28. Bericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Bettina Gayk

zum Datenschutz

für die Zeit vom 1. Januar 2022 bis zum 31. Dezember 2022

und zur Informationsfreiheit

für die Zeit vom 1. Januar 2021 bis zum 31. Dezember 2022

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: 28. Bericht LDI NRW

ISSN: 0179–2431

Düsseldorf 2023

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

Vorwort

Seit Mai 2018 und damit seit fünf Jahren gilt die Datenschutz-Grundverordnung – kurz die DS-GVO. Sie hat die Betroffenenrechte deutlich gestärkt und eine enge Zusammenarbeit der Datenschutzaufsichtsbehörden vorgegeben, damit die Regelungen einheitlich angewendet werden. Dies erforderte einen grundlegenden Anpassungsprozess in meiner Behörde in ihrer Funktion als Datenschutzaufsicht. Die Zahl der Beschwerden und die Beratungsersuchen der Stellen, die personenbezogene Daten verarbeiten, haben sich nach dem Inkrafttreten der DS-GVO verdreifacht. Dies zeigte, dass das Bewusstsein der Betroffenen für die eigenen Datenschutzrechte durch die neuen Regelungen gestärkt wurde. Wir agieren bei der Beschwerdebearbeitung nicht mehr als bloße Petitionsinstanz, sondern führen nun förmliche Verwaltungsverfahren und können, wie jede andere Verwaltungsbehörde, verklagt werden.

Die Verfahren, die eine europaweit einheitliche Anwendung der DS-GVO sicherstellen sollen, sind ein einzigartiges Projekt der europäischen Behördenzusammenarbeit. In grenzüberschreitenden Fällen sollen nicht detailliertere untergesetzliche Ausführungsvorschriften eine einheitliche Anwendung der DS-GVO garantieren, sondern zeitlich eng getaktete Abstimmungsverfahren zwischen den europäischen Datenschutzaufsichtsbehörden. Das ist für meine Behörde oft arbeitsintensiv, aber notwendig. Ebenso mit dem Ziel der einheitlichen Auslegung der DS-GVO arbeiten meine Mitarbeiter*innen in Arbeitsgruppen des EDSA mit und erarbeiten dort Leitlinien zu ihrer Anwendung. Dies ist eine wichtige Arbeit, die auch den Stellen hilft, die unsere Beratung zur richtigen Anwendung der

neuen Vorschriften erfragen. Unser Ziel ist hier, europaweit einheitliche Antworten geben zu können.

Ich möchte mich an dieser Stelle ausdrücklich bei den Mitgliedern des Landtags dafür bedanken, dass sie mich darin unterstützen, dass die Behörde die Herausforderungen bewältigen kann, die mit der DS-GVO entstanden sind. Dass ich in diesem Haushaltsjahr zusätzliches Personal zur Verfügung gestellt bekommen habe, hilft dabei sehr. Auch den Beschäftigten meines Hauses bin ich sehr dankbar, dass sie den Weg der notwendigen Veränderungen konstruktiv mitgehen. Die Neueinstellungen werden die Belastungen verringern.

Die DS-GVO wird nicht die einzige Herausforderung für die Datenschutzaufsicht bleiben. Die Europäische Kommission hat im Rahmen ihrer Datenstrategie einen Prozess angestoßen, mit dem sie das Potential von Daten für die Allgemeinheit, aber auch als Wirtschaftsgut ausschöpfen will. Sie hat dazu eine ganze Reihe von Gesetzgebungsverfahren eingeleitet, die Rückwirkungen auf die Datenschutzaufsicht haben werden. Die Kommission betont bei allen Verfahren, dass sie den Datenschutz gewährleisten will und die Vorschriften der DS-GVO unangetastet bleiben. Ob dies in der Praxis gelingt, wird von der Datenschutzaufsicht zu überwachen sein. Hier werden neue Aufgaben auf die Datenschutzbehörden zukommen oder zumindest neue Rahmenbedingungen entstehen. Der Bericht geht auf die einzelnen Vorhaben der Strategie ein.

Nicht nur der sich ändernde Rechtsrahmen, sondern auch die rasant fortschreitende technische Entwicklung sind ständig daraufhin zu prüfen, ob personenbezogene Daten rechtmäßig verarbeitet werden. In aller

Munde ist die Künstliche Intelligenz (KI). Sie scheint Segen und Fluch zugleich zu sein. Sicher ist sie eine enorme Herausforderung für den Datenschutz, der garantiert, dass jede*r erfahren können muss, wer welche Daten zur eigenen Person verarbeitet, dass diese Daten richtig sind und nur mit gesetzlicher Erlaubnis oder Einwilligung der betroffenen Person verarbeitet werden. KI wertet in der Regel große Massen von Daten aus, und es ist oft schwierig nachzuvollziehen, ob all diese Daten rechtmäßig verarbeitet werden und auch richtige Daten enthalten. KI ist nach dem Internet und den Sozialen Medien eine weitere Entwicklung, deren Nutzen, aber auch deren Gefahren wir im Blick behalten müssen. Insbesondere dann, wenn es um die Bewertung von Menschen und ihrer Verhaltensweisen geht, muss es klare Grenzen für den Einsatz von KI geben, die Menschen vor diskriminierenden Ergebnissen schützt und sie vor einer Beurteilung bewahrt, die auf reiner Statistik oder gar auf einer unsoliden Datenbasis beruht. Eine Verordnung zur Regulierung von KI hat die Europäische Union vorgelegt. Eine Verabschiedung lässt leider noch auf sich warten.

KI kann etwa in der medizinischen Diagnostik ein außerordentlich gutes Hilfsmittel sein. Werden beispielsweise Bilder von bestimmten Erkrankungen maschinell ausgewertet, kann KI viel besser als das menschliche Auge bei einem zu diagnostizierenden Vergleichsbild die Erkrankung feststellen oder ausschließen. Solche Anwendungen, deren Nutzen niemand bestreitet, sind umso besser, je mehr Vergleichsmaterial von der KI ausgewertet werden konnte. Das heißt, dass von einer Krankheit Betroffene ihre Bilder zum Training der KI zur Verfügung stellen müssen, damit solche Verfahren optimiert werden können. Gesundheitsdaten sind sensible Daten und es

wird zu diskutieren sein, unter welchen Umständen es im allgemeinen Interesse erlaubt werden kann, dass diese Daten für KI-Training zur Verfügung stehen.

ChatGPT hingegen, das zurzeit in aller Munde ist, produziert Ergebnisse unter anderem durch Verknüpfung von Daten, die im Internet verfügbar sind. Das erzeugt bei Auskünften über natürliche Personen teils merkwürdige Ergebnisse. Ein Selbstversuch, in dem ChatGPT gefragt wurde, was über mich bekannt ist, hat mir in meiner Biografie neue und willkommene Qualifikationen verschafft, die ich aber leider nicht habe. Das belastet mich persönlich bisher noch nicht so sehr. Ein australischer Bürgermeister hat für sich hingegen Anlass für eine Klage gesehen, denn ihm wurde eine Beteiligung an einem Bestechungsskandal durch die KI hinzugedichtet. In anderen Einsatzbereichen, wie etwa dem Schreiben von Gedichten, soll diese KI teils erstaunlich gute Ergebnisse produzieren. Unter dem Aspekt des Persönlichkeitsschutzes aber werden die Datenschutzaufsichtsbehörden sich mit solchen KI-Anwendungen intensiv befassen müssen. Auch der Entwurf der KI-Verordnung, den die Europäische Kommission vorgelegt hat, sieht den Bedarf, die Datenschutzaufsichtsbehörden bei der Beurteilung von KI einzubeziehen, wenn es um die Verarbeitung personenbezogener Daten geht.

Dieser Bericht gibt Einblick in einige Aufgabenstellungen, die uns als Datenschutzaufsicht im zurückliegenden Jahr beschäftigt haben. Darüber hinaus enthält er den Informationsfreiheitsbericht, der alle zwei Jahre vorgelegt wird. Hier möchte ich besonders auf die Veranstaltung hinweisen, die wir aus Anlass des 20. Geburtstags des Informationsfreiheitsgesetzes in

Nordrhein-Westfalen gemeinsam mit dem Landtagspräsidenten in den Räumen des Landtags veranstaltet haben. Dem Landtagspräsidenten, der die Veranstaltung möglich gemacht hat, und auch seinem Vertreter, der die Veranstaltung durch seinen Zeitzeugenbericht aus der Gesetzgebungsphase sehr bereichert hat, darf ich an dieser Stelle noch einmal besonders danken.

Das IFG NRW ist inzwischen also mehr als volljährig. Aus meiner Sicht ein guter Anlass, sich Gedanken darüber zu machen, dass diese Regelungen weiterentwickelt und um Elemente der in anderen Ländern bereits verabschiedeten Transparenzgesetze ergänzt werden. Hier geht es darum, dass allgemein interessierende Informationen den Bürger*innen aktiv und leicht zugänglich gemacht werden. Für Informationen, die aktiv veröffentlicht werden, müssen Informationsanträge gar nicht mehr gestellt und von der Verwaltung auch nicht mehr bearbeitet werden. Zudem sind unmittelbare Informationen, die die Verwaltung über ihr Handeln zur Verfügung stellt, ein gutes Mittel, um Fake News über das Verwaltungshandeln vorzubeugen.

Bettina Gayk

Düsseldorf im Frühjahr 2023

Abkürzungsverzeichnis

Abs.	Absatz
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BfDI	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BGB	Bürgerliches Gesetzbuch
DSK	Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DS-GVO	Datenschutz-Grundverordnung
EDSA	Europäischer Datenschutzausschuss (englisch European Data Protection Board: EDPB)
SGB	Sozialgesetzbuch
TKG	Telekommunikationsgesetz
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz

1. Teil: Datenschutzbericht

1. Überblick

- **Eingaben**

  Im Jahr 2022 haben uns insgesamt rund **10.800 schriftliche Eingaben** erreicht, einschließlich Meldungen nach Art. 33 DS-GVO (sog. Datenpannen). Etwa 380 Eingaben im Jahr 2022 betrafen das Thema Informationsfreiheit. Im Jahr 2021 haben wir dazu etwa 450 Eingaben erhalten.

  Weitere Einzelheiten zu den **Eingaben** und **Beschwerden** sowie **Meldungen von Datenschutzverletzungen, Abhilfemaßnahmen, Europäischen Verfahren** und **Rechtsetzungsvorhaben** finden sich unter 2. im Kapitel „Zahlen und Fakten“.

- **Anlasslose Prüfungen**

  Im Jahr 2022 haben wir mehrere Kontrollen bzw. Prüfungen durch- bzw. weitergeführt:

  - Überprüfung des berechtigten Interesses bei Bonitätsabfragen bei Wirtschaftsauskunfteien. Siehe hierzu unter 9.1.
  - Datenschutzbeauftragte bei Detekteien. Siehe hierzu unter 9.2.
  - Ausschreibungen im Schengener Informationssystem der zweiten Generation (SIS-II). Siehe hierzu unter 6.3.
  - Lichtbildabgleiche zu Fahrer*innenermittlungen bei Ordnungswidrigkeiten. Siehe hierzu unter 6.4.
  - Verfahrensrückmeldungen der Staatsanwaltschaften an die Polizeibehörden. Siehe hierzu unter 6.5.

- **Informationen und Öffentlichkeitsarbeit**

  Unser allgemeines und laufend aktualisiertes Informationsangebot finden Sie auf unserer Internetseite www.ldi.nrw.de.

  Alle Veröffentlichungen der DSK sind auf der gemeinsamen Internetseite www.datenschutzkonferenz-online.de abrufbar.

  Wir beteiligen uns am **Virtuellen Datenschutzbüro** www.datenschutz.de, das Bürger*innen als erste zentrale Informations- und Anlaufstelle dient. Insbesondere um Jugendliche zu erreichen, beteiligen wir uns zudem an der Webseite **www.youngdata.de**.

- **Vorträge und Erfahrungsaustausche**
  - Vortrag zum Datenschutz im Bereich der Bewährungshilfe/Führungsaufsicht – Anforderungen an die Übermittlung personenbezogener Daten beim Fachverband für Soziale Arbeit, Strafrecht und Kriminalpolitik (DBH e.V)
  - Vortrag zu den Erfahrungen der LDI NRW bei der Umsetzung der DS-GVO und datenschutzrechtliche Konsequenzen im Falle eines Hackerangriffs beim 15. Kommunalen Datenschutzkongress
  - Podiumsdiskussionen zum Stellenwert von Grundrechten (insbesondere Datenschutz) in einer demokratischen Gesellschaft im Rahmen der Schul-Projekttage Überwachung 2.0
  - Vortrag zur Datenübermittlungen zwischen öffentlichen Stellen bei der Hochschule des Bundes
  - Teilnahme am Jahrestreffen der behördlichen Datenschutzbeauftragten an Schulen in NRW der Medienberatung NRW

- Teilnahme am Jahrestreffen der behördlichen Datenschutzbeauftragten an Schulen im Regierungsbezirk Arnsberg
- Vortrag zur Anwendung des IFG NRW in der Justizverwaltung bei der Justizakademie NRW
- Austausch mit regionalen Erfahrungsaustauschkreisen der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)
- Erfahrungsaustausch mit Kreditinstituten in NRW
- Vortrag zu aktuellen Themen der Datenschutzaufsicht und Best Practices bei der Fachtagung Datenschutz der Sparkassenakademie NRW
- Vortrag „The Open Banking Approach of PSD2“ beim Virtual Workshop OECD/Future of Privacy Forum: Data Portability in Open Banking: Privacy and other Cross-Cutting Issues
- Austausch zur Markterhebung Kontoinformationsdienste (PSD2) bei der Verbraucherzentrale Bundesverband e.V.
- Jährlicher Erfahrungsaustausch zwischen den Hochschuldatenschutzbeauftragten NRW und der LDI NRW
- Treffen mit dem Bankenverband auf europäischer Ebene (European Banking Federation)
- Erfahrungsaustausch mit Versicherungsunternehmen
- Hackerangriffe aus der Sicht der LDI NRW bei der Kommunal Agentur NRW

- **Datenschutzkonferenz und Expertengruppen des Europäischen Datenschutzausschusses**

  Die Beauftragten des Bundes und der Länder besprechen wichtige Datenschutzfragen in der **DSK** und streben einheitliche Bewertungen an, die in **Arbeitskreisen** vorbereitet werden.

Im Rahmen der DSK leitet die LDI NRW die Arbeitskreise

- Wirtschaft (vormals Düsseldorfer Kreis),
- Statistik und
- Kreditwirtschaft.

Die Leitung des Arbeitskreises Auskunfteien, den wir bisher gemeinsam mit Hessen geführt haben, haben wir an das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) abgegeben. Wir werden dafür gemeinsam mit dem BayLDA zukünftig den Arbeitskreis Adresshandel und Werbung leiten.

Der **Europäische Datenschutzausschuss** hat zu seiner Unterstützung mehrere Ausschüsse – sog. **Expert Subgroups** – gebildet, in denen auch die nationalen Aufsichtsbehörden vertreten sind. Die LDI NRW ist in den Expert Subgroups

- Key Provisions,
- Compliance, E-Government & Health und
- Financial Matters

aktiv und vertritt dort die deutschen Aufsichtsbehörden.

Eine Mitarbeiterin der LDI NRW war für einen Monat im Sekretariat des EDSA eingesetzt. Praktische Erfahrungen und Eindrücke von dort verbessern die Zusammenarbeit mit dem EDSA-Sekretariat und anderen Aufsichtsbehörden.

2. Zahlen und Fakten

- **Eingabesituation im Überblick**

  Im Jahr **2022** haben uns insgesamt rund **10.480** schriftliche Eingaben erreicht, einschließlich Meldungen nach Art. 33 DS-GVO – sog. Datenpannen. Grundsätzlich nicht erfasst haben wir die zahlreichen telefonischen Anfragen.

  Im Jahr 2021 waren es 11.900 schriftliche Eingaben, 2020 waren es 12.150 und 2019 waren es insgesamt etwa 12.500.

  Von den Eingaben waren

  - **6.136 Beschwerden** nach Art. 77 DS-GVO,
  - **522** von **Dritten gemeldete Beschwerden**,
  - **947 schriftliche Beratungsanfragen**,
  - **17 Begleitungen bei Rechtsetzungsvorhaben,**
  - **1 Genehmigungsverfahren,**
  - **1.829 Meldungen nach Art. 33 DS-GVO** zu sog. Datenpannen und
  - **277 Eingaben ohne Kategorie.**

- **Beschwerden und Beratungsanfragen**

  Im Jahr 2022 haben uns **6.136 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 Amts wegen aufgreifen. Solche **Eingaben von Dritten** haben wir **522** erhalten.

Schriftliche **Beratungsanfragen** haben wir **947** erhalten, sowohl von Verantwortlichen als auch von Auftragsverarbeitern und betroffenen Personen.

- **Meldungen von Datenschutzverletzungen**

  Meldungen nach Art. 33 DS-GVO zu sog. Datenpannen haben uns **1.829** erreicht. Im Jahr 2021 waren es 1.841, 2020 waren es 1.775 Meldungen und 2019 waren es 2.235 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.

  Als Maßnahme nach **Art. 58 Abs. 2 Buchstabe i** wurden bei der Zentralen Bußgeldstelle der LDI NRW **156** Bußgeldverfahren eingeleitet bzw. zur weiteren Verfolgung von den Staatsanwaltschaften übernommen. **85** Bußgeldbescheide wurden erlassen und **123** Verfahren wurden durch Rechtskraft, Einstellung oder Gerichtsentscheidungen abgeschlossen. Die aus den Bußgeldverfahren vom Land vereinnahmten Gelder stellen sich wie folgt dar:

Anzahl Bußgeldbescheide	Betrag in Euro	Gesamtbetrag in Euro
3	150	450
21	250	5.250
27	500	13.500
1	650	650
13	1.000	13.000
12	1.500	18.000
2	2.500	5.000
2	3.000	6.000
1	3.500	3.500
3	5.000	15.000
85		**80.350**

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

- **868 Hinweise** nach Art. 58 Abs. 1 d),
- **26 Warnungen** nach Art. 58 Abs. 2 a),
- **20 Verwarnungen** nach Art. 58 Abs. 2 b),
- **45 Anweisungen** nach Art. 58 Abs. 2 d).

Davon erfasst sind Verfahren, die bereits in den Vorjahren eingeleitet wurden, während viele im Jahr 2022 begonnene Verfahren noch nicht beendet und nicht erfasst sind. Oft sind die Verfahren sowohl in

zeitlicher als auch in rechtlicher Hinsicht aufwändig. 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 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 2022 war die LDI NRW in **1.721 Fällen** mit gestarteten IMI-Modulen befasst. Im Jahr 2021 waren es 1.558 Fälle. Im Jahr 2020 waren es ebenfalls 1.558 und im Jahr 2019 1.390 Fälle.

Wir hatten bei vier europäischen Verfahren die Federführung, bei 22 Verfahren waren wir in unserer Zuständigkeit betroffen und in 11 Verfahren nach Art. 60 ff. DS-GVO (Zusammenarbeit oder Kohärenzverfahren) beteiligt.

- **Förmliche Begleitung bei Rechtsetzungsvorhaben**

  Im Jahr 2022 wurde die LDI NRW bei **17** Rechtsetzungsvorhaben beteiligt. Im Jahr 2021 waren es 33 und im Jahr 2020 insgesamt 44 Vorhaben.

  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). In einzelnen Verfahren war die Beteiligung sehr kurzfristig. Vor allem, wenn wir von einem

Gesetzgebungsverfahren erst im Zusammenhang mit der Kabinettbeteiligung vor Verbändeanhörung oder gar Einbringung in den Landtag erfahren, ist es oft schwierig, noch sachdienliche Hinweise zu geben. Werden wir hingegen schon frühzeitig vom zuständigen Ressort in die Erarbeitung von Regelungen mit Datenschutzrelevanz einbezogen, können wir darauf hinwirken, dass die entscheidenden Fragen von vornherein datenschutzkonform gelöst werden.

Unsere Hinweise in den Beteiligungsverfahren wurden vielfach aufgegriffen und umgesetzt. Ein Fokus unseres Tätigwerdens in diesem Bereich lag dabei zum einen weiterhin auf der Aufrechterhaltung des bestehenden Datenschutzniveaus in NRW und zum anderen auf der umfassenden Umsetzung der Anforderungen der DS-GVO und der JI-Richtlinie.

Wir wurden in unterschiedlicher Intensität und in verschiedenen Phasen der Verfahren von der Landesregierung bei den folgenden Gesetzesvorhaben beteiligt:

- Gesetz zur Anpassung des Polizeigesetzes des Landes Nordrhein-Westfalen und anderer Gesetze an das Telekommunikation-Telemedien-Datenschutz-Gesetz
- Entwurf eines Gesetzes über die Beauftragte oder den Beauftragten für den Opferschutz des Landes Nordrhein-Westfalen
- Gesetz zur Einführung digitaler Sitzungen für kommunale Gremien und zur Änderung kommunaler Vorschriften
- Digitalsitzungsverordnung
- Ausbildungs- und Prüfungsverordnung für Rettungssanitäter*innen sowie Rettungshelfer*innen

- Flüchtlingsaufnahmegesetz-Datenschutzverordnung
- Justizgesetz NRW
- Verordnung über die Einrichtung von Distanzunterricht (Distanzunterrichtsverordnung)
- Änderung der Meldedatenübermittlungsverordnung
- Aktualisierung des NRW-Ausführungserlasses zum Staatsangehörigkeitsrecht
- Gesetz zur Umsetzung des Gesetzes über die Berufe in der medizinischen Technologie in Nordrhein-Westfalen
- Gesetz zur Umsetzung des Sofortzuschlages gem. § 145 SGB XII
- Gesetz zur Umsetzung des Gesetzes über den Beruf der pharmazeutisch-technischen Assistentin und des pharmazeutisch-technischen Assistenten und zur Anpassung weiterer landesrechtlicher Regelungen (PTA-Umsetzungsgesetz NRW)
- Gesetzesentwurf Einführung Corona-Sonderzahlung, Anpassung Dienst- und Versorgungsregelungen

3. Datenstrategie der EU – neue Regelungen

Die Datenstrategie der EU stellt seit 2020 den Rahmen und die Zielrichtung für verschiedene EU-Regelungen bereit, von denen einige bereits in Kraft sind. Die Folgen für den Schutz personenbezogener Daten sind differenziert zu betrachten.

Die Datenstrategie behandelt Regulierungsansätze für Datenzugang und Datennutzung, Investitionen, Kompetenzen von Einzelnen und Unternehmen sowie das Konzept der europäischen Datenräume. Zugleich will sie die europäischen Grundrechte gewährleisten. Abgeleitet aus der Strategie sind die folgenden EU-Rechtsakte:

Der **Daten-Governance-Rechtsakt** (Data Governance Act, Verordnung (EU) 2022/868) trifft Regelungen zur Weiterverwendung von bestimmten Daten von öffentlichen Stellen, zu Datenvermittlungsdiensten und zum Datenaltruismus. Zudem führt er einen europäischen Dateninnovationsrat ein. Der Rechtsakt ist keine Rechtsgrundlage zur Datenverarbeitung und lässt das Datenschutzrecht unberührt. Die Regelung ist in Kraft und ab September 2023 anzuwenden.

Datenvermittlungsdienste (auch „PIMS“, personal information management services genannt) könnten Lösungen beispielsweise für das Einwilligungsmanagement bei Internetseiten bieten. Beim Datenaltruismus geht es um Einwilligungen für die Nutzung von Daten für Gemeinwohlzwecke. Welche Auswirkungen dies auf die Praxis haben wird, ist noch offen.

Der Europäische Dateninnovationsrat ist unter anderem für die Entwicklung von europäischen Datenräumen von Bedeutung. Der EDSA ist dort Mitglied, so

dass auch die LDI NRW hier Positionen (mit-)beeinflussen kann.

Welche Aufsichtsbehörden in Deutschland welche Aufgaben übernehmen, ist noch offen. Denkbar wäre eine Anbindung von Aufgaben auch bei den Datenschutzaufsichtsbehörden. Wenn andere Behörden die Aufgaben wahrnehmen, wäre die Zusammenarbeit mit der Datenschutzaufsicht notwendig, soweit es um personenbezogene Daten geht. In beiden Varianten werden neue Aufgaben auf die LDI NRW zukommen.

Das **Datengesetz (Data Act)** soll den Datenaustausch und die Datennutzung sowohl zwischen Unternehmen und Verbraucher*innen als auch zwischen Unternehmen regeln. Betroffen sind daher viele Produkte und Dienstleistungen, die mit Daten arbeiten. Dazu zählen auch „Internet-of-Things“-Anwendungen, medizinische Geräte und virtuelle Assistenten.

Das Gesetz ist noch im Gesetzgebungsverfahren. Der EDSA und der Europäische Datenschutzbeauftragte haben dazu Änderungsvorschläge gemacht. Dabei ist wichtig, deutlicher zu regeln, dass die Datenschutzregelungen unberührt bleiben und keine Unklarheiten durch die neuen Regelungen entstehen.

Welche Aufsichtsbehörden die Aufgaben nach dem Gesetz erhalten, ist noch offen.

Das **Gesetz über digitale Dienste** (Digital Services Act, Verordnung (EU) 2022/2065) soll eine transparente und sichere Online-Umgebung gewährleisten. Es hat insbesondere zum Ziel, Risiken und Gefahren für die Gesellschaft zu begegnen, die aus den Geschäftsmodellen hinter vielen Online-Plattformen und

den eingesetzten Algorithmen resultieren. Dabei werden jeweils spezifische Pflichten für verschiedene Kategorien von Online-Intermediären (Betreiber von Vermittlungs- und von Hostingdiensten sowie Betreiber von mittelgroßen, großen und sehr großen Online-Plattformen) begründet. Das Gesetz betrifft etwa die Gestaltung von Algorithmen, Maßnahmen gegen die Verbreitung von Hassreden, die Kennzeichnung von Deep Fakes und das Verbot von Dark Patterns. Es ist in Kraft und spätestens ab Februar 2024 anzuwenden.

Für gezielte Online-Werbung und Profiling werden Transparenz- und Rechenschaftsregeln verbessert. Weitere Einschränkungen oder ein Verbot sind nicht geregelt worden. Dies hätte zu einer zusätzlichen Verbesserung des Datenschutzes im Internet beitragen können. Auch dieses Gesetz soll Datenschutzrecht nicht beeinträchtigen.

Zwischen den Behörden, die die Anwendung dieses Gesetzes beaufsichtigen werden, und den Datenschutzaufsichtsbehörden sollte eine gute Zusammenarbeit angestrebt werden.

Das **Gesetz über digitale Märkte** (Digital Markets Act, Verordnung (EU) 2022/1925) bestimmt Pflichten für sehr große Betreiber von Internet-Plattformen (sog. Gatekeeper), damit diese ihre Marktmacht nicht missbrauchen können. Für diese Unternehmen sollen beispielsweise Selbstbegünstigungsverbote, Diskriminierungsverbote und Verpflichtungen zur Interoperabilität gelten. Die Aufsicht über die Gatekeeper führt die EU-Kommission. Auch wenn das Gesetz vorrangig Wettbewerb und Verbraucherschutz betrifft, kann es zu Reibungen mit Datenschutzvorschriften kom-

men. Außerdem nimmt das Gesetz in einigen Vorschriften Bezug auf die DS-GVO. Es kann deren Schutzniveau ergänzen und bei der Durchsetzung helfen.

Das Gesetz ist in Kraft und ab Mai 2023 anzuwenden.

Das **Gesetz über Künstliche Intelligenz (Artificial Intelligence Act)** soll einen Rechtsrahmen für den sicheren und gesetzeskonformen Betrieb von KI-gestützten Systemen schaffen. Dabei soll die Entwicklung von KI-Systemen in der EU gefördert werden. Das Gesetz enthält eine nach Risiken abgestufte Regulierung. Danach sind bestimmte Systeme verboten oder unterliegen als Hochrisiko-Systeme besonderen Anforderungen. Die Erfüllung der gesetzlichen Anforderungen muss durch eine Konformitätsbewertung bereits vor der Bereitstellung auf dem Markt nachgewiesen werden. Nationale Aufsichtsbehörden überwachen den Markt. Das Gesetz ist noch im Gesetzgebungsverfahren.

Zu den Verbesserungsvorschlägen für den Gesetzentwurf gehören ein Verbot der automatisierten Erkennung von personenbezogenen Merkmalen in öffentlichen Räumen und ein Verbot der Bewertung von sozialem Verhalten.

Bei der Frage, welche Aufsichtsbehörde national für das Gesetz zuständig sein soll, ist zu berücksichtigen, dass der Regelungsgehalt über Datenschutzfragen hinausgeht. Es liegt deshalb nicht nahe, einer Datenschutzaufsichtsbehörde die Zuständigkeit für das gesamte Gesetz zuzuweisen. Es ist aber wichtig, dass die Datenschutzaufsichtsbehörden eingebunden werden, soweit sie nicht selbst die Aufsicht nach dem

KI-Gesetz führen, wenn KI personenbezogene Daten nutzt oder Personen bewertet.

Die Vorbereitungen für europäische Datenräume, bei denen für bestimmte Sektoren besondere Regeln geschaffen werden sollen, sind unterschiedlich weit gediehen. Der EDSA wird die Entwürfe sorgfältig prüfen und Stellungnahmen abgeben. Einen Entwurf gibt es etwa für den Europäischen Gesundheitsdatenraum. Die in dem Entwurf vorgesehene Sekundärnutzung privilegiert bestimmte Datennutzungen. Nach erster Einschätzung dürfte der vorgelegte Entwurf bei der Sekundärnutzung sensibler Gesundheitsdaten noch nicht den notwendigen Schutz bieten, um den Datenschutz der Betroffenen zu gewährleisten.

Eine erste Gesamtbewertung erweckt zunächst den Eindruck, dass die neuen Regelungen darauf abzielen, Daten möglichst vielfältig und leicht nutzen zu können. Die Datennutzung wird dafür mit einigen Zusatzregeln sowie einer Aufsichts- und Genehmigungsbürokratie abgesichert. Manche meinen sogar, das datenschutzrechtliche Prinzip der Datensparsamkeit werde abgeschafft.

Auf den zweiten Blick wird aber deutlich, dass die neuen Gesetze in aller Regel gerade keine neuen Rechtsgrundlagen für den Umgang mit personenbezogenen Daten bestimmen. Vielmehr soll das Datenschutzrecht grundsätzlich unberührt bleiben, übrigens auch das Prinzip der Datensparsamkeit. Die politische Entscheidung, ob bestimmte Datenverarbeitungen generell zulässig sein sollen oder nicht, wird für viele Fälle gar nicht getroffen. Voraussichtlich werden deshalb in der Praxis viele Verarbeitungen von perso-

nenbezogenen Daten davon abhängen, ob die betroffene Person dafür eine Einwilligung abgegeben hat – nicht anders als bisher.

Da das Ziel der intensiveren Datennutzung trotzdem zu erkennen ist, werden die Datenschutzaufsichtsbehörden gerade mit den neuen Gesetzen verstärkt darauf achten müssen, dass die bekannten Datenschutzregeln eingehalten werden.

Im Einzelnen ist oft noch gar nicht klar, welche Behörden für die neuen Aufgaben zuständig sein werden.

Die Gesetze, die aus der Datenstrategie abgeleitet werden, enthalten viele Schnittstellen zu datenschutzrechtlichen Regelungen und erhebliches Konfliktpotenzial. Auch wenn sie häufig Datenschutzrecht ausdrücklich unberührt lassen, wird angestrebt, personenbezogene Daten vermehrt zu nutzen. Sowohl bei der Gesetzgebung als auch bei der Anwendung der neuen Gesetze müssen Datenschutzaufsichtsbehörden sehr aufmerksam auf die datenschutzrechtlichen Folgen achten.

4. Internet und Medien

4.1 Was passiert jetzt mit Facebook-Seiten von Behörden?

Die deutschen Datenschutz-Aufsichtsbehörden haben festgestellt, dass Facebook-Seiten (früher als Fanpages bezeichnet) derzeit nicht datenschutzkonform betrieben werden können. Die Aufsichtsbehörden wirken deshalb darauf hin, dass von Landes- bzw. Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können. Nicht nur Behörden, sondern auch Unternehmen und Private, die sich datenschutzkonform verhalten wollen, sind gut beraten, auf eigene Facebook-Seiten zu verzichten, denn der Nachweis der Datenschutzkonformität wird derzeit kaum geführt werden können.

Spätestens auf Basis der Arbeiten einer zur datenschutzrechtlichen Bewertung eingesetzten Taskforce ist unter den Datenschutzbehörden unstreitig, dass ein rechtskonformer Betrieb von Facebook-Seiten nicht möglich ist. Es fehlt an einer hinreichend klaren Information über die beim Aufruf einer solchen Seite ausgelösten Verarbeitungen der Nutzerdaten sowie an einer wirksamen Einwilligung in verschiedene Verarbeitungen nach § 25 TTDSG und Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a und Art. 7 DS-GVO. Auch die Übermittlung personenbezogener Daten in Drittländer außerhalb der EU und des EWR wirft Fragen auf. Den Abschluss einer Vereinbarung zwischen META/Facebook und den Seitenbetreiber*innen, mit der zentrale Zuständigkeiten für die Erfüllung der da-

tenschutzrechtlichen Pflichten geregelt werden, verweigert META/Facebook und bietet eine solche Vereinbarung nur mit Blick auf die sog. Insights an, eine statistische Übersicht, die META/Facebook für die oder den jeweiligen Seitenbetreiber*in erstellt.

Vor diesem Hintergrund werden die Datenschutz-Aufsichtsbehörden gegenüber den Betreiber*innen der Seiten tätig. Der BfDI hat eine Anhörung zu einer beabsichtigten Untersagung des Betriebs einer Facebook-Seite an das Bundespresseamt (BPA) versandt und auch die LDI NRW ist in Gesprächen mit dem Landespresse- und Informationsamt NRW. Der Anhörung des BfDI ist zu Beginn des Jahres 2023 eine Untersagungsverfügung gefolgt. Wir rechnen damit, dass es zu einer gerichtlichen Klärung über die Frage der Zulässigkeit des Betriebs derartiger Auftritte öffentlicher Stellen in sozialen Netzwerken kommen wird. Unabhängig von Maßnahmen, die wir im ersten Schritt in Bezug auf Oberste Landesbehörden noch vorbereiten, gehen wir momentan nicht gegen weitere Behörden vor, wenn sie als Verantwortliche für Facebook-Seiten wichtige Bedingungen erfüllen:

- Öffentliche Stellen müssen gewährleisten, dass die in sozialen Medien geteilten Inhalte jederzeit und jedenfalls gleichzeitig auch über alternative digitale Verbreitungswege, zum Beispiel eine „normale“ Website, zugänglich sind. Im Ergebnis darf niemand gezwungen sein, soziale Netzwerke zur Informationsbeschaffung aufzusuchen. Öffentliche Stellen dürfen keine Anreize für Bürger*innen setzen, soziale Netzwerke zu nutzen und so ggf. sensible persönliche Informationen preiszugeben.

- Auftritte in sozialen Medien – von öffentlichen sowie von nicht-öffentlichen Stellen – müssen über eine adäquate Datenschutzerklärung verfügen. Aus ihr muss deutlich werden, dass der Betreiber/die Betreiberin der Facebook-Seite diesen Auftritt datenschutzrechtlich jedenfalls im Sinne einer gemeinsamen Verantwortung (Art. 26 DS-GVO) mitverantwortet. Darüber hinaus ist – auch wenn die Informationen nicht bis ins Detail vorliegen – insbesondere darzustellen, dass beim Aufruf der Seite personenbezogene Daten von META/Facebook erhoben und diese auch zu verschiedenen Zwecken – regelmäßig auch zu Werbezwecken sowie zur Profilerstellung – weiterverarbeitet werden.

Ein dauerhafter rechtskonformer Betrieb von Facebook-Seiten wird nicht möglich sein. Den Betreibern von Facebook-Seiten ist daher dringend zu empfehlen, ihre Social-Media-Präsenzen auf den Prüfstand zu stellen und baldmöglichst die Weichen für eine datenschutzfreundlichere Ausrichtung ihres Kommunikationskonzepts zu stellen.

4.2 Der Facebook Like Button beschäftigt die Datenschutzbeauftragten und den Verbraucherschutz gleichermaßen

Ein seit 2015 laufendes Verfahren der Verbraucherzentrale gegen ein Unternehmen, das auf seiner Website den Facebook Like Button integriert hatte, ist im November 2022 ohne Entscheidung des OLG Düsseldorf zu Ende gegangen, nachdem die Berufung zurückgenommen wurde. Damit ist die 2016 ergangene Entscheidung des Landge-

richts Düsseldorf rechtskräftig. Nach diesem Urteil darf das verantwortliche Unternehmen das Plug-in nicht in einer Form auf seiner Website einbetten, die einen Zugriff auf IP-Adresse und Browserstring der Nutzer*innen ermöglicht, ohne dass vorher eine Einwilligung eingeholt wurde.

Die Rücknahme der Berufung seitens des beklagten Unternehmens beendet ein Verfahren, das viel Aufmerksamkeit aus den Medien sowie den Fachkreisen erhalten hat. Ausgangspunkt des Verfahrens war eine Klage des Verbraucherzentrale NRW e.V. nach dem Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz). Die Verbraucherzentrale NRW berief sich darauf, dass die Einbettung eines Plug-ins, die es ermöglicht, Daten der Besucher*innen einer Website auszulesen und weiterzuleiten, nicht datenschutzkonform war. Denn zu diesem Zeitpunkt hatten sie keine Möglichkeit, dieser Datenverarbeitung zu widersprechen. Das war aber bereits nach der Datenschutz-Richtlinie und der Umsetzung im BDSG, die zum Zeitpunkt der Klageerhebung maßgeblich waren, erforderlich. Das Landgericht Düsseldorf gab ihr Recht (Urteil vom 9. März 2016, Az. 12 O 151/15): Verantwortliche sind beim Einsatz des Facebook Like Buttons auf ihrer Seite verpflichtet, vor entsprechenden Zugriffen die Nutzer*innen der Seite über die durch das Plug-in erfolgenden Datenverarbeitungen umfassend zu informieren, aufgrund der nunmehr geltenden DS-GVO eine Einwilligung einzuholen sowie auf die Widerruflichkeit einer solchen Einwilligung hinzuweisen. Grundlage dieser Entscheidung war, dass das Gericht Websitebetreiber*innen als verantwortlich für von ihnen integrierte Plug-ins eines anderen Verantwortlichen (hier: Facebook, jetzt META) und die

dadurch angestoßenen Datenverarbeitungen betrachtete.

In der gegen das Urteil eingelegten Berufung rief das OLG Düsseldorf zunächst den Europäischen Gerichtshof (EuGH) mit verschiedenen Fragen zur Verantwortlichkeit für den Einsatz entsprechender Plug-ins sowie zur Reichweite des Klagerechts von Verbraucherverbänden bei Datenschutzverstößen an. Der EuGH entschied zum Facebook Like Button, dass eine gemeinsame Verantwortlichkeit von Websitebetreiber und Facebook bestehe (Urteil vom 29 Juli 2019, Az. C-40/17).

Nach Abschluss dieses sowie eines weiteren Verfahrens zum Verbandsklagerecht der Verbraucherzentralen vor dem EuGH wurde die Berufung beim OLG Düsseldorf zurückgenommen. Damit bleibt es bei der Entscheidung des LG Düsseldorf zum Facebook Like Button.

Aufgrund der Entscheidung des EuGH sind Betreiber*innen einer Website auch für Verarbeitungsvorgänge (mit)verantwortlich, die durch (Fremd-)Plug-ins angestoßen werden. Mit der Integration dieser Plug-ins in eine Website übernehmen Betreiber*innen die Verantwortlichkeit für von den Plug-ins ausgehende Datenverarbeitungen. Darüber hinaus ist geklärt, dass Verbraucher*innenverbänden ein entsprechendes Klagerecht nach dem Unterlassungsklagegesetz zusteht.

4.3 Neue Datenschutzregeln für Telekommunikationsdienste und ihre Auswirkungen auf die Datenschutzaufsicht über den Einsatz von Videokonferenz-Tools

Videokonferenzen (VK) haben sich während der Corona-Pandemie etabliert und sind inzwischen unverzichtbar in vielen Bereichen der Bildungs- und Arbeitswelt. Seit Dezember 2021 haben sich die Verantwortlichkeiten für die im Rahmen von VK verarbeiteten personenbezogenen Daten verändert.

Seit Inkrafttreten des neuen TKG und des TTDSG am 1. Dezember 2021 gelten „in der Regel gegen Entgelt erbrachte“ VK-Dienste grundsätzlich als Telekommunikationsdienste (TK-Dienste). Zu „in der Regel gegen Entgelt erbrachten“ VK-Diensten zählen vor allem die auf dem Markt gängigen, online zur Verfügung stehenden VK-Systeme.

Waren Unternehmen und andere Stellen, welche die VK-Dienste einsetzten, bis zum 30. November 2021 selbst für sämtliche Verarbeitungen personenbezogener Daten verantwortlich und mussten sie bis dahin noch Auftragsverarbeitungsverträge mit den Anbietern schließen, so hat sich dies mit dem 1. Dezember 2021 geändert. Denn seither sind die Anbieter von VK-Diensten als TK-Diensteanbieter für die Verarbeitung der Metadaten (wer kommuniziert wann und wie oft mit wem) und den Transport der dem Fernmeldegeheimnis unterliegenden Kommunikation (Inhaltsdaten) verantwortlich – und nicht mehr diejenigen, die den VK-Dienst in ihrem Unternehmen, ihrer Behörde oder sonstigen Stelle einsetzen. Für die datenschutzrechtliche Aufsicht über TK-Anbieter ist der BfDI zu-

ständig (vgl. § 29 TTDSG). Auch ist kein Auftragsverarbeitungsvertrag mehr mit den Anbietern der VK-Dienste zu schließen. Grund: Da die TK-Diensteanbieter den spezifischen Regeln des TKG und des TTDSG, welche die ePrivacy-Richtlinie und die Richtlinie (EU) 2018/1972 (Europäischer Kodex für die elektronische Kommunikation) umsetzen, unterworfen sind, dürfen sie diese nicht durch vertragliche Verpflichtungen aus einer Auftragsverarbeitungsvertrag umgehen.

Stellen, die VK-Dienste einsetzen, sind aber weiterhin für die in ihrem Einflussbereich stattfindende Verarbeitung personenbezogener Daten verantwortlich. Hierzu zählen zum Beispiel

- Daten im Zusammenhang mit der Herstellung der Kommunikation (beispielsweise Verwendung von E-Mail-Adressen zur Übersendung des Besprechungslinks),
- Inhaltsdaten, soweit sie in ihrem Einflussbereich verarbeitet werden (Beispiel: Speicherung oder anderweitige Verarbeitung von Inhalten, die zum Gegenstand der Videokonferenzen oder der im Rahmen der Videokonferenzen stattfindenden Chats gemacht werden) sowie
- die datenschutzfreundlichen Voreinstellungen bei der Verwendung der Tools.

Zudem sollte bereits bei der Auswahl des Videokonferenzdienstes darauf geachtet werden, dass Inhalte angemessen verschlüsselt werden und ein Löschkonzept vorliegt. Insoweit unterliegen die Stellen in NRW, die VK-Dienste nutzen, der Datenschutzkontrolle der LDI NRW.

VK-Diensteanbieter sind als TK-Anbieter zu qualifizieren und für die Verarbeitung der Metadaten und den Transport der Inhaltsdaten datenschutzrechtlich verantwortlich. Die Stellen, die VK-Dienste nutzen, müssen nun keine Auftragsverarbeitungsverträge mehr mit den Anbietern schließen. Sie müssen sich allerdings nach wie vor darum kümmern, dass die in ihrem Einflussbereich stattfindenden Verarbeitungen personenbezogener Daten DS-GVO-konform sind.

4.4 Vorgehen gegen negative Bewertungen in Bewertungsportalen

Was können Handwerker*innen oder Dienstleister tun, wenn sie auf Bewertungsportalen verrissen werden – und vielleicht sogar personenbezogene Daten von ihnen veröffentlicht werden? Immer häufiger werden aus dem vermeintlichen Schutz der Anonymität heraus alle Hemmungen vergessen und Bewertete verunglimpft.

Bewertungen von Waren, Dienstleistungen oder auch beruflichen Fähigkeiten spielen eine große Rolle und beeinflussen unsere (Konsum-)Entscheidungen. Wenn es zu negativen Bewertungen im Internet kommt, stellen sich Unternehmen und Einzelpersonen häufig die Frage, wie sie sich effektiv gegen diese wehren können.

Die bloße Tatsache, dass jemand im Internet in seiner beruflichen Stellung bewertet wird (etwa bei Ärzt*innen und Lehrer*innen oder Professor*innen), stellt zunächst noch keinen Verstoß gegen das Datenschutzrecht dar. Denn die Bewertung betrifft die sog. Sozialsphäre – also die öffentliche Außenwirkung – ihres Tuns. Bewertungen sind hier in aller Regel von der Meinungsfreiheit gedeckt.

Deshalb kann die LDI NRW nur in solchen Fällen tätig werden, in denen tatsächlich personenbezogene Daten unrechtmäßig verarbeitet oder veröffentlicht wurden, die für eine Bewertung nicht notwendig sind. Ein Beispiel: Ein Schüler bewertet nicht nur eine Lehrerin, sondern nennt dabei auch ihren Wohnort.

Wollen sich Betroffene gegen Äußerungen zu ihrer Person wehren, sollten sie sich zunächst an das Bewertungsportal wenden. In der Regel gibt es hierfür eine gesonderte Funktion auf den Webseiten der Bewertungsportale - zum Beispiel „Beitrag melden“. Da die Betreiber der Portale verpflichtet sind, die Kontaktdaten ihrer Datenschutzbeauftragten in der Datenschutzerklärung zu veröffentlichen, kann man sich auch an diese wenden.

Die Betroffenen können sich auch an die LDI NRW wenden. Sofern die Kontaktdaten recherchierbar sind, kann diese dann die bewertende Person anschreiben und die Löschung von unrechtmäßig veröffentlichten personenbezogenen Daten anordnen oder auch ein Bußgeld gegen diese verhängen.

Zudem ist es möglich, auf dem Zivilgerichtsweg die Löschung einer Bewertung anzustreben, sofern sie beispielsweise unwahre Tatsachen enthält oder über die Grenzen der Meinungsfreiheit hinausgeht (Schmähkritik).

Beleidigungen, üble Nachrede oder wenn in einer Bewertung ein Foto von der betroffenen Person ohne ihre Einwilligung veröffentlicht wird, können zudem Straftatbestände erfüllen und verfolgt werden. Hierfür sind dann die Polizei und die Staatsanwaltschaften zuständig.

Problematisch ist in diesem Zusammenhang häufig, dass die Bewertungen oder die Kommentare zu Bewertungen anonym erfolgen. Bewertungsportale sind in der Regel nicht dazu verpflichtet, den betroffenen Personen eine Auskunft zu den Kontaktdaten der bewertenden Person zu erteilen. Denn damit würden sie selbst gegen Datenschutzrecht verstoßen – in diesem

Falle gegen das TTDSG. Eine Ausnahme von diesem Grundsatz besteht dann, wenn der Inhalt der Bewertung selbst gegen strafrechtliche Normen verstößt, also etwa eine Beleidigung, üble Nachrede, Verleumdung oder Bedrohung darstellt. Auskünfte dürfen die Portale aber selbst in diesen Ausnahmefällen nur dann erteilen, wenn eine gerichtliche Anordnung erfolgt ist.

Da auch die LDI NRW in solchen Fällen keine Auskunft über die Kontaktdaten erhält, bleibt allein die Möglichkeit, gegen das Bewertungsportal selbst vorzugehen.

Als unkomplizierte Möglichkeit auf eine Bewertung effektiv zu reagieren, bietet sich an, die negative Bewertung selbst zu kommentieren. Aber Vorsicht: Bewertete dürfen trotz Verärgerung in ihrem Gegenkommentar nicht selber gegen datenschutzrechtliche Vorgaben verstoßen. Tabu ist, Daten zur Person, etwa Finanzdaten, oder gar sensible Daten wie zum Beispiel Gesundheitsdaten im Gegenkommentar zu verwenden. Eine sachliche Gegenkritik kann der ursprünglichen Bewertung die Wirkung nehmen.

Die LDI NRW unterstützt Betroffene bei der Verteidigung ihrer Datenschutzrechte und der Löschung unrechtmäßig veröffentlichter personenbezogener Daten in Bewertungsportalen, wenn der Portalbetreiber nicht weiterhilft. Je nach Sachlage können Betroffene darüber hinaus Strafanzeigen erstatten oder die Unterlassung der Bewertung zivilrechtlich verfolgen. Ein sachlicher Gegenkommentar kann unmittelbar und schnell etwas bewirken und auf eine andere Sicht der Dinge hinweisen.

4.5 „Deceptive Design Patterns“ - EDSA-Leitlinien zur Gestaltung der Nutzer*innen-Oberfläche in sozialen Medien

Wer kennt das nicht: Beim Aufruf sozialer Netzwerke öffnen sich Cookie-Banner, die einem durch ihre optische Gestaltung die Einwilligung in möglichst weitreichende Datenverarbeitungen nahelegen. Wann ist eine so eingeholte Einwilligung noch freiwillig, und wieviel unterschwellige Beeinflussung der Einwilligungsentscheidung ist zulässig? Diese und weitere Fragen adressieren die neuen Leitlinien des EDSA 3/2022, die darauf abzielen, gezielte Beeinflussungen durch sog. „Deceptive Design Patterns“ (in der Vorversion noch als „Dark Patterns“ bezeichnet) zu erkennen und zu vermeiden. Diese Leitlinien sind zwar formell nicht verbindlich für die Aufsichtsbehörden. Besonders für grenzüberschreitende Konstellationen beeinflussen sie jedoch maßgeblich die Auslegung der DS-GVO und haben somit eine faktische Bindungswirkung.

Mit „Deceptive Design Patterns“ sind manipulative Oberflächengestaltungen gemeint, die aufgrund ihres Designs und ihrer Struktur Nutzer*innen veranlassen sollen, entgegen ihren Interessen unbewusste, unbeabsichtigte und möglicherweise schädliche Entscheidungen hinsichtlich der Verarbeitung ihrer personenbezogenen Daten zu treffen. Mittels derartiger „Deceptive Design Patterns“ werden Personen, die auf sozialen Netzwerken aktiv sind, beispielsweise

- dazu bewogen, mehr Daten über sich preiszugeben, als sie eigentlich möchten,
- Einwilligungen abzugeben, die sie nicht abgeben möchten,

- oder davon abgehalten, ihre Betroffenenrechte auszuüben.

Am 14. März 2022 hat der EDSA diese Leitlinien unter dem Titel „Guidelines on dark patterns in social media platform interfaces: How to recognise and avoid them“ angenommen.

Die Leitlinien wurden anschließend in einem Konsultationsverfahren zur öffentlichen Diskussion gestellt; Anmerkungen konnten bis zum 2. Mai 2022 eingebracht werden. Die Auswertung der eingegangenen Stellungnahmen ist mittlerweile abgeschlossen. Im Zuge der Finalisierung des Textes haben die Guidelines ihren Titel geändert und sind jetzt als „Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them“ (Version 2.0) auf der Internetseite des EDSA abrufbar. Der Text dieser Leitlinien liegt bislang nur auf Englisch vor.

Der EDSA bildet in den Leitlinien sechs übergeordnete Kategorien problematischer Designs:

- Überladung: Nutzer*innen werden mit unüberschaubar vielen Informationen konfrontiert, die sie nicht überblicken können. Das Ziel ist, dass ihnen die Auseinandersetzung mit der Informationsflut zu mühevoll ist und sie deswegen Entscheidungen bezüglich der Verarbeitung ihrer Daten treffen, die sie eigentlich nicht wollen und auch nicht durchschauen.
- Überspringen: Die Seite ist so gestaltet, dass Nutzer*innen Aspekte nicht bemerken, mit denen sie sich auseinandersetzen sollten, um das Ausmaß der Verarbeitung der eigenen Daten zu verstehen

- Berühren: Die Gestaltung der Seite spricht die Nutzer*innen emotional an oder nutzt visuelle Anstöße und verleitet Nutzer*innen dadurch, bestimmte eigentlich nicht gewollte Entscheidungen bezüglich der Verarbeitung der eigenen Daten zu treffen oder nicht zu treffen.
- Behinderung: Die Nutzer*innen werden in der Ausübung von Rechten oder dem Treffen von Entscheidungen durch Hindernisse oder einen beschwerlich gestalteten Prozess beeinträchtigt.
- Inkonsistenz: Die Darstellung ist unklar, widersprüchlich oder nicht schlüssig und Nutzer*innen können deswegen nicht verstehen, was mit ihren Daten passiert oder wie sie ihre Rechte ausüben können.
- Im Dunkeln lassend: Die Gestaltung der Seite verbirgt Informationen oder Datenschutzkontrollinstrumente oder lässt die Benutzer im Unklaren darüber, wie sie Einfluss auf die Verarbeitung ihrer Daten nehmen können.

Bekannte Beispiele für solche Manipulationsversuche sind etwa Auswahlbuttons unterschiedlicher Größe oder Farbe (die vom Anbieter gewünschte Wahl ist farbig, die im Interesse der betroffenen Person liegende grau). Auch Auswahlfenster, bei denen eine Zustimmung zu der vom Verantwortlichen gewünschten Verarbeitung unmittelbar möglich ist, eine Ablehnung hingegen mehrere Klicks erfordert, fallen in diese Kategorie. Darüber hinaus wird eine ganze Reihe weiterer, nicht immer auf den ersten Blick erkennbarer manipulativer Designs und Strukturen erörtert.

Mit den Leitlinien stellt der EDSA eine Handreichung zur Verfügung, um Web-Designer*innen zur datenschutzgerechten Gestaltung von Webseiten anzuhalten und Nutzer*innen die Möglichkeit zu geben, „Deceptive Design Patterns“ leichter zu erkennen und ihnen entgegenzuwirken. Die Leitlinien enthalten viele konkrete, häufig durch Bilder illustrierte Beispiele verschiedener Kategorien von „Deceptive Design Patterns“. Darüber hinaus werden positive „best practices“ dargestellt. Dabei orientiert sich der Aufbau der Leitlinien an verschiedenen Beispielen, die den Lebenszyklus eines Social-Media-Kontos abbilden: Unter anderem werden Beispiele im Rahmen der Registrierung, bei den Datenschutzeinstellungen und dem Löschen eines Kontos gezeigt.

Die Leitlinien legen auch im Einzelnen dar, welche Normen der DS-GVO oder ePrivacy-Richtlinie besonders relevant sind. Zu nennen sind hier die Grundsätze der Datenverarbeitung nach Art. 5 DS-GVO und hier besonders die Grundsätze der Verarbeitung nach Treu und Glauben, der Transparenz, der Datenminimierung und die Rechenschaftspflicht der verantwortlichen Stelle. Auch der Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) ist in diesem Zusammenhang zu nennen. Darüber hinaus spielt hier die Einwilligung nach Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a DS-GVO und Art. 5 Abs. 3 ePrivacy-Richtlinie, und hier insbesondere deren Freiwilligkeit, eine große Rolle. In den Leitlinien wird zu jedem (Negativ-)Beispiel im Einzelnen erklärt, warum ein Verstoß gegen die DS-GVO vorliegt. Schließlich enthält der Annex zu den Leitlinien eine Checkliste, anhand der geprüft werden kann, ob in einem konkreten Fall „Deceptive Design Patterns“ eingesetzt werden.

Die neuen „Guidelines on deceptive design patterns in social media platform interfaces: How to recognise and avoid them“ schaffen ein europaweit einheitliches Verständnis dafür, welche Gestaltungselemente in sozialen Medien – aber ebenso beispielsweise auf Websites – in welcher Form datenschutzkonform zum Einsatz kommen können. Sie können sowohl Nutzer*innen als auch Gestalter*innen von Internetangeboten sensibilisieren, welche bewusst oder unbewusst auf die Entscheidungsfreiheit einwirkenden Gestaltungselemente eingesetzt werden und Zweifel an einer rechtmäßigen Datenverarbeitung nähren. Last but not least werden auch die Aufsichtsbehörden auf diese Guidelines zurückgreifen, wenn sie die Zulässigkeit von Datenverarbeitungen bewerten.

5. Schule und Bildung

5.1 Veröffentlichungen der LDI NRW

- **Handreichung zu Online-Prüfungen an Hochschulen**

  Inzwischen sind Hochschulen gesetzlich befugt, Online-Prüfungen durchzuführen (§ 64 Abs. 2 Sätze 2 und 3 Hochschulgesetz NRW). Einzelheiten zur Art und Weise der Abnahme der Online-Prüfungen und der dazu erforderlichen Verarbeitung von personenbezogenen Daten sind in den jeweiligen Prüfungsordnungen der Hochschulen festzulegen. Um die Chancengleichheit der Prüflinge zu sichern, sind auch Kontrollen vorzusehen. Diese müssen dabei den Persönlichkeitsrechten der Prüflinge so weit wie möglich Rechnung tragen und dürfen insbesondere keinen permanenten Kontrolldruck erzeugen. Für das Ausmaß der Überwachung bei Online-Prüfungen sollte die Präsenzsituation als Vergleich im Blick behalten werden.

  Die neue Handreichung zu Online-Prüfungen gibt den Hochschulen Hilfestellungen. Sie zeigt die Grenzen videobasierter Aufsicht im Verhältnis zum Schutz der Persönlichkeitsrechte der Prüflinge auf. Die Handreichung ist unter www.ldi.nrw.de abrufbar.

- **Homepagebeitrag „Digitaler Unterricht in Schulen – Der Grundstein ist gelegt“**

  Die Vorteile des Digitalunterrichts liegen auf der Hand: Erhöhte Flexibilität, Vermeidung von Unterrichtsausfällen sowie die Vorbereitung der Schüler*innen auf ein Leben im digitalen Zeitalter. Dabei dürfen ihre Persönlichkeitsrechte, aber auch die der Lehrkräfte nicht außer Acht gelassen werden. Durch die

Erweiterung der §§ 120, 121 Schulgesetz NRW hat der Landesgesetzgeber den Schulen die Möglichkeit eingeräumt, ihren Unterricht über den analogen Präsenzbetrieb hinaus digital zu gestalten. Der Homepagebeitrag soll die verantwortlichen Stellen unterstützen, die datenschutzrechtlichen Vorgaben zu erfüllen. Er ist unter www.ldi.nrw.de abrufbar.

5.2 Telepräsenzroboter im Schulunterricht

Telepräsenzroboter sollen im stellvertretend für Schüler*innen eingesetzt werden, denen es aufgrund einer Langzeiterkrankung nicht möglich ist, regelmäßig den Präsenzunterricht in der Schule zu besuchen. Die damit verbundene Datenverarbeitung regeln nunmehr schulgesetzliche Normen.

Telepräsenzroboter werden im Klassenzimmer auf dem Platz des*der betroffenen Schüler*in aufgestellt und haben eine eingebaute Kamera und ein Mikrofon, um per Live-Stream den Präsenzunterricht zu übertragen.

Nach dem Begründungstext zum 16. Schulrechtsänderungsgesetz, soll die Neuregelung in § 120 Abs. 5 Satz 2 Schulgesetz NRW nicht nur einen für alle Beteiligten mittels Videokonferenz durchgeführten Unterricht umfassen. Vielmehr sollte auch die Möglichkeit geschaffen werden, „Schüler*innen, die nicht am Präsenzunterricht teilnehmen können (beispielsweise aufgrund von Quarantäne, Wechsel von Präsenz- und Distanzphasen, Krankheit etc.), zum Unterricht vor Ort „zuzuschalten“ und somit am Unterricht teilhaben zu lassen“. Die Nutzer*innen haben die Möglichkeit, sich mit ihrer Stimme am Unterricht zu beteiligen. Ihre Bilddaten werden jedoch nicht an die

Schüler*innen und Lehrkräfte im Präsenzunterricht übertragen.

Die Einsatzbedingungen der Telepräsenzroboter sind mit denen eines Videokonferenzsystems vergleichbar. Die Schule hat zu entscheiden, ob der Einsatz eines Telepräsenzroboters für die Erfüllung des gesetzlichen Bildungs- und Erziehungsauftrags erforderlich ist und inwieweit hiervon Gebrauch gemacht wird. Die verarbeiteten Daten sind durch technische und organisatorische Maßnahmen zu schützen.

Eltern oder andere Personen aus dem häuslichen Umfeld der Schüler*innen dürfen regelmäßig nicht am Unterricht teilnehmen. Soweit möglich, sollte das durch technische Maßnahmen unterbunden sein oder muss durch Nutzungsregelungen ausgeschlossen werden. Auch Unterrichtsmitschnitte sind nicht zulässig. Schulleitungen sollten bei der Auswahl des Anbieters darauf achten, dass entsprechende technische Vorkehrungen zum Ausschluss solcher unzulässigen Datenverarbeitungen getroffen werden können.

Außerdem hat die Schule für eine ausreichende Sicherheit bei dem von dem*der betroffenen Schüler*in eingesetzten mobilen Endgerät (Tablet, Smartphone) zu sorgen. Idealerweise sollten die Betroffenen daher von der Schule bereitgestellte und verwaltete Endgeräte nutzen, auf denen sich die erforderlichen Sicherheitsmaßnahmen am effektivsten sicherstellen lassen.

Nähere Einzelheiten zum Einsatz sog. Telepräsenzroboter finden sich in unserer Veröffentlichung „Digitaler Unterricht – Der Grundstein ist gelegt“ (Seite 19

ff.), abrufbar unter https://www.ldi.nrw.de/digitaler-unterricht-schulen-der-grundstein-ist-gelegt.

Telepräsenzroboter ermöglichen langzeiterkrankten Schüler*innen, Kontakt zu ihren Mitschüler*innen und Lehrkräften zu halten und trotz ihrer Erkrankung am Unterricht teilzunehmen. Im Interesse der Betroffenen begrüßt die LDI NRW, dass für die in diesem Zusammenhang stattfindende Datenverarbeitung nunmehr eine gesetzliche Rechtsgrundlage zur Verfügung steht.

5.3 Einsatz von Microsoft 365 in Schulen

Ein datenschutzgerechter Einsatz von Microsoft 365 in Schulen ist weiterhin zweifelhaft. Microsoft stellt nicht die notwendige Transparenz über die Verarbeitung personenbezogener Daten von Schüler*innen und Lehrer*innen her, die mit dem Produkt arbeiten.

Eine Arbeitsgruppe der DSK hat Gespräche mit Microsoft geführt, um das Unternehmen zu Nachbesserungen für einen datenschutzgerechten Einsatz von Microsoft 365 zu bewegen. Die Gespräche sind zwischenzeitlich abgeschlossen. Die DSK hat den Bericht der Arbeitsgruppe in ihrer Sitzung am 24. November 2022 zur Kenntnis genommen. Sie hat daraus den Schluss gezogen, dass Verantwortliche den Nachweis, Microsoft 365 datenschutzgerecht zu betreiben, auf der Grundlage der ihr von Microsoft zur Verfügung gestellten Informationen derzeit nicht führen können. Die Informationen versetzen die Verantwortlichen nicht in die Lage, die ihnen obliegende Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO) erfüllen zu können. Solange das Unternehmen insbesondere die

notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für seine eigenen Zwecke nicht herstelle und deren Rechtmäßigkeit nicht belege, könne der Rechenschaftsnachweis nicht erbracht werden, so die DSK.

Die Zusammenfassung des Berichts und der Beschluss der DSK vom 24. November 2022 sind unter dem Link https://www.datenschutzkonferenz-online.de/beschluesse-dsk.html abrufbar.

Neben der Arbeitsgruppe der DSK gibt es auch eine noch laufende Gesprächsinitiative aus der Kultusminister*innenkonferenz der Länder mit Microsoft, an der einige Datenschutzaufsichtsbehörden beratend teilnehmen. Diese Initiative zielt darauf, einen datenschutzgerechten Einsatz von Microsoft 365 in Schulen zu erreichen. Wesentlich dafür ist, dass Microsoft die im Auftrag der Schulen verarbeiteten personenbezogenen Daten ausschließlich nach deren Weisung verarbeitet. Schulen sind nicht befugt, einem Unternehmen die Daten ihrer Lehrer*innen und Schüler*innen zu unbekannten Zwecken oder Zwecken zur Verfügung zu stellen, die über das für ihre Aufgabenerfüllung erforderliche Maß hinausgehen. Möglicherweise wird diese rechtliche Besonderheit in Bezug auf Schulen von Microsoft unterschätzt.

Schulen, die Microsoft 365 nutzen, sind datenschutzrechtlich verantwortliche Stellen. Bei einer Überprüfung im Einzelfall müssen sie der LDI NRW nachweisen können, dass die im Zusammenhang mit dem Einsatz von Microsoft 365 in ihrer Schule stattfindende Datenverarbeitung den datenschutzrechtlichen Vorschriften entspricht. Angesichts der bisherigen Feststellungen der DSK ist kaum vorstellbar, dass

den betroffenen Schulen ein solcher Nachweis gelingt. Um Schulen dabei zu unterstützen, einen datenschutzgerechten Auftragsverarbeitungsvertrag mit Microsoft abzuschließen, wird nunmehr von einer Arbeitsgruppe verschiedener Datenschutzbehörden, an der sich auch die LDI NRW beteiligt, eine Handreichung erarbeitet.

Die Ergebnisse dieser Prozesse werden wir noch abwarten, bevor wir Aufsichtsmaßnahmen gegen Schulen ergreifen, die ihrer Rechenschaftspflicht nicht nachkommen können. Wir legen derweil in der Kommunikation mit Schulen Wert darauf, dass die Schüler*innen, die bzw. deren Eltern sich über den Einsatz von Microsoft 365 beschwert haben, nicht schutzlos gestellt sind und diskriminiert werden. Daher werden diese Schulen von uns aufgefordert, für die Klasse oder Kurse dieser Schüler*innen Alternativlösungen bereitzustellen, die allen gleichermaßen eine adäquate Teilnahme am Unterrichtsgeschehen ermöglichen. Nur so können wir ohne weitere aufsichtsrechtliche Maßnahmen an den betroffenen Schulen an einer datenschutzgerechten Lösung für alle Schüler*innen weiterarbeiten.

Langfristig muss nicht nur in den Schulen, zu denen uns Beschwerdefälle vorliegen, sondern in allen Schulen, die derzeit Microsoft 365 einsetzen, der Datenschutz gewährleistet sein. Wir begrüßen daher die Absicht des Schulministeriums, mit der Weiterentwicklung von LOGINEO NRW datenschutzgerechte Alternativen für den digitalen Unterricht bereitzustellen. Auch die Schulträger sind hier gefordert, ihren Schulen datenschutzgerechte Lösungen anzubieten. In einigen Ländern haben solche Entwicklungen dazu

geführt, dass Schulen digitalen Unterricht weitgehend ohne Datenschutzprobleme anbieten können.

Wir empfehlen weiterhin allen Verantwortlichen im Schulbereich, datenschutzfreundlichere Alternativen für die Gestaltung des digitalen Unterrichts einzusetzen. Wenn sich mit Microsoft keine datenschutzgerechten Lösungen erreichen lassen, werden wir weitere Aufsichtsmaßnahmen ergreifen müssen.

6 Sicherheit, Justiz und Verwaltung

6.1 Gerichtsentscheidungen

Der EuGH urteilt mehrfach zur Vorratsdatenspeicherung und erklärt u.a. die deutsche Regelung für europarechtswidrig

Gleich in mehreren Entscheidungen (Urteil vom 5. April 2022, Az. C-140/20, Urteile vom 20. September 2022, Az. C-339/20 und Az. C-397/20 sowie Az. C-793/19 und Az. C-794/19) hat sich der EuGH im Berichtsjahr zu Möglichkeiten und Grenzen der Vorratsdatenspeicherung geäußert. Dabei erteilte er einer anlasslosen allgemeinen und unterschiedslosen Speicherung zum wiederholten Male eine Absage. Gleichzeitig konkretisierte er die engen Grenzen, in denen eine Speicherung allgemeiner Verkehrsdaten oder von IP-Adressen zulässig sein kann. Neben einer allgemeinen und unterschiedslosen Speicherung im Fall einer ernsten Bedrohung für die nationale Sicherheit ist die seit langem in der Diskussion stehende sog. Quick-Freeze-Regelung danach grundsätzlich mit Unionsrecht vereinbar. Bei letzterer dürfen die Verkehrsdaten bestimmter Personen bei dem Anfangsverdacht einer Straftat und nach richterlicher Anordnung für die Zukunft gespeichert werden.

Nach der EUGH-Rechtsprechung war die deutsche (Neu-)Regelung von 2015, die eine anlasslose flächendeckende Speicherung der Verkehrsdaten für vier bis zehn Wochen zuließ, mit dem Europarecht nicht vereinbar. Dieser Regelung war schon eine weitere Entscheidung des EuGH (Urteil vom 8. April 2014, Az. C-293/12 und Az. C-594/12) vorangegangen, mit der die europäische Vorgängerregelung für

unionsrechtswidrig erklärt wurde. Die Bundesregierung hat eine Neuregelung angekündigt.

Der EuGH erklärt nach einem Vorabentscheidungsverfahren bestimmte nationale Umsetzungen der sog. PNR-Richtlinie für unionsrechtswidrig; Die Entscheidung hat auch Auswirkungen für Deutschland

Die PNR-Richtlinie schreibt zur Bekämpfung von Terrorismus und schwerer Kriminalität die systematische Verarbeitung einer großen Zahl von PNR-Daten (Passenger Name Record) der Fluggäste von Flügen zwischen der Union und Drittstaaten (Drittstaatsflüge) bei der Einreise in die bzw. der Ausreise aus der Union vor. Darüber hinaus können die Mitgliedstaaten diese Richtlinie nach ihrem Art. 2 auch auf Flüge innerhalb der Union (EU-Flüge) anwenden. Für die Anwendung der PNR-Richtlinie auf EU-Flüge hat der EuGH (Urteil vom 21. Juni 2022, Az. C-817/19) nun konkrete Anforderungen aufgestellt. Gegenstand der Entscheidung war eine belgische Regelung. Der Gerichtshof hat mit dem Urteil insbesondere entschieden, dass bei Reisen innerhalb der Union durch die Mitgliedstaaten keine anlasslose Verarbeitung der Daten aller Reisenden zugelassen werden darf. In diesen Fällen ist – vergleichbar mit den Entscheidungen des EuGH zur Vorratsdatenspeicherung (s. o.) – vielmehr eine reale und aktuelle oder vorhersehbare terroristische Bedrohung eines Mitgliedstaats erforderlich. Ohne eine solche terroristische Bedrohung darf die Datenverarbeitung dagegen nicht auf alle EU-Flüge erstreckt werden, sondern muss sich auf solche EU-Flüge beschränken, die etwa bestimmte Flugverbindungen, Reisemuster oder Flughäfen be-

treffen, für die es nach der Einschätzung des betreffenden Mitgliedstaats Anhaltspunkte gibt, die eine Verarbeitung von PNR-Daten rechtfertigen können. Daneben hat der EuGH eine strikte Zweckbindung der PNR-Daten allein für die Zwecke der PNR-Richtlinie festgelegt und eine Speicherfrist von fünf Jahren für alle nach der PNR-Richtlinie verarbeiteten Daten für unionsrechtswidrig erklärt. Ob aufgrund der Entscheidung eine Änderung des deutschen Fluggastdatengesetzes, mit der die PNR-Richtlinie in deutsches Recht umgesetzt wird, erfolgt, ist noch unklar. Jedenfalls macht die Entscheidung Änderungen in dessen praktischer Ausführung erforderlich.

Das Bundesverfassungsgericht hat zum Bayerischen Verfassungsschutzgesetz (Bay. VSG) geurteilt; mit weitreichenden Auswirkungen, auch für den Verfassungsschutz in NRW

Das Gericht erklärte eine Vielzahl von Regelungen im Bay VSG für verfassungswidrig, die in dieser oder vergleichbarer Form auch im Verfassungsschutzgesetz des Bundes oder der Länder enthalten sind (Urteil vom 26. April 2022, Az. 1 BvR 1619-17). Für unzulässig gehalten wurden unter anderem die Regelungen zu den Eingriffsmaßnahmen der Wohnraumüberwachung, Online-Durchsuchung, Ortung von Mobilfunkgeräten, Auskunft über auf Vorrat gespeicherte Telekommunikationsverkehrsdaten, Einsatz von Vertrauenspersonen und verdeckten Ermittlern sowie längerfristigen Observationen außerhalb von Wohnungen. Grund hierfür war, dass die gesetzlichen Voraussetzungen für die Maßnahmen zu niedrig angesetzt oder die Regelungen nicht normenklar formuliert waren. Darüber hinaus verlangt das BVerfG

zu einzelnen Maßnahmen vor deren Durchführung eine unabhängige Vorabkontrolle.

Gleichzeitig wurden die Vorschriften zur Weiterverarbeitung und Übermittlung personenbezogener Daten, die mit nachrichtendienstlichen Mitteln erhoben wurden, insbesondere an Strafverfolgungsbehörden, für unzulässig erklärt.

Auch für NRW ergibt sich aus dem Urteil Handlungsbedarf, wenngleich dieser geringer ausfällt, als in anderen Ländern oder dem Bund. Das Innenministerium NRW hat uns gegenüber für 2023 einen Gesetzentwurf in Aussicht gestellt.

Das OVG Münster hat mehrere Entscheidungen des VG Köln zur polizeilichen Videoüberwachung (27. Bericht unter Punkt 6.1) weitgehend aufgehoben und auch eine Videoüberwachung in Dortmund für vorläufig zulässig befunden.

Das OVG Münster hat am 16. Mai 2022 in mehreren Entscheidungen des VG Köln, in denen dieses den Klägern im Rahmen einstweiliger Verfahren weitgehend Recht gegeben hatte, in wesentlichen Punkten abweichend entschieden. Die Videoüberwachung an den angegriffenen Standorten (Neumarkt – Az. 5 B 264/21, Ebertplatz – Az. 5 B 1289/21 und Breslauer Platz – Az. 5 B 137/21) kann somit zunächst weitgehend unverändert fortgesetzt werden. Gleichzeitig hat das Gericht sehr konkrete Vorgaben für die Polizeibehörden formuliert, wie diese künftig das Vorliegen der gesetzlichen Voraussetzungen für eine polizeiliche Videoüberwachung zu prüfen und nachzuweisen haben und eine ausreichende Beschilderung vor Ort zu erfolgen hat. Die Entscheidungen in der Hauptsache

stehen noch aus. Auch die Videoüberwachung im Bereich der Münsterstraße in Dortmund kann laut Beschluss des OVG Münster vom 23. September 2022 (Az. 5 B 303-21) zunächst fortgeführt werden. In dieser Entscheidung wird erneut betont, dass für eine ausreichende Beschilderung zu sorgen ist. Ein videoüberwachter Bereich muss bereits vor Betreten als solcher erkennbar sein. Auch spricht laut Gericht vieles für eine verpflichtende Angabe der Überwachungszeiten auf den Schildern. Die Einsatzreaktionszeit der Polizei von über 15 Minuten hielt das Gericht dagegen wohl für unzureichend.

Das Bundesverwaltungsgericht bestätigt den Anspruch auf kostenlose Klausurkopien für Examenskandidat*innen

Bereits die Vorinstanzen hatten entschieden: Prüflinge haben gegenüber dem Landesjustizprüfungsamt NRW einen Anspruch auf kostenfreie Überlassung der im zweiten juristischen Staatsexamen angefertigten Klausuren mitsamt Gutachten – entweder in Papierform oder in elektronischem Format. Die gegen die Entscheidung des OVG NRW eingelegte Revision des Landes NRW ist nun erfolglos geblieben. Mit Urteil vom 30. November 2022 (Az. 6 C 10.21) bestätigt das Bundesverwaltungsgericht das Bestehen des Anspruchs auf unentgeltliche Kopien und damit auch die Auffassung der LDI NRW (siehe bereits im 26. Bericht unter 6.7).

6.2 Veröffentlichungen

- Wahlen und Datenschutz: Jede Frage braucht eine Antwort!

6.3 Schengener Informationssystem – Fahndungsausschreibungen nach Art. 36 SIS-II-Beschluss

Eine Kontrolle von verdeckten Fahndungsausschreibungen im SIS II hat zu keinen datenschutzrechtlichen Beanstandungen oder weiteren Maßnahmen durch die LDI NRW geführt. Die Begründung der dem Ermittlungsgericht vorzulegenden Anträge war jedoch in einigen Fällen zu oberflächlich.

Aufgrund Europäischer Vorschriften ist die LDI NRW gehalten, alle vier Jahre zumindest stichprobenartige Kontrollen im Bereich des sog. SIS II durchzuführen. Bei SIS II handelt es sich um das Schengener Informationssystem der zweiten Generation, einem den Mitgliedstaaten des Schengen-Übereinkommens zugängliches länderübergreifendes polizeiliches Dateisystem. Hierin können bei Vorliegen der gesetzlichen Voraussetzungen insbesondere Fahndungen nach Personen oder Gegenständen aufgenommen werden. Da es sich um europaweite Ausschreibungen handelt, die von einer Vielzahl an Sicherheitsbehörden eingesehen werden können, sind die rechtlichen Voraussetzungen höher als für rein nationale Fahndungen. Bei den Fahndungen nach Art. 36 SIS-II-Beschluss handelt es sich um verdeckte Ausschreibungen. Das bedeutet, dass bei Personen, die beispielsweise an Grenzübergängen und Flughäfen im Rahmen einer Routinekontrolle überprüft werden, die Ausschreibungsbehörde über das Antreffen der betroffenen Person informiert wird, die betroffene

Person hierüber jedoch keine Information erhält. Auf diese Weise kann die Ausschreibungsbehörde Reiseverläufe beobachteter Personen nachvollziehen.

Im Rahmen unserer Kontrolle haben wir festgestellt, dass in den geprüften Fällen die rechtlichen Voraussetzungen für die Ausschreibungen zwar objektiv vorlagen bzw. anhand des Sachverhaltes hergeleitet werden konnten. Dies wurde jedoch in den Anträgen auf Einrichtung einer Ausschreibung, die dem Ermittlungsgericht vorzulegen sind, nicht immer ausreichend dokumentiert. Es fehlte an einer überzeugenden Darstellung der rechtlichen Gründe und vor allem der Erforderlichkeit der Ausschreibungsmaßnahme. In einigen Fällen wurde auch die vom Gesetz geforderte sog. Negativprognose nicht durchgeführt bzw. dokumentiert.

Daneben haben wir festgestellt, dass die nach sechs Monaten zwingend durchzuführende Prüfung des andauernden Vorliegens der Ausschreibungsvoraussetzungen teilweise nicht vorgenommen bzw. auch dies nicht im Vorgang vermerkt wurde.

Im Nachgang zu unserem Prüfbericht hat das Justizministerium seinen Geschäftsbereich auf die Einhaltung der Dokumentations- und Begründungspflichten hingewiesen. Auch das geprüfte Polizeipräsidium hat bestätigt, unsere Hinweise umgesetzt und die Bediensteten entsprechend informiert und angewiesen zu haben.

Es ist wichtig, dass rechtliche Voraussetzungen für eine Datenverarbeitung gegeben sind bzw. eingehalten wurden. Für eine bessere Nachvollziehbarkeit ihrer Zulässigkeit sind die Tatsachen und Gründe, aus denen sich die Rechtmäßigkeit der Datenverarbeitung ergibt, sowie die Einhaltung weiterer gesetzlicher Vorgaben zu dokumentieren. Inhalt und Umfang der Begründung müssen eine Überprüfung des Abwägungsergebnisses am Grundsatz der Verhältnismäßigkeit nicht nur für den Betroffenen selbst und für das zur Bestätigung der Anordnung berufene Gericht, sondern auch im Rahmen der Eigenkontrolle gewährleisten.

6.4 Kontrolle zu Lichtbildabgleichen – wenn „Verkehrssünder*innen“ Unrecht geschieht

Wer schon einmal „geblitzt“ wurde, der kennt es: Einige Zeit später flattert ein Brief einer Behörde zu dem Verkehrsverstoß ins Haus. Doch wie kann diese sich sicher sein, die richtigen Beschuldigten im Ordnungswidrigkeitenverfahren zu adressieren? Den Behörden stehen dazu verschiedene Ermittlungsmaßnahmen zur Verfügung, darunter der Abgleich des „Blitzerfotos“ mit Lichtbildern, die bei den Personalausweisbehörden hinterlegt sind. Das Anfordern eines Lichtbildes ist allerdings an enge Voraussetzungen geknüpft. Wie unsere stichprobenartige Kontrolle bei zwei Kreisen belegt, werden diese nicht immer eingehalten.

Werden im Straßenverkehr durch stationäre Messanlagen Geschwindigkeitsverstöße festgestellt, sind die zuständigen Behörden bestrebt, die jeweiligen Fahrer*innen der Fahrzeuge zu ermitteln. Nur gegen diese kann auf Basis des Ordnungswidrigkeitengesetzes ein Bußgeld hinsichtlich des konkreten Verstoßes ausgesprochen werden. Anhand der fotografierten Kennzeichen sind allerdings zunächst nur Rückschlüsse auf die Halter*innen der Fahrzeuge möglich, sodass diese die erste Anlaufstelle darstellen. Können durch die Kontaktaufnahme mit den Halter*innen keine Erkenntnisse hinsichtlich der Fahrer*innen gewonnen werden – beispielsweise wenn die Halter*innen sich nicht äußern oder angeben, nicht selber gefahren zu sein – ziehen die Behörden häufig von den Personalausweisbehörden die dort hinterlegten Lichtbilder der Halter*innen oder von anderen Personen heran.

Die Rechtmäßigkeit eines solchen Schrittes richtet sich nach den Vorgaben im Personalausweisgesetz und wird durch einen Runderlass des Ministeriums für Inneres und Kommunales des Landes NRW aus dem Jahr 2010 (43.8 – 57.04.16) konkretisiert. Einzelheiten dazu haben wir in unserer Veröffentlichung „Ermittlung von Fahrer*innen mittels Lichtbildabgleichs bei Ordnungswidrigkeiten“ beschrieben, abrufbar unter www.ldi.nrw.de. In dieser wird die Bedeutung der vorherigen Anhörung der Betroffenen für die Durchführung eines rechtmäßigen Lichtbildabgleichs hervorgehoben. Sie hat immer zu erfolgen – zwingend ist bei der Gelegenheit zur Anhörung auf die Möglichkeit eines Lichtbildabgleichs hinzuweisen. Ein Abgleich mit dem bei der Personalausweisbehörde hinterlegten Bild ist von vornherein nicht zulässig, wenn sich aus den Halter*innendaten ergibt, dass das aufgenommene Foto offensichtlich nicht die Person abbildet, der das Fahrzeug gehört. Dann sind zunächst weitere Ermittlungen erforderlich – die sodann verdächtigten Fahrer*innen sind allerdings vor einem Lichtbildabgleich wiederum zwingend anzuhören.

Beschwerden von Bürger*innen haben wir zum Anlass genommen, eine stichprobenartige Kontrolle bei zwei Kreisen vorzunehmen. In den 21 von uns überprüften Vorgängen haben Verstöße festgestellt. In drei Fällen erfolgte der Lichtbildabgleich ohne vorherige Anhörung der betroffenen Person. In einem weiteren Fall hat die Behörde die betroffene Person zwar angehört. Sie führte den Lichtbildabgleich allerdings zu früh durch, nämlich noch vor Ablauf der Anhörungsfrist.

In einem anderen Vorgang wurden die Vorgaben zur Durchführung eines Lichtbildabgleiches zwar eingehalten. Bei der Durchsicht der Akte ist uns allerdings aufgefallen, dass zusätzlich zeitgleich ein Aufsuchen des Betroffenen durch Ermittlungsbeamt*innen in Auftrag gegeben wurde. Ein solches Vorgehen ist unzulässig. Zum einen ist ein Lichtbildabgleich als weniger eingriffsintensive Maßnahme vorrangig durchzuführen. Zum anderen ist die zeitgleiche Vornahme beider Maßnahmen nicht erforderlich.

Losgelöst von den Anforderungen an die Durchführung von Lichtbildabgleichen haben wir in 18 Vorgängen unrechtmäßige Einholung von Auskünften über die betroffenen Personen aus der „Verkehrssünderkartei“, dem Fahreignungsregister des Kraftfahrtbundesamts, festgestellt. Die Kenntnis über etwaige „Punkte in Flensburg“ ist für die Behörde zwar notwendig, da diese zu einer Erhöhung der Regelgeldbuße führen können. Sie ist aber erst dann erforderlich, wenn die Fahrereigenschaft der Person bereits feststeht. In den 18 Vorgängen erfolgten die Abfragen bereits vor Abschluss der Ermittlungen und damit zu früh. Die beiden Kreise haben uns mitgeteilt, dass sie eine Veränderung der Arbeitsabläufe bzw. der verwendeten Formulare sowie eine Sensibilisierung der Beschäftigten für die Belange des Datenschutzes vorgenommen haben.

Unsere Kontrolle hat die Defizite, die uns aus der Bearbeitung von Beschwerden bekannt sind, teilweise bestätigt. Wir werden daher in Zukunft erneut Prüfungen dieser Art durchführen und auf diese Weise auf die Einhaltung der rechtlichen Vorgaben im Bereich der Verkehrsordnungswidrigkeiten dringen.

6.5 Kontrolle von Verfahrensrückmeldungen der Staatsanwaltschaften an die Polizeibehörden – Abschließendes Prüfergebnis

Hat in Strafverfahren zunächst die Polizei ermittelt, ist die Staatsanwaltschaft nach Abschluss des Verfahrens verpflichtet, der Polizei den Verfahrensausgang mitzuteilen. Die Polizei muss dann prüfen, ob ihre Datenbestände aufgrund der Rückmeldung zu bereinigen sind.

Bereits im letzten Bericht informierten wir über eine durchgeführte Kontrolle im Bereich der Strafverfolgung. Siehe 27. Bericht unter 6.5.

Dabei wurden Defizite sowohl bei den Rückmeldungen von Verfahrensausgängen durch die geprüfte Staatsanwaltschaft, als auch im Umgang der zuständigen Polizeibehörden mit den Rückmeldungen festgestellt. Sofern die Staatsanwaltschaft oder ein Gericht nämlich zu dem Ergebnis gekommen ist, dass schon kein Anfangsverdacht vorgelegen hat, oder die betroffene Person die ihr vorgeworfene Tat erwiesenermaßen nicht begangen hat, darf eine Fortspeicherung der betroffenen Person als Täter*in bzw. Beschuldigte*r in den polizeilichen Datenbanken nicht weiter erfolgen.

Wo dies nach unseren Feststellungen erforderlich war, haben uns die geprüften Polizeibehörden die Anpassung ihres Vorgehens zugesichert.

Das Justizministerium NRW hat aufgrund unserer Prüfung per Erlass eine Sensibilisierung der Staatsanwaltschaften für zeitnahe und inhaltlich vollständige Verfahrensrückmeldungen an die Polizei veranlasst.

Unsere Hinweise wurden umgesetzt. Das ist ein gutes Beispiel dafür, dass Kontrollen der LDI NRW einen effektiven Beitrag im Interesse der Betroffenen leisten können

6.6 Datenübermittlung an Fahrerlaubnisbehörden durch die Polizei

Das Straßenverkehrsgesetz (StVG) erlaubt der Polizei die Übermittlung von Gesundheitsdaten an die Fahrerlaubnisbehörde. In Einzelfällen bedarf es einer verfassungskonformen engen Auslegung dieser sehr weit und allgemein formulierten Vorschrift, denn die Datenübermittlung durch öffentliche Stellen ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung und nur in einem verhältnismäßigen Umfang zulässig. Darauf haben wir das Innenministerium aufmerksam gemacht.

Eine Beschwerde veranlasste unsere grundsätzliche Auseinandersetzung mit der Anwendung von § 2 Abs. 12 StVG in der Polizeipraxis. Jede Datenübermittlung durch öffentliche Stellen ist gleichzeitig ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung und ist nur auf Grundlage einer verfassungskonformen – das heißt insbesondere verhältnismäßigen – Rechtsgrundlage zulässig. Dem Wortlaut der Vorschrift nach hat die Polizei sämtliche „Informationen über Tatsachen, die auf nicht nur vorübergehende Mängel hinsichtlich der Eignung oder auf Mängel hinsichtlich der Befähigung einer Person zum Führen von Kraftfahrzeugen schließen lassen, den Fahrerlaubnisbehörden zu übermitteln“. Der Wortlaut ist somit sehr weit und enthält weder Ausnahmetatbestände noch Anforderungen an die Erforderlichkeit der Übermittlung. Auch wird die Übermittlung nicht

etwa in das Ermessen der Polizei gestellt, sondern gesetzlich angeordnet. Der Wortlaut umfasst damit auch Sachverhalte, bei denen sich im Einzelfall eine Datenübermittlung als unverhältnismäßig erweisen kann.

Nur am Wortlaut orientiert wären – auch die Fahreignung in Frage stellende Gesundheitsdaten von Personen zu übermitteln, die von der Polizei bei der Beschlagnahme von Patientenakten in den Räumlichkeiten von Ärzt*innen erlangt wurden, gegen die strafrechtlich ermittelt wird. Durch die Beschlagnahme befinden sich die Daten im Besitz der Polizei und unterfallen damit dem Wortlaut des § 2 Abs. 12 StVG.

Diese Konstellation weist aber mehrere Besonderheiten auf. Bei Gesundheitsdaten handelt es sich um besondere Kategorien personenbezogener Daten, die einem hohen Schutz unterliegen. Patientenakten berühren zudem das gesetzlich besonders geschützte Ärzt*innen-Patienten*innen-Verhältnis. Schließlich haben die betroffenen Personen, deren Unterlagen in die Hände der Polizei gelangt sind, selbst keinerlei Anlass für ein polizeiliches Handeln gegeben, sondern sich nur zufällig die falsche Praxis ausgesucht. Im Vergleich zu vielen anderen Patient*innen, bei denen objektiv Anhaltspunkte für eine fehlende Fahreignung in den medizinischen Akten dokumentiert sind, ohne dass die Fahrerlaubnisbehörde jemals davon erfährt, wird hier durch eine strafrechtliche Ermittlung in den Schutz des Ärzt*innen-Patient*innen-Verhältnisses eingegriffen. Das ist angesichts des Schutzgutes einer von Vertrauen geprägten Behandlung der Patient*innen nicht angemessen und auch eine Ungleichbehandlung, im Verhältnis zu anderen Erkrank-

ten, bei denen sich aus der medizinischen Behandlung Anhaltspunkte für eine Fahruntauglichkeit ergeben.

Zwar ist die Sicherheit des Straßenverkehrs ein wichtiges Rechtsgut. Deswegen ermöglicht § 2 Abs. 12 StVG mit guten Gründen, Daten zwecks einer Überprüfung der Fahrtauglichkeit an die zuständige Fahrerlaubnisbehörde zu übermitteln. Auch für diesen legitimen Zweck, ist allerdings die Übermittlung von Gesundheitsdaten an die Fahrerlaubnisbehörde aus in Strafverfahren gegen Ärzt*innen beschlagnahmten Patient*innenunterlagen aus o. a. Gründen nicht mehr verhältnismäßig. Diese Übermittlung der Gesundheitsdaten ist bei verfassungskonformer Auslegung von § 2 Abs. 12 StVG also nicht zulässig. Das IM NRW hat inzwischen einen Erlass an die Polizeibehörden versandt, der diese Problematik aufgreift.

§ 2 Abs. 12 StVG dient der Sicherstellung der Sicherheit im Straßenverkehr. Er erfüllt damit einen wichtigen und legitimen Zweck. In den meisten Konstellationen ist eine Datenübermittlung an Fahrerlaubnisbehörden durch die Polizei zulässig, um Gefahren für den Straßenverkehr abzuwenden. In Einzelfällen würde die Norm aufgrund ihres zu weiten Wortlauts jedoch zu unverhältnismäßigen Ergebnissen führen. Sie ist daher verfassungskonform einschränkend auszulegen.

6.7 Proof of Concept – Datenkonsolidierung

Die Polizei NRW hat ihre Planungen zu einem neuen elektronischen Datenverarbeitungsverfahren nach einer Warnung der LDI NRW ausgesetzt.

Im Jahr 2020 informierte uns die Polizei NRW, dass sie neben zwei weiteren Bundesländern Pilotland für ein neues elektronisches Datenverarbeitungsverfahren der Polizei sei. Das Projekt wurde im Verlauf als Teilprojekt in das Programm Polizei 2020 (jetzt: P20) zur grundlegenden Umstrukturierung der polizeilichen Datenverarbeitung aufgenommen.

Das als Proof of Concept (PoC) bezeichnete Pilotprojekt ist faktisch eine Machbarkeitsstudie. Sie soll unter anderem das bisherige Verfahren polizeilicher Erkenntnisanfragen vereinfachen. Sie soll auch helfen, polizeiliche Daten zu identifizieren, die sog. Verbundrelevanz haben und deswegen im bundesweiten Polizeidatensystem allen Polizeibehörden zur Verfügung stehen dürfen.

Die Polizei kann im Rahmen ihrer gesetzlichen Befugnisse auch bei den Polizeibehörden des Bundes und anderer Bundesländer nachfragen, ob dort relevante Erkenntnisse zu einer Person vorliegen (sog. Erkenntnisanfragen), wenn dies für ihre Aufgabenerfüllung in einem konkreten Fall erforderlich ist. Bisher erfolgt hierzu eine Anfrage per elektronischer Post an das LKA NRW, das die Anfrage insbesondere an die Landeskriminalämter der anderen Bundesländer weiterleitet. Deren Rückmeldungen erhält das LKA NRW, welches die Informationen dann an die ursprünglich anfragende Polizeibehörde weiterleitet. Das Verfahren war nicht nur kompliziert. Teils blieben die Er-

kenntnisanfragen nach der Bearbeitung bei den angefragten Landeskriminalämtern noch für geraume Zeit ungelöscht. Dies ist datenschutzrechtlich bedenklich, denn die angefragte Behörde benötigt diese Erkenntnis über ein Verfahren in NRW für ihre eigene Aufgabenerfüllung meist nicht.

Anders ist es nur, wenn sich anlässlich einer solchen Erkenntnisanfrage Hinweise darauf ergeben, dass eine länderübergreifende Relevanz bei der Person vorliegt, auf die sich die Anfrage bezog. Dies ist eine von drei Voraussetzungen, unter denen personenbezogene Daten im bundesweiten polizeilichen Informationssystem gespeichert werden dürfen, auf das alle deutschen Polizeibehörden Zugriff haben.

Schon früh im Verfahren wies die LDI NRW zusammen mit den Datenschutzaufsichtsbehörden von Rheinland-Pfalz und dem Saarland, deren Polizeibehörden ebenfalls Teil des Pilotverfahrens waren, auf Mängel des Konzepts hin. Im PoC liegt es – anders als im bisherigen Verfahren – nicht mehr in der Hand der angefragten Behörde, die eigenen Unterlagen daraufhin zu prüfen, welche Informationen für den Sachverhalt der anfragenden Behörde relevant sind und die Datenübermittlung auf diese erforderlichen Daten zu beschränken. Vielmehr eröffnet das PoC der anfragenden Behörde bereits einen unmittelbaren Einblick in die in anderen Ländern vorliegenden Daten zu der Person, die Gegenstand der Anfrage ist. Dies können mitunter auch Informationen über die Person sein, die keinerlei Bezug zu der konkreten Aufgabe der anfragenden Behörde haben und daher von der angefragten Behörde auch nicht übermittelt werden dürften.

Die Anzeige dieser nicht geringfügigen „Vorab“-Daten aus den anderen Ländern bei der anfragenden Behörde ist bereits eine Datenübermittlung. Soweit es sich um Daten handelt, die keinen Bezug zum Gegenstand der Untersuchung der anfragenden Behörde aufweisen, gibt es aber keine Rechtsgrundlage für eine solche Übermittlung.

Faktisch führt dieses System eine neue polizeiliche Verbunddatei unter den Polizeibehörden der beteiligten Länder ein. Aufgrund der hohen Eingriffsintensität einer bundesweiten Verfügbarkeit polizeilicher Daten ist der Datenaustausch über Ländergrenzen hinweg und mit dem Bund zu Recht an strenge Eingriffsschwellen geknüpft. Mit dem PoC, das zunächst nur unter den beteiligten Ländern, perspektivisch aber bundesweit eingeführt werden sollte, würde ein neues bundesweites Polizeidatensystem entstehen, das diese gesetzlich geregelten und verfassungsrechtlich gebotenen Schwellen umgehen würde.

Die beteiligten Datenschutzaufsichtsbehörden haben den Pilotpolizeibehörden früh und mehrfach ihre Bedenken übermittelt. Dennoch wurde unverändert an dem Konzept festgehalten. Daher sahen sich die beteiligten Datenschutzaufsichtsbehörden gezwungen, eine Warnung auszusprechen, mit der auf die potenzielle Datenschutzwidrigkeit eines geplanten künftigen Datenverarbeitungsverfahrens hingewiesen wird. In der Folge hat die Polizei NRW das Projekt PoC Datenkonsolidierung ausgesetzt und von einem Echteinsatz abgesehen. Auf diese Weise konnte eine umfangreiche rechtswidrige Verarbeitung personenbezogener Daten verhindert werden.

Die LDI NRW hat zusammen mit der Warnung Vorschläge für eine Umgestaltung der Planungen unterbreitet, mit denen die grundsätzlich erstrebenswerten Ziele des POC im Einklang mit dem Grundrecht auf informationelle Selbstbestimmung erreicht werden könnten. Die Zukunft des polizeilichen Projekts ist offen. Die polizeiliche Reaktion auf unsere mit der Warnung verbundenen Hinweise steht weiterhin aus.

Eine polizeiliche Datenverarbeitung muss sich auf eine Rechtsgrundlage stützen und ist immer auf das für die Aufgabenerfüllung Erforderliche zu beschränken. Das Übermitteln einer großen Menge an Daten mit dem Ziel, dass die empfangende Polizeibehörde die für sie nutzbaren Daten herausfiltert, erfüllt diese Voraussetzung nicht. Auch und gerade im Rahmen eines elektronischen Datenverarbeitungsverfahrens ist darauf zu achten, dass nur die tatsächlich im Einzelfall notwendigen Daten übermittelt werden.

6.8 Zwei kurze Erfolgsmeldungen

So kann Datenschutz im Polizeibereich funktionieren!

Das Innenministerium hat uns mitgeteilt, künftig die Telefonnummern von Unfallbeteiligten und Zeug*innen lediglich auf der polizeilichen Durchschrift der Unfallmitteilung zu notieren. Für diese enthielt der Vordruck bisher beim Feld „Telefonnummer“ den Zusatz „freiwillig“. Unfallbeteiligen, die diese Angabe freiwillig machten, war aber oft nicht bewusst, dass die Telefonnummer mit der Durchschrift des gesamten Bogens in jedem Fall sämtlichen Unfallbeteiligten ausgehändigt wurde. Die Personen gingen vielmehr

häufig davon aus, dass lediglich die Polizei die Telefonnummer für Rückfragen erhalten würde. Aufgrund der bisherigen Praxis wurden Zeug*innen im Nachhinein mitunter von Unfallbeteiligten kontaktiert. Dabei kam es teilweise zu Versuchen der Einflussnahme oder gar Bedrohungen. Dieses Risiko dürfte mit der neuen Vorgehensweise nun deutlich reduziert werden, ohne die polizeiliche Unfallbearbeitung zu erschweren.

Zwar dürfen personenbezogene Daten im Einzelfall an private Dritte weitergegeben werden, wenn und soweit dies zur Durchsetzung privater Rechte erforderlich ist. Dies trifft nach der nunmehr übereinstimmenden Auffassung der LDI NRW und des Innenministeriums allerdings auf Telefonnummern von Unfallbeteiligten und Zeug*innen regelmäßig nicht zu.

Einen besonders schnellen Erfolg konnten wir zudem bei dem Vordruck für Versammlungsanmeldungen erzielen. Hier wurden bisher zu viele Pflichtangaben gefordert, beispielsweise die Geburtsdaten der Versammlungsleiter*innen. Das Landesamt für Zentrale Polizeiliche Dienste hat die Vordrucke auf unsere Beratung hin geändert.

Oft bedarf es nicht viel Aufwands, um dem Datenschutz gerecht(er) zu werden.

6.9 Löschmoratorien für Daten der Verwaltung zur Beweissicherung für Parlamentarischer Untersuchungsausschüsse (PUA)

Auch im Rahmen von Beweisaufnahmeverfahren durch PUA und im Zusammenhang damit verhängter sog. Löschmoratorien ist das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen zu beachten.

Während der 17. Legislaturperiode des nordrhein-westfälischen Landtags wurden fünf PUA eingesetzt. Diese sind ein Instrument der parlamentarischen Kontrolle der Regierungstätigkeit. Durch sie kann der Landtag, die Tätigkeit der Landesregierung zu einem konkreten Untersuchungsgegenstand überprüfen und mögliche Mängel der Landesverwaltung bei der Wahrnehmung ihrer gesetzlichen Aufgaben aufdecken. Aufgrund dieser wichtigen Kontrollfunktion des Parlaments über die Landesregierung sind PUA mit umfangreichen Beweisrechten ausgestattet. Sie dürfen von der Landesverwaltung grundsätzlich sämtliche für den Untersuchungsgegenstand erforderlichen Akten anfordern. Um den Bestand der beweisrelevanten Akten zu sichern, werden regelmäßig sog. Löschmoratorien verhängt. Das heißt, Vorgänge der Landesverwaltung, die nach den gesetzlichen Vorgaben für personenbezogene Daten eigentlich zu löschen wären, weil sie beispielsweise unrichtig oder für die Tätigkeit der Landesverwaltung nicht länger erforderlich sind, werden von der Löschung ausgenommen, wenn sie für den PUA von Beweiswert sind.

Diese grundsätzlich klaren und nachvollziehbaren Vorgaben führen in der Praxis zu einer Reihe von Detailproblemen. Diese beginnen bei der Frage, in welchem Zeitrahmen die Landesverwaltung Akten zu

übersenden und personenbezogene Daten von der Löschung auszunehmen hat. Häufiger Diskussionspunkt ist auch die Frage nach dem genauen Umfang der zu übermittelnden Daten. Schließlich ergeben sich praktische Probleme bei der Trennung von untersuchungsrelevanten und nicht relevanten personenbezogenen Daten in großen Datenbanken.

Um den Untersuchungsauftrag des PUA nicht zu gefährden, sind die Beweisbeschlüsse der PUAe häufig zunächst weit formuliert. Dies kann auf Seiten der Landesverwaltung zu Schwierigkeiten bei der Bestimmung der von dem Beschluss umfassten Daten führen. Dabei hat sie einerseits die gesetzliche Pflicht zu erfüllen, alle von dem Untersuchungsauftrag erfassten Daten an den PUA zu übermitteln und notwendige Daten von der Löschung auszunehmen. Gleichzeitig dürfen keine Daten an den PUA übermittelt und von der Löschung ausgenommen werden, die nicht von dem Beweisbeschluss umfasst sind. Dies genauer zu bestimmen, kann nur gelingen, wenn die Landesregierung und die jeweiligen PUA im Wege eines nachgelagerten Dialogs genauer bestimmen, welche Daten für den Untersuchungszweck relevant sind.

Für diejenigen, deren Daten bei der Verwaltung vorhanden sind, bedeutet ein Löschmoratorium immer, dass ihre Ansprüche auf Löschung der eigenen Daten für die Dauer des Moratoriums und den Untersuchungsgegenstand des PUA ausgesetzt sind. Deswegen ist es nicht gerechtfertigt, dass Daten, die für den Untersuchungsgegenstand irrelevant sind, ebenfalls dem Löschmoratorium unterworfen werden. Aber auch solche Daten, die dem Löschmoratorium un-

streitig unterfallen, dürfen nicht mehr von der Verwaltung genutzt werden, wenn sie bereits hätten gelöscht werden müssen und nur noch aus Anlass eines Moratoriums vorzuhalten sind. Hierzu fehlt derzeit eine klare Rechtsgrundlage, die sicherstellt, dass solche Daten ausschließlich für die Beweisaufnahme des PUA verwendet werden dürfen und dem Verwaltungsvollzug im Übrigen entzogen sind.

Nicht zuletzt aufgrund der Vielzahl von PUAe in den letzten Jahren und der rasant zunehmenden Datenmenge, die bei Behörden vorhanden ist, sind die obenstehenden Fragestellungen im vergangen Jahr verstärkt in den Blick der Datenschutzaufsichtsbehörden gelangt, die sich dazu positioniert haben. Siehe Entschließung der DSK „Parlamentarische Untersuchungsausschüsse und Löschmoratorien: Datenschutz durch klare Vorgaben und Verarbeitungsbeschränkungen für Behörden“ vom 23. März 2022 (Abdruck im Anhang).

Die LDI NRW hat zu diesem Thema Gespräche mit dem Innenministerium NRW und einem PUA des Landtags NRW geführt. Dabei wurde die Reichweite eines Löschmoratoriums in Bezug auf polizeiliche Datenbanken besprochen. Für Betroffene ist es oft von besonderem Interesse, dass ihre Daten aus Polizeidatenbanken gelöscht werden, wenn es keinen Grund (mehr) für deren Speicherung gibt. Die Gespräche machten deutlich, dass große und dynamische Datenbanken der Verwaltung erhebliche Schwierigkeiten bereiten, dem Datenschutz einerseits und dem Untersuchungsauftrag von PUAe andererseits gerecht zu werden. Umso wichtiger ist es, hier vorab in einem Dialog die Teile der Datenbank zu identifizieren, die für den Untersuchungsauftrag eines

PUA relevant sind und dem Löschmoratorium unterliegen. Das Gesetz über die Einsetzung und das Verfahren von Untersuchungsausschüssen des Landtags NRW enthält keine Regelungen für den Umgang mit Datenbanken und kann daher keine Lösungsansätze bieten.

Die LDI NRW hat gegenüber dem Parlament und seinen PUA keine Aufsichtsfunktion und ist daher insoweit nur beratend tätig.

Eine klare gesetzliche Regelung für den Umgang mit Daten, die bei der Verwaltung digital gespeichert sind und für Zwecke eines PUA benötigt werden, ist wünschenswert. Darin sollte auch geregelt werden, dass die Verwaltung datenschutzrechtlich zu löschende Daten, die für einen PUA noch vorgehalten werden, nicht mehr für Verwaltungsaufgaben nutzen darf. Bei der Programmierung großer Datenbanken der Verwaltung ist die Möglichkeit zur Trennung von Daten zu gewährleisten. Daten, die für die Erfüllung von Verwaltungsaufgaben noch notwendig sind und Daten, die nur noch für Kontrollzwecke vorgehalten werden müssen, müssen abtrennbar sein.

6.10 Zensus 2022 – Eigentum verpflichtet

Viele Vermieter*innen wandten sich anlässlich der Befragungen zum Zensus 2022 an die LDI NRW und zeigten sich besorgt, Vor- und Nachnamen ihrer Mieter*innen im Rahmen der Befragung zum Zensus 2022 ohne deren Einwilligung gegenüber den statistischen Ämtern preiszugeben.

Wegen der Pandemie ein Jahr später als ursprünglich vorgesehen fand in 2022 eine Volksbefragung, der Zensus 2022, statt.

Mit dem Zensus werden verschiedene Informationen über die Lebens- und Wohnsituation der Menschen in Deutschland ermittelt, um eine zuverlässige Datengrundlage für politische und gesellschaftliche Entscheidungen zu schaffen. Zu diesem Zweck wurden nicht nur Haushalte auf Stichprobenbasis befragt. Zusätzlich fand auch eine Gebäude- und Wohnungszählung statt.

Im Rahmen dieser Gebäude- und Wohnungszählung sind Eigentümer*innen, Verwalter*innen sowie die sonstigen Verfügungs- und Nutzungsberechtigten von Gebäuden oder Wohnungen gesetzlich aufgrund des Zensusgesetzes 2022 (ZensG 2022) verpflichtet, bestimmte Informationen an die statistischen Landesämter zu übermitteln.

Eigentümer*innen müssen als Vermieter*innen unter anderem neben der Anschrift der vermieteten Wohnung und der Zahl ihrer Bewohner*innen auch Namen und Vornamen von bis zu zwei Personen übermitteln, die die jeweilige Wohnung nutzen (§ 24 Abs. 1 in Verbindung mit §§ 9, 10 Abs. 2 Nr. 3 ZensG).

Diese sog. Hilfsmerkmale sind für die „Haushaltegenerierung“ (§ 29 Abs. 2 ZensG 2022) erforderlich. Über die Erhebung der Namen der Wohnungsnutzer*innen ist es möglich, Haushalte eindeutig konkreten Wohnungen zuzuordnen. Erst diese Zuordnung ermöglicht es, wichtige gesellschaftliche Fragen zu beantworten, etwa danach, in welchen Wohnverhältnissen Familien oder Alleinstehende leben. Die bereits in amtlichen Registern vorhandenen Informationen über zusammenwohnende Personen sind hierfür allein nicht ausreichend.

Wichtig ist, dass sämtliche Hilfsmerkmale, und damit auch die Namen der Mieter*innen aus der Gebäude- und Wohnungszählung, nach Abschluss der Aufbereitungs- und Prüfarbeiten durch die statistischen Ämter gemäß § 31 Abs. 1 Satz 1 ZensG 2022 gelöscht und nicht veröffentlicht werden.

Zwar sind die Vermieter*innen zur Auskunft gegenüber dem Landesstatistikamt verpflichtet. Gleichzeitig sind sie aber auch für die konkrete Übermittlung personenbezogener Daten datenschutzrechtlich verantwortlich. Daher müssen sie ihre Mieter*innen nach Art. 13 DS-GVO auch über die Weitergabe ihrer personenbezogenen Daten zum Zwecke der Zensusdurchführung vorab informieren.

Eigentümer*innen, Verwalter*innen sowie die sonstigen Verfügungs- und Nutzungsberechtigten von Gebäuden oder Wohnungen sind im Rahmen des Zensus 2022 gesetzlich unter anderem dazu verpflichtet, dem Landesstatistikamt die Namen von bis zu zwei Mieter*innen (Vor- und Nachname) mitzuteilen. Insoweit bedarf es keiner Einwilligung der Mieter*innen.

6.11 Handelsregister.de – Sensible Daten im Internet

Seit August 2022 ist eine Einsicht in das Handelsregister online ohne Registrierung und Gebühr möglich. In der Folge haben sich Bürger*innen an uns gewandt, weil sie dort beispielsweise Kopien ihrer Ausweise vorfanden und sich um eine missbräuchliche Verwendung dieser Daten sorgten.

Das von den Amtsgerichten als öffentliches Register geführte Handelsregister dient durch eine Registrierung von wesentlichen Rechtsverhältnissen der Kauf-

leute und Unternehmen der Sicherheit und Transparenz des geschäftlichen Verkehrs. Die Einsicht in das Handelsregister ist daher jedem zu Informationszwecken gestattet (§ 9 Handelsgesetzbuch, HGB) und wird über das Portal „Handelsregister.de“ ermöglicht. Dies betrifft grundsätzlich auch die Dokumente, die zum Register eingereicht werden müssen, etwa einen Gesellschaftsvertrag bei der Gründung einer GmbH.

Aufgrund der gesetzlich vorgeschriebenen Publizität der Daten finden dabei die Rechte der DS-GVO nur eingeschränkt Anwendung (§ 10a HGB). So werden beispielsweise überholte Daten in Dokumenten, etwa die Namen nicht mehr in einer Gesellschaft tätiger Geschäftsführer*innen nicht aus dem Handelsregister gelöscht. Vor dem Hintergrund der Publizität bleiben sie auch nach einer Veränderung weiter sichtbar. Es soll nachvollziehbar bleiben, wer zu welchem Zeitpunkt die Geschicke des betroffenen Unternehmens bestimmt hat.

Dass der Bundesgesetzgeber die Erfassung personenbezogener Daten im Handelsregister und die Möglichkeit einer Einsichtnahme vorsieht, ist keineswegs neu. Die seit dem 1. August 2022 eingetretene Änderung besteht allein darin, dass Abrufe aus dem Register nicht mehr kostenpflichtig sind und keine Nutzerregistrierung mehr vorgesehen ist.

Sowohl der Bundesregierung (BT-Drs. 20/4502 vom 15. November 2022, Seite 3) als auch vielen Betroffenen wurde allerdings erst nach Eintreten der Änderung bewusst, dass teils sensible Daten wie Ausweiskopien von den jeweiligen Amtsgerichten als Bestandteil der Dokumente veröffentlicht wurden. Vor dem Hintergrund der deutlich erhöhten Reichweite der abrufbaren Daten bzw. der Zahl der Personen,

die faktisch auf das Portal zugreifen, und der teils nicht erkennbaren Notwendigkeit, diese Informationen der Öffentlichkeit bereitzustellen, haben wir die Sorgen der Betroffenen über eine mögliche missbräuchliche Verwendung ihrer Daten ernst genommen.

Allerdings sind verantwortliche Stelle für die Eintragungen in das Register die jeweiligen Registergerichte, die insoweit nicht unserer Kontrolle unterliegen, da es sich um justizielle Tätigkeiten handelt, die zum Schutz der unabhängigen Entscheidungsfindung der Gerichte unserer Zuständigkeit entzogen sind (vgl. Art. 55 Abs. 3 DS-GVO). Auch gegenüber dem Ministerium der Justiz NRW als Betreiber des Portals „Handelsregister.de" bestand keine Möglichkeit eines zielführenden Einschreitens. Das Ministerium veröffentlicht die Dokumente pflichtgemäß und ohne Befugnis einer inhaltlichen Einflussnahme im Auftrag der insoweit unabhängigen Registergerichte.

Da der Veröffentlichung der Daten im Handelsregister bundesgesetzliche Normen zu Grunde liegen, können Änderungen an diesen Regelungen nicht unmittelbar durch nordrhein-westfälische Behörden bewirkt, sondern lediglich angeregt werden. Wir sind diesbezüglich bereits im August 2022 mit dem Ministerium der Justiz NRW in Kontakt getreten und haben zudem die Notarkammern in NRW (aufgrund der Schnittstellenfunktion der Notar*innen zwischen Registergerichten und Betroffenen) für datenschutzrechtliche Belange bei der Einreichung von Dokumenten sensibilisiert.

In der Zwischenzeit hat das Bundesministerium der Justiz Änderungen in § 9 der Handelsregisterverordnung vorgenommen, mit denen zukünftig der Umfang der zu veröffentlichenden Dokumente reduziert wird.

Zudem wurde klargestellt, dass Betroffene bei den jeweiligen Registergerichten einen Austausch von Dokumenten beantragen können, wenn diese Angaben enthalten, die nicht veröffentlicht werden mussten.

Aber Achtung: Auch nach der Änderung der Handelsregisterverordnung haben Betroffene bzw. Notar*innen besondere Sorgfalt bei der Einreichung der Dokumente walten zu lassen. Beinhaltet eine Datei Dokumente, deren Einreichung vorgeschrieben ist, kann das Registergericht grundsätzlich alle in der Datei enthaltenen Dokumente mit der Folge einer Veröffentlichung in den sog. Registerordner einstellen und ist im Regelfall nicht dazu angehalten, bei den Anmeldenden nachzufragen, ob eine Veröffentlichung gewünscht ist (BR-Drs. 560/20 vom 2. November 2022, Seite 29). Die Verantwortung, Dokumente gegebenenfalls in gesonderten Dateien einzureichen, soll daher auf die Einreichenden übertragen werden.

Eine Datenschutzberatung bei der Überarbeitung der Verordnung ist durch unser Haus nicht erfolgt, da diese in den Zuständigkeitsbereich des BfDI fällt.

Um weitere Verbesserungen zu erreichen, hat der Bundesrat das Bundesministerium der Justiz aufgefordert, weitere Schritte zu prüfen, die einer missbräuchlichen Nutzung von im Register veröffentlichten Daten entgegenwirken (BR-Drs. 560/22, Beschluss Seite 1). Zudem erwägen die Landesjustizverwaltungen unter Beteiligung der Bundesnotarkammer die Dienstordnung für Notar*innen zu ändern, mit dem Ziel für das Register nicht erforderliche Angaben nicht in die Beurkundung aufzunehmen.

Die Publizitätsfunktion des Handelsregisters rechtfertigt die Veröffentlichung bestimmter für die Nachvollziehbarkeit des Registers notwendiger personenbezogener Daten. Seit das Handelsregister ohne weitere Hürden für jede*n über das Internet erreichbar ist, wurde offensichtlich, dass darin auch nicht für die Registerführung notwendige personenbezogene Daten enthalten sind, die damit potentiell missbräuchlich genutzt werden können. Der Bundesgesetzgeber hat die Notwendigkeit erkannt, korrigierend tätig zu werden, und erste sinnvolle Schritte zur Wahrung der Rechte von Betroffenen unternommen.

7. Gesundheit und Soziales

7.1 Bedarfsermittlung zur Rehabilitation und Teilhabe von Menschen mit Behinderung

Die LDI NRW hilft dabei, den Datenschutz zu verbessern, wenn es darum geht, den individuellen Unterstützungsbedarf von Menschen mit Behinderung festzustellen.

Menschen mit Behinderungen haben Anspruch auf Unterstützungsleistungen zur Rehabilitation und Teilhabe, die sich an ihrem individuellen Bedarf orientieren. Das Neunte Buch Sozialgesetzbuch (SGB IX) unterteilt diese Leistungen in fünf Gruppen: Leistungen zur medizinischen Rehabilitation, Leistungen zur Teilhabe am Arbeitsleben, (sonstige) ergänzende unterhaltssichernde Leistungen, Leistungen zur sozialen Teilhabe sowie Leistungen zur Teilhabe an Bildung.

In NRW sind die Landschaftsverbände Rheinland und Westfalen-Lippe als Träger der Eingliederungshilfe für Menschen mit Behinderungen für die Feststellung ihres individuellen Bedarfs zuständig. Die konkreten Leistungen werden nach der Bewilligung von Leistungserbringern, zum Beispiel Wohlfahrtsverbänden, erbracht.

Im Zuständigkeitsbereich des Landschaftsverbands Rheinland gibt es ein besonderes Modell, um die Leistungen möglichst passgenau auf den individuellen Bedarf zuzuschneiden: Dort unterstützen Mitarbeiter*innen der jeweiligen Leistungserbringer*innen Menschen mit Behinderungen dabei, ihre individuelle Hilfsbedürftigkeit zu ermitteln und Anträge zu stellen. Die ermittelten Hilfebedarfe werden sodann von Mit-

arbeiter*innen der Leistungserbringer auf einer Onlineplattform erfasst. Bedienstete des Landschaftsverbandes Rheinland können sie dort einsehen, prüfen und bewilligen. Das Verfahren ist gesetzlich in dieser Form nicht vorgesehen. Diese partizipative Zusammenarbeit kann andererseits bewirken, dass die einen Menschen mit Behinderung betreuenden Leistungserbringer und der Leistungsträger bei der Unterstützung der Menschen Hand in Hand arbeiten und ihre Angebote für die jeweilige Person optimal abstimmen. Das Verfahren kann mangels gesetzlicher Grundlage aber nur auf Basis einer informierten Einwilligung durchgeführt werden.

Es hatte sich bei der Prüfung der Verfahrensabläufe herausgestellt, dass die Eintragungen in der Online-Plattform nicht nur für die Bediensteten des Landschaftsverbandes, sondern auch für alle anderen Beschäftigten der Leistungserbringer lesbar waren, die mit dem jeweiligen Fall betraut waren. Dies ist dann problematisch, wenn Bedarf aus verschiedenen Lebensbereichen, zum Beispiel aus den Bereichen Arbeiten und Wohnen, beantragt wird. Um den Bedarf für bestimmte Hilfeleistungen näher zu begründen, werden sehr persönliche und zum Teil intime Angaben zu sensiblen Themen auf der Onlineplattform festgehalten, beispielweise zu gesundheitlichen Veranlagungen, familiären und partnerschaftlichen Beziehungen und daraus resultierenden Schwierigkeiten. Nicht immer sind die Informationen, die ein Leistungserbringer im Bereich Wohnen erhebt, zugleich für einen Leistungserbringer im Bereich Arbeit relevant. Was für Leistungserbringer nicht relevant ist, dürfen sie auch nicht erfahren.

Gemeinsam mit dem Landschaftsverband Rheinland haben wir daraufhin die Prozessabläufe geprüft und analysiert. Hier zeigte sich, dass es besonderer Vorkehrungen bedarf, damit nur diejenigen auf diese Daten zugreifen können, deren Kenntnisnahme unbedingt erforderlich ist. Zudem muss sichergestellt sein, dass lediglich solche intimen und sensiblen Daten erfasst werden, die zur Beurteilung eines konkreten Hilfebedarfs erforderlich sind. Auch eine Erfassung von Daten Dritter bedarf besonderer Vorkehrungen.

Wir haben dem Landschaftsverband Rheinland zahlreiche Hinweise an die Hand gegeben, um den Schutz der Daten von Menschen mit Behinderungen zu verbessern.

Die Hinweise beziehen sich nicht nur auf technische Änderungen bei den Zugriffsberechtigungen für die Daten, die auf der Onlineplattform erfasst sind. Sie umfassen auch eine wesentliche Verbesserung der Einwilligungserklärungen, die die Antragstellenden zur Verarbeitung personenbezogener Daten abgeben. Durch eine deutlich transparentere und detailliertere Gestaltung soll ihnen klar aufgezeigt werden, wer welche Daten verarbeitet. Es soll ausdrücklich darauf hingewiesen werden, dass mehrere Leistungserbringer die gespeicherten Daten einsehen können, damit Antragstellende dies bei ihrer Einwilligungsentscheidung berücksichtigen können. Zudem sollen die erteilten Einwilligungen besser dokumentiert werden. Soweit Daten Dritter wie Partner*innen oder Familienangehörige auf der Onlineplattform gespeichert werden sollen, haben wir darauf hingewiesen, dass dies lediglich mit deren Einwilligung bzw. nach einer Pseudonymisierung dieser Daten möglich ist. Schließlich

haben wir eine deutlichere Information darüber gefordert, dass die Einwilligung zur Datenverarbeitung durch Leistungsträger auch verweigert werden kann. Sie soll mit dem ausdrücklichen Hinweis darauf verbunden werden, dass in diesem Fall die weitere Bedarfsermittlung ausschließlich durch Bedienstete des Landschaftsverbandes erfolgt.

Um sicherzustellen, dass lediglich solche Daten in der Onlineplattform gespeichert werden, die für die Ermittlung des Hilfebedarfs wirklich erforderlich sind, haben wir eine Sensibilisierung aller Mitarbeiter*innen der Leistungserbringer*innen gefordert, die an der Bedarfsermittlung beteiligt sind. Die Mitarbeiter*innen müssen vor jeder Eintragung im Einzelfall kritisch prüfen, ob die Erfassung der Daten an sich und im bestimmten Umfang erforderlich ist.

Die LDI NRW prüft, ob diese Maßnahmen umgesetzt werden.

Die Wohlfahrtsverbände, die ihre datenschutzrechtlichen Bedenken zum bisherigen Verfahren vorgetragen hatten, haben das Vorgehen der LDI NRW ausdrücklich begrüßt.

Besonders sensible persönliche Daten von Menschen mit Behinderung bedürfen eines besonderen Schutzes. Die LDI NRW hat den verantwortlichen Stellen konkrete Hinweise zur Verbesserung in den Prozessen der Bedarfsermittlung gegeben und überwacht die Umsetzung.

7.2 Bewertungen von Ärzt*innen im Internet

Reagieren Ärzt*innen im Internet auf negative Online-Bewertungen ihrer Patient*innen, dürfen sie den besonderen Schutz von Gesundheitsdaten nicht aus dem Blick verlieren.

Mitunter äußern sich Patient*innen auf Bewertungsportalen im Internet kritisch über ärztliche Behandlungen. In einem Fall veröffentlichte ein Arzt einen Gegenkommentar zu einem aus seiner Sicht ungerechtfertigten Angriff. Dabei gab er Erkenntnisse aus den Arztbesuchen, Diagnosen, Behandlungsergebnisse usw. preis. Dies ist unzulässig und wurde mit einem Bußgeld geahndet.

Bürger*innen, die Arztpraxen online bewerten, können sich hierbei grundsätzlich auf ihre Meinungsfreiheit berufen. Neben straf- und zivilrechtlichen Grenzen, etwa bei Beleidigungen, müssen sie jedoch datenschutzrechtliche Vorgaben einhalten, sofern sie personenbezogene Daten Dritter verarbeiten. So dürfen Bürger*innen etwa nicht einfach private Adressen oder Telefonnummern ihrer Ärzt*innen in einem Bewertungsportal veröffentlichen.

Halten Ärzt*innen wiederum eine kritische Online-Bewertung für ungerechtfertigt, können sie zwar die Bewertung durch einen eigenen Kommentar richtigstellen. Allerdings dürfen auch sie hierbei nicht gegen das Datenschutzrecht oder die ärztliche Schweigepflicht verstoßen.

Vor allem dürfen Ärzt*innen durch eine Online-Gegendarstellung keine Inhalte des Ärzt*innen-Patient*innen-Verhältnisses offenbaren. Denn Angaben über den Gesundheitszustand, Praxisbesuche bzw.

Untersuchungen, die sich auf eine bestimmte oder bestimmbare Person beziehen, unterliegen als Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO einem besonderen Schutz. Sie dürfen nur unter strengen datenschutzrechtlichen Voraussetzungen verarbeiten werden (vgl. Art. 9 Abs. 2 DS-GVO). Patient*innen müssen darauf vertrauen können, dass Informationen über Krankheiten, körperliche bzw. psychische Beschwerden usw., die sie im Rahmen einer ärztlichen Behandlung offenbart haben, nicht leichtfertig veröffentlicht werden.

Keinesfalls rechtfertigt eine negative Online-Bewertung als solche die Veröffentlichung sensibler Gesundheitsdaten. Die Meinungsfreiheit der Ärzt*innen muss in diesem Fall hinter dem Recht auf informationelle Selbstbestimmung der Patient*innen zurückstehen.

Nach Einleitung eines aufsichtsbehördlichen Verfahrens durch die LDI NRW entfernte der Arzt seine Gegenkommentare. Wegen des gravierenden datenschutzrechtlichen Verstoßes setzte die LDI NRW gegenüber dem Arzt ein Bußgeld fest.

Wollen Ärzt*innen kritische Online-Bewertungen von Patient*innen öffentlich durch Kommentierung der Bewertung richtigstellen, dürfen sie dabei ihrerseits keine vertraulichen Gesundheitsdaten von Patient*innen offenbaren.

7.3 Erfasst der Auskunftsanspruch die Erläuterung von medizinischen Fachbegriffen?

Patient*innenakten enthalten zahlreiche Fachbegriffe, die für medizinische Laien oft nicht verständlich sind. Deshalb wird immer wieder die Frage aufgeworfen, ob Patient*innen im Zusammenhang mit Auskunftsansprüchen verlangen können, dass ihnen medizinische Fachbegriffe nachvollziehbar erläutert werden.

Der Auskunftsanspruch aus Art. 15 DS-GVO ist ein zentrales Betroffenenrecht. Er begegnet insbesondere hinsichtlich Art und Umfang der zu erteilenden Auskunft einigen Herausforderungen. Dies betrifft auch Auskünfte aus Patient*innenakten. Hierin dokumentieren Ärzt*innen sämtliche aus medizinischer Sicht notwendigen Behandlungsschritte: Anamnesen, Diagnosen, Untersuchungen, Befunde, Therapien, operative Eingriffe, Behandlungsergebnisse und -verläufe usw. Naturgemäß werden hierzu vorwiegend medizinische Fachbegriffe verwendet. Dies macht es medizinischen Laien oft schwer, den Inhalt von Patient*innenakten zu verstehen.

Art. 12 Abs. 1 DS-GVO sieht vor, dass datenschutzrechtliche Auskünfte in einer „klaren und einfachen Sprache“ erfolgen sollen. Vor dem Hintergrund, dass der Auskunftsanspruch das Ziel hat, Betroffenen die Möglichkeit einzuräumen, zu prüfen, welche personenbezogenen Daten von datenschutzrechtlich verantwortlichen Stellen zu ihrer Person verarbeitet werden, bedeutet das für die Verwendung medizinischer Fachbegriffe Folgendes:

Zwar sind medizinische Fachbegriffe, die sich auf jeweils betroffene Personen beziehen, generell Teil der

verpflichtenden Auskunft. Jedoch umfasst diese Auskunft grundsätzlich nicht die Erklärung, welche Bedeutung diese haben. Allein die Bedeutung dieser Begriffe stellt nämlich keine datenschutzrechtliche, sondern eine medizinische Fachfrage dar. Die verständliche Erläuterung der medizinischen Diagnose, ist Bestandteil des Behandlungsverhältnisses und keine datenschutzrechtliche Frage.

Abweichend davon sind medizinische Fachbegriffe im Rahmen der Auskunft nach Art. 15 DS-GVO jedenfalls dann zu erläutern, wenn und soweit ihnen eine Bedeutung für die Datenverarbeitung zukommt: Wird zum Beispiel der Löschungszeitpunkt von personenbezogenen Daten an einen medizinischen Umstand geknüpft, muss der betroffenen Person für Laien verständlich verdeutlicht werden, von welchem konkreten medizinischen Faktor die Löschung abhängt. Denn auf diese Weise wird sichergestellt, dass Patient*innen über die Ausübung ihrer Betroffenenrechte entscheiden können.

Medizinische Fachbegriffe müssen bei der Geltendmachung des Auskunftsrechts nach Art. 15 DS-GVO in der Regel nicht näher erläutert werden. Eine Ausnahme gilt dann, wenn eine konkrete Datenverarbeitung durch einen medizinischen Fachbegriff bedingt ist.

7.4 Auskunftsansprüche von Tierhalter*innen

Tierhalter*innen haben in der Regel kein Auskunftsrecht zur „Patient*innenakte“ ihrer Haustiere.

Oft werden Tierhalter*innen Auskünfte aus der Behandlungsakte ihres Haustieres verweigert. Dies liegt

daran, dass der Auskunftsanspruch aus Art. 15 DS-GVO nur personenbezogene Daten erfasst, also nur solche, die einer Person zuzuordnen sind. Daten, die sich allein auf ein Tier beziehen, fallen hingegen nicht unter diesen Anspruch. Jedoch können Daten, die einen Bezug zu den Tierhalter*innen haben, Gegenstand eines Auskunftsanspruchs sein. Ein solcher Bezug besteht zum Beispiel für die Angabe, dass eine bestimmte Tierhalterin Eigentümerin eines bestimmten Tieres ist. Hierbei handelt es sich um ein personenbezogenes Datum. Anders verhält es sich, wenn Daten betroffen sind, die nur den Gesundheitszustand eines Tieres oder Behandlungsmaßnahmen dokumentieren. Diese Daten weisen in der Regel keinen Personenbezug auf.

Daraus folgt: Ein datenschutzrechtlicher Auskunftsanspruch bezieht sich lediglich auf die Teile einer Behandlungsakte des Haustieres, die auch Informationen über die Tierhalter*innen enthalten. Dies wäre der Fall bei Notizen über Telefonate, die mit diesen geführt wurden, Notizen zu besonderen Wünschen oder deren Anweisungen. Lediglich diese Daten wären im Rahmen eines Auskunftsanspruchs nach Art. 15 DS-GVO mitzuteilen.

Tierhalter*innen können ihre darüber hinausgehenden Anliegen zivilrechtlich aus dem von ihnen abgeschlossenen Tierbehandlungsvertrag verfolgen.

Die Gesundheitsdaten eines Haustieres beziehen sich auf das Tier selbst und stellen damit keine personenbezogenen Daten dar. Ein Auskunftsanspruch nach Art. 15 DS-GVO besteht für diese Daten in der Regel nicht.

7.5 Abrechnung über privatärztliche Verrechnungsstellen durch Labore

Lassen Labore, die als verantwortliche Stellen agieren, ihre Abrechnung über privatärztliche Verrechnungsstellen durchführen, ist hierfür eine datenschutzrechtliche Einwilligung von den Patient*innen erforderlich. Auch ein fehlender Patient*innenkontakt ändert hieran nichts.

Die LDI NRW erreichen immer wieder Nachfragen dazu, ob für Abrechnungen von Laborleistungen über privatärztliche Verrechnungsstellen eine gesonderte Einwilligungserklärung von Patient*innen erforderlich ist. Ärzt*innen verschicken im Zusammenhang mit Behandlungen oft verschiedenste Proben zur Untersuchung an externe Labore. Hierfür ist in der Regel keine gesonderte Einwilligung von Patient*innen erforderlich. Vielmehr schließen die behandelnden Ärzt*innen für die Untersuchung der Proben in Stellvertretung für ihre Patienten*innen einen Behandlungsvertrag mit den Laboren ab. Die Abrechnung der laborärztlichen Leistungen erfolgt in diesen Fällen deshalb nicht über die behandelnden Ärzt*innen sondern durch die Labore selbst. Ob für diese Abrechnungen eine gesonderte Einwilligung der Patient*innen erforderlich ist, hängt davon ab, ob die Labore diese selbst vornehmen oder externe Abrechnungsstellen einschalten.

Soweit Labore die Abrechnung nicht selbst vornehmen, sondern eine privatärztliche Verrechnungsstelle beauftragen, bedarf es hierfür einer ausdrücklichen Einwilligung der Patienten*innen.

Labore sind in datenschutzrechtlicher Hinsicht eigenständig verantwortliche Stellen, sofern sie durch

eine*n Laborärzt*in geleitet werden. Als solche benötigen sie, wie alle anderen Leistungserbringer auch, eine datenschutzrechtliche Einwilligung zur Übermittlung und Verarbeitung der Gesundheitsdaten durch eine externe Abrechnungsstelle. Labore wenden dagegen häufig ein, dass ihnen die nachträgliche Einholung einer Einwilligung nicht zumutbar sei, da sie keinen unmittelbaren Kontakt zu den Patient*innen hätten. Das ist aber rechtlich unerheblich. Die Einwilligung ist in diesem Fall die notwendige Rechtsgrundlage, die den Laboren überhaupt erst die Übermittlung der Patient*innendaten erlaubt. Sie ist auch dann nicht verzichtbar, wenn die verantwortliche Stelle einigen Aufwand betreiben muss, um die Einwilligungserklärung einzuholen. Eine Möglichkeit, könnte darin bestehen, entsprechende Einwilligungen nach Absprache bereits durch die behandelnden Ärzt*innen einholen zu lassen. Laboren obliegt als verantwortlichen Stellen die Nachweispflicht nach Art. 5 Abs. 2 in Verbindung mit Abs. 1 Buchstabe a DS-GVO.

Wird eine Einwilligung nicht erteilt, muss die Abrechnung durch das Labor selbst erfolgen. Weiterhin ist zu beachten, dass Labore als verantwortliche Stellen für die Erteilung der Informationspflichten nach Art. 14 DS-GVO zuständig sind. Diese könnten ebenso über die behandelnden Ärzt*innen erteilt werden bzw. auch im Nachgang unter den Voraussetzungen des Art. 14 Abs. 3 Buchstabe a oder b DS-GVO.

Sofern Labore als eigenverantwortliche Stellen agieren, müssen sie auch die Einwilligung zur Abrechnung über privatärztliche Verrechnungsstellen einholen und die Informationen nach Art. 14 DS-GVO erteilen.

7.6 Unbefugte Nutzung von Forschungsdaten

Forschungsdaten, die aufgrund einer Einwilligung erhoben wurden, dürfen grundsätzlich nur für die Zwecke genutzt werden, für die sie zur Verfügung gestellt werden. Die Nutzung für weitere Studien ist nicht ohne Weiteres zulässig.

Im Rahmen eines groß angelegten länderübergreifenden Forschungsprojektes diverser Universitätskliniken wurden mit Einwilligung der Probanden Daten für die Durchführung einer Prostatakrebsstudie erhoben. Diese Daten wurden anschließend ohne Wissen der Probanden zusätzlich für eine Sexualstudie ausgewertet. Die Ergebnisse beider Studien wurden veröffentlicht. Die Daten für beide Studien wurden – wenn auch in getrennten Fragebögen – gemeinsam erhoben. An keiner Stelle wurde allerdings darauf hingewiesen, dass die Daten auch noch für eine andere Studie als die Krebsstudie erhoben werden. Inhaltlich ließen die Fragen bereits starke Zweifel daran aufkommen, ob die Erhebung zur Erforschung von Prostatakrebs erforderlich sein könnte. Die Fragen betrafen intime sexuelle Details, die mit der Erforschung der Krankheit nicht in Verbindung gebracht werden konnten.

Die zusätzliche Nutzung der Daten zur Erforschung eines von der Einwilligung nicht gedeckten Forschungsgegenstandes, der einen sehr intimen Lebensbereich betrifft, ist ein erheblicher Eingriff in das Recht auf informationelle Selbstbestimmung. Da die eingeholte Einwilligung mit keinem Wort diesen weiteren Forschungsgegenstand erkennen ließ, war die Verarbeitung der Daten rechtswidrig.

Die Forschungsfreiheit ist zwar grundrechtlich geschützt und die DS-GVO privilegiert sie an zahlreichen Stellen, etwa bei den Informationspflichten (Art. 14 Abs. 5 Buchstabe b oder beim Recht auf Vergessenwerden (Art. 17 Abs. 3 Buchstabe d DS-GVO). Frei von datenschutzrechtlichen Vorgaben ist sie jedoch nicht. Tatsächlich wird die wissenschaftliche Forschung auch hinsichtlich der Zweckangabe im Rahmen der Einwilligung privilegiert. So reicht unter Umständen die Angabe bestimmter Forschungsbereiche bereits aus, wenn der Zweck der Verarbeitung für die wissenschaftliche Forschung zum Zeitpunkt der Erhebung nicht vollständig angegeben werden kann. Dadurch wird dem Umstand Rechnung getragen, dass wissenschaftliche Forschung einem dynamischen Prozess unterliegt und sich beständig verändert. Dabei darf die ursprüngliche Zweckbindung aber nicht verlassen werden.

Bei der vermeintlichen Prostatastudie war jedoch von vornherein klar, dass der Fragebogen nicht allein auf eine Datenerhebung im Zusammenhang mit der Erforschung von Krebserkrankungen abzielte. Hierüber hätten die Probanden informiert werden müssen. Ihre Einwilligung zur Verarbeitung ihrer Daten hätte sich eindeutig auch auf die zweite Studