Wahrung der Betroffenenrechte und Erfüllung der Informationspflichten

Die Hersteller und Entwickler müssen als die jeweils Verantwortlichen für die Verarbeitung die betroffenen Personen über die Verarbeitung personenbezogener Daten sowie ihre Betroffenenrechte gemäß der Art. 12 ff. DS-GVO informieren und hierzu geeignete Maßnahmen treffen. Aufgrund der Vielzahl der Informationen ist es nicht zweckmäßig, diese vollständig auf einem sich bewegenden Auto anzubringen. Es ist vielmehr angezeigt, die Informationen auf mehrere Ebenen zu verteilen. Wesentliche Informationen müssen auf dem Fahrzeug angebracht werden. Da die Identität der betroffenen Personen zum Zeitpunkt der Datenerhebung in der Regel nicht bekannt ist und diese auch nicht angesprochen werden können, müssen die Hersteller und Entwickler eine Webseite mit einer Datenschutzerklärung (insbesondere Informationen zu den Betroffenenrechten) einrichten und bewerben, um der Informationspflicht gemäß der DS-GVO nachzukommen.

Um die betroffenen Personen über die Video- und Audioaufzeichnung und diese Webseite zu informieren, sind die Testfahrzeuge mit geeigneten und gut sichtbaren Piktogrammen sowie der Benennung der verantwortlichen Stelle, des Zwecks und der URL zu einer Informationsseite zu versehen:



+ Verantwortlicher[10] + Ansprechpartner + URL + Hauptverarbeitungszweck

Auf der Webseite müssen den betroffenen Personen dann alle Informationen zur Erfüllung der Informationspflichten zur Verfügung stehen.

Die Rechte betroffener Personen, insbesondere Auskunftsansprüche (Art. 15 DS-GVO) sowie das Recht auf Widerspruch (Art. 21 DS-GVO) und Löschung (Art. 17 DS-GVO), sind zu erfüllen, soweit keine Ausnahmenvorschrift greift. Da davon auszugehen ist, dass die im Fahrzeugumfeld erfassten Personen regelmäßig nicht ohne Zusatzinformationen identifiziert werden können und eine solche Identifizierung für die von den Herstellern und Entwicklern verfolgten Zwecke auch nicht erforderlich ist, sind Hersteller und Entwickler gemäß Art. 11 Abs. 1 DS-GVO nicht zu einer zusätzlichen Datenverarbeitung zum Zweck der Identifikation verpflichtet. Sofern Verantwortliche in diesen Fällen potenziellen Betroffenen nachweisen, dass sie nicht in der Lage sind, diese zu identifizieren, finden die Pflichten nach Art. 15 bis 20 DS-GVO keine Anwendung (Art. 11 Abs. 2 DS-GVO). Etwas anderes gilt nur dann, wenn betroffene Personen im Einzelfall selbst zusätzliche Informationen bereitstellen, die ihre

10 Soweit der Schutz von Geschäftsgeheimnissen bei einer Offenlegung des Verantwortlichen tangiert ist, ist die Ausgestaltung der Informationspflichten im Einzelfall mit der zuständigen Datenschutzaufsichtsbehörde zu klären

Identifizierung ermöglichen (Art. 11 Abs. 2 Satz 2 DS-GVO). Die Hersteller und Entwickler müssen die Information über die erforderlichen Angaben für eine Identifizierung in geeigneter Weise zur Verfügung stellen.

Folgende Eckpunkte im Umgang mit Betroffenenrechten sind insbesondere zu beachten:

- Auskunftsanspruch: Eine Auskunftserteilung über die Umstände einer Aufnahme hat zu erfolgen, wenn die betroffene Person ihrerseits Informationen bereitstellt, die ermöglichen festzustellen, ob sie Gegenstand einer Aufnahme sein könnte, indem sie z. B. den genauen Ort und den Tag mit der genauen Uhrzeit der Aufnahme nennt (Art. 11 Abs. 2 DS-GVO).

- Löschungsanspruch bzw. Widerspruch: Die Hersteller und Entwickler müssen im Einzelfall entscheiden und dokumentieren, ob eine Löschung die Zwecke der (Weiter-)Entwicklung von Fahrerassistenzsystemen und des automatisierten und autonomen Fahrens ernsthaft beeinträchtigt (Art. 17 Abs 3 Buchst. d DS-GVO) bzw. ein Widerspruch aufgrund zwingender schutzwürdiger Verarbeitungsgründe, die die Interessen, Rechte und Freiheiten der betroffenen Personen überwiegen, nicht in Betracht kommt (Art. 21 Abs. 1 DS-GVO).

Die Daten müssen im Einklang mit geltendem Datenschutzrecht gelöscht werden. Zur Verteidigung von Rechtsansprüchen (Produkthaftung usw.) dürfen die Daten gemäß den gesetzlichen Vorgaben ggf. länger gespeichert werden.

3.5. Datenschutzrechtliche Verantwortlichkeit, Datenübermittlung

Die Hersteller und Entwickler arbeiten nach eigenen Angaben mit technischen Entwicklungsdienstleistern, Forschungskooperationspartnern (z. B. Universitäten oder Institute der angewandten Forschung) sowie Technologiepartnern und anderen Mitgliedern der Automobilwirtschaft (Kooperationspartner) zusammen. In bestimmten Fällen würden Datensätze auch an externe Partner weitergegeben. Dies sei beispielsweise der Fall, wenn sich die Hersteller und Entwickler an öffentlich geförderten Forschungsprojekten mit akademischen Partnern beteiligen und die Daten zur Durchführung eines solchen Forschungsprojektes benötigt werden. Auch ein Austausch der Datensätze innerhalb einer Kooperation mit Technologiepartnern oder anderen Mitgliedern der Automobilwirtschaft falle darunter.

In diesem Rahmen müssen die gesetzlich vorgegebenen datenschutzrechtlichen Verantwortlichkeiten in Bezug auf die Beteiligten klar zugewiesen (Artikel 24, 26 oder 28 DS-GVO, d. h. unabhängige Verantwortliche, gemeinsam

Verantwortliche, Auftragsverarbeiter) und dokumentiert werden. Dazu müssen entsprechende Verträge bestehen, die den gesetzlichen Anforderungen genügen. Die einzelnen Dienstleister oder Kooperationspartner dürfen hierfür Daten zweckbezogen in Abhängigkeit der durchzuführenden Aufgaben oder angestrebten Entwicklungsziele und unter Berücksichtigung einer Rechtsgrundlage für die Übermittlung nach Art. 6 Abs. 1 DS-GVO erhalten.

Werden personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt, sind die Anforderungen an den internationalen Datentransfer (insbesondere unter Beachtung des neuen EU-US Data Privacy Framework[11]) ein-zuhalten. Dies ist vom Verantwortlichen im Rahmen der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nachzuweisen.

22.03.2023 – Bewertung von Pur-Abo-Modellen auf Websites

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) beschließt im Zusammenhang mit sogenannten Pur-Abo-Modellen auf Websites:

1. Grundsätzlich kann die Nachverfolgung des Nutzendenverhaltens (Tracking) auf eine Einwilligung gestützt werden, wenn alternativ ein trackingfreies Modell angeboten wird, auch wenn dies bezahlpflichtig ist. Die Leistung, die Nutzende bei einem Bezahlmodell erhalten, muss jedoch erstens eine gleichwertige Alternative zu der Leistung darstellen, die diese durch eine Einwilligung erlangen. Zweitens muss die Einwilligung alle in der Da-tenschutz-Grundverordnung (DS-GVO) normierten Wirksamkeitsvoraussetzungen, d. h. insbesondere die in Art. 4 Nr. 11 sowie Art. 7 DS-GVO aufgeführten Erfordernisse, erfüllen (In diesem Zusammenhang wird auch auf die Leitlinien 05/2020 des Europäischen Datenschutzausschusses verwiesen: EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 20.05.2020, Rn. 37 f., www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf)

2. Ob die Bezahlmöglichkeit – also z. B. ein Monats-Abo – als eine gleichwertige Alternative zur Einwilligung in das Tracking zu betrachten ist, hängt insbesondere davon ab, ob den Nutzenden gegen ein marktübliches Entgelt ein gleichwertiger Zugang zu derselben Leistung eröffnet wird. Ein gleichwertiger Zugang liegt in der Regel vor, wenn die Angebote zumindest dem Grunde nach die gleiche Leistung umfassen.

3. Nehmen Nutzende das Angebot im Rahmen eines „trackingfreien“ Abonnements wahr und erteilen keine zusätzliche Einwilligung, dürfen gemäß

11 „Übermittlung personenbezogener Daten aus Europa an die USA – Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023“, Anwendungshinweise der DSK vom 04.09.2023 (www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf).

§ 25 Abs. 1 des 1 Gesetzes über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG) nur Speicher- und Auslesevorgänge erfolgen, die für den von ihnen ausdrücklich gewünschten Telemediendienst unbedingt erforderlich sind. Nachfolgende Verarbeitungen personenbezogener Daten sind nur dann zulässig, wenn die Anforderungen der DS-GVO, insbesondere die gesetzlichen Erlaubnistatbestände gemäß Art. 6 Abs. 1 DS-GVO und, je nach Einzelfall, Art. 9 DS-GVO, erfüllt sind. Diesbezüglich wird auf die allgemeinen Ausführungen in der Orientierungshilfe der DSK für Anbieter von Telemedien (OH Telemedien 2021, Version 1.1) Bezug genommen.

4. Die Wirksamkeit von Einwilligungen von Nicht-Abonnentinnen und Nicht-Abonnenten ist bei den sogenannten Pur-Abo-Modellen sicherzustellen. Soweit mehrere Verarbeitungszwecke vorliegen, die wesentlich voneinander abweichen, müssen die Anforderungen an die Freiwilligkeit dahingehend erfüllt werden, dass Einwilligungen granular erteilt werden können. Dies bedeutet unter anderem, dass Nutzende die Möglichkeit haben müssen, die einzelnen Zwecke, zu denen eine Einwilligung eingeholt werden soll, selbst und aktiv auswählen zu können (Opt-in). Nur wenn Zwecke in einem sehr engen Zusammenhang stehen, kann eine Bündelung von Zwecken in Betracht kommen. Eine pauschale Gesamteinwilligung in insoweit verschiedene Zwecke kann nicht wirksam erteilt werden.

5. Darüber hinaus müssen die Einwilligungen den sonstigen Anforderungen der DSGVO gerecht werden, insbesondere auch jenen an Transparenz, Verständlichkeit und Information für die betroffenen Personen aus Art. 4 Nr. 11 und Art. 7 Abs. 2 DS-GVO (vgl. hierzu die Orientierungshilfe der DSK für Anbieter von Telemedien (OH Telemedien 2021, Version 1.1).

31.02.2023 – Zur datenschutzrechtlichen Bewertung von Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder bewertet Zugriffsmöglichkeiten öffentlicher Stellen von Drittländern auf personenbezogene Daten, die nach Art. 28 DSGVO im Auftrag im EWR verarbeitet werden, datenschutzrechtlich wie folgt:

1. Die Gefahr allein, dass – etwa über gesellschaftsrechtliche Weisungsrechte – die Drittlands-Muttergesellschaft eines EWR-Unternehmens dieses anweisen könnte, oder dass öffentliche Stellen von Drittländern unmittelbar EWR-Unternehmen anweisen könnten, personenbezogene Daten in ein Drittland zu übermitteln, genügt nicht, um eine Übermittlung in ein Drittland i.S.d. Art. 44 ff. DSGVO anzunehmen.

2. Allerdings kann eine solche Gefahr dazu führen, dass solchen Rechtsvorschriften unterliegenden Auftragsverarbeitern die Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO fehlt, soweit nicht diese – oder auch der Verantwortliche – technische und/oder organisatorische Maßnahmen ergriffen haben, die hinreichend Garantien dafür bieten, dass der Auftragsverarbeiter seinen Pflichten nachkommt, insbesondere was das Unterlassen von Verarbeitungen personenbezogener Daten ohne oder gegen die Weisung des Verantwortlichen angeht, im Speziellen auf der Grundlage von Verpflichtungen aus drittstaatlichem Recht.

3. Soweit das Risiko besteht, dass eine Norm oder Praxis, die nach EU-Recht unzulässige Verarbeitungen personenbezogener Daten verlangen kann, auch auf EWR-Tochtergesellschaften von Drittlands-Unternehmen anwendbar ist, genügt die Verarbeitung durch eine EWR-Tochtergesellschaft als Auftragsverarbeiter für sich genommen nicht, um eine Zuverlässigkeit im Sinne von Art. 28 Abs. 1 DSGVO zu erreichen. Soweit eine Norm oder Praxis eines Drittlands die abstrakte Gefahr einer nach EU-Recht unzulässigen Übermittlung personenbezogener Daten aus dem EWR in ein Drittland durch eine als Auftragsverarbeiter tätige Stelle in dem EWR – z. B. die EWR-Tochtergesellschaft eines Drittlands-Unternehmens – begründet, sind an die Sorgfalt der Zuverlässigkeitsprüfung im Sinne von Art. 28 Abs. 1 DSGVO besonders hohe Anforderungen zu stellen, die dieser Gefahr Rechnung tragen.

4. Dies erfordert zunächst eine Bewertung sämtlicher Umstände des Einzelfalls, ob der Auftragsverarbeiter und/oder die von ihm verarbeiteten Daten unter diese drittstaatliche Norm oder Praxis fallen und wenn ja, ob der Auftragsverarbeiter dennoch hinreichend Garantien dafür bietet, dass es nicht zu Verarbeitungen kommt, die nach den Maßstäben der DSGVO bzw. des anwendbaren mitgliedstaatlichen Rechts unzulässig sind.

Dabei sind insbesondere die folgenden Punkte zu berücksichtigen:

- das Ergebnis einer Prüfung hinsichtlich einer extraterritorialen Anwendbarkeit des Drittlands-Rechts und einer ggf. darüber hinausgehenden praktischen extraterritorialen Anwendung,
- bei einer extraterritorialen Anwendbarkeit und/oder Anwendung: das Ergebnis einer Prüfung, ob das Recht oder die Praxis des Drittlands die Verpflichtungen aus dem Auftragsverarbeitungsvertrag beeinträchtigen könnten (in Anlehnung an die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses),
- das Risiko, dass die Drittlands-Muttergesellschaft eines EWR-Tochterunternehmens dieses anweisen könnte, personenbezogene Daten in ein Drittland zu übermitteln (Prüfung der Erkenntnisse zur Rechtslage/-praxis),

- ob der Auftragsverarbeitungsvertrag nach europäischen Maßstäben unzulässige Verarbeitungen auf der Grundlage von Drittlands-Recht erlaubt,
- etwaige Zusicherungen der Drittlands-Muttergesellschaft und des EWR-Unternehmens zum Umgang mit kollidierenden Anforderungen des Rechts eines Drittstaates und der EU,
- eine Bewertung der Rechtslage und -praxis des Drittlands, ob derartige Zusicherungen auch tatsächlich eingehalten werden können,
- eine Bewertung aller weiteren Aspekte, ob derartige Zusicherungen auch tatsächlich eingehalten werden,
- etwaige in der Vergangenheit festgestellte Datenschutzverstöße,
- die Schwere und Wahrscheinlichkeit einer Sanktionierung von Zuwiderhandlungen nach EU-Recht und dem Recht des Drittlands sowie
- der Ausschluss unzulässiger Übermittlungen durch geeignete technische und organisatorische Maßnahmen.

Bietet der Auftragsverarbeiter nach dieser Prüfung keine hinreichenden Garantien, sind die Risiken der europarechtswidrigen Datenverarbeitung durch technische und/oder organisatorische Maßnahmen auszugleichen, die genau diejenigen Defizite der Rechtslage oder -praxis des drittstaatlichen Rechts ausgleichen, die zu der mangelnden Zuverlässigkeit des Auftragsverarbeiters geführt haben. Für die Frage, welche Maßstäbe an diese Maßnahmen zu stellen sind, können Verantwortliche die Empfehlungen 01/2020 des Europäischen Datenschutzausschusses heranziehen, wobei jedoch zu beachten ist, dass diese Empfehlungen für den Kontext von Datenübermittlungen in Drittländer konzipiert worden sind,6 sodass abweichende Bewertungen der Eignung bestimmter Maßnahmen nicht ausgeschlossen sind. Soweit eine Verarbeitung personenbezogener Daten im Auftrag den Zugriff des Auftragsverarbeiters auf Klardaten erfordert, ist in entsprechender Anwendung des Anwendungsfalls 6 des Anhangs 2 der Empfehlungen 01/2020 besonders kritisch zu prüfen, wie den Anforderungen des Art. 28 Abs. 1 DSGVO ausreichend Rechnung getragen werden kann.

5. Der Verantwortliche muss in der Lage sein, den Nachweis zu führen, dass ein Auftragsverarbeiter die Anforderungen aus Art. 28 Abs. 1 und ErwG 81 DSGVO an Fachwissen, Zuverlässigkeit und Ressourcen erfüllt.

Die DSK wird sich auf der Grundlage dieses Beschlusses für eine weitere Behandlung dieser Fragestellung im Europäischen Datenschutzausschuss (EDSA) einsetzen.

Bild-Nachweise

Abbildung 1 | Seite 5 – LDI NRW;
Abbildung 2 | Seite 9 – Bildagentur PantherMedia / artjazz;
Abbildung 3 | Seite 13 – Bildagentur PantherMedia / faabi (YAYMicro);
Abbildung 4 | Seite 17 – Bildagentur PantherMedia / Andriy Popov;
Abbildung 5 | Seite 25 – PantherMedia / Birgit Korber;
Abbildung 6 | Seite 29 – Gerichtshof der Europäischen Union;
Abbildung 7 | Seite 33 – PantherMedia / Yuri Arcurs;
Abbildung 8 | Seite 37 – Bildagentur PantherMedia / NewAfrica;
Abbildung 9 | Seite 41 – Bildagentur PantherMedia /spirit-alex;
Abbildung 10 | Seite 47 – PantherMedia / paolo de santis;
Abbildung 11 | Seite 53 – Bildagentur PantherMedia / dpcrestock (Dirk Püschel);
Abbildung 12 | Seite 55 – Bildagentur PantherMedia / heiko119;
Abbildung 13 | Seite 62 – PantherMedia / Peter Wienerroither;
Abbildung 14 | Seite 65 – PantherMedia / vilevi (YAYMicro);
Abbildung 15 | Seite 70 – PantherMedia / Lenets_Tatsiana;
Abbildung 16 | Seite 73 – PantherMedia / AntonMatyukha;
Abbildung 17 | Seite 81 – PantherMedia / Melpomene;
Abbildung 18 | Seite 85 – Bildagentur PantherMedia / Funtap;
Abbildung 19 | Seite 88 – PantherMedia / Ilka Erika Szasz-Fabian;
Abbildung 20| Seite 90 – Bildagentur PantherMedia / Przemyslaw Klos;
Abbildung 21 | Seite 92 – Bildagentur PantherMedia / dimmushka;
Abbildung 22 | Seite 95 – PantherMedia / uflypro (YAYMicro);
Abbildung 23 | Seite 104 – Gerichtshof der Europäischen Union;
Abbildung 24 | Seite 107 – Bildagentur PantherMedia / Kiyoshi Takahase Segundo.

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

Diese Broschüre kann unter www.ldi.nrw.de abgerufen werden.
Zitiervorschlag: 29. Bericht LDI NRW
ISSN: 0179–2431
Düsseldorf 2024
Titelbild © Bildagentur PantherMedia / kentoh (YAYMicro)
Gedruckt auf chlorfreiem Recyclingpapier

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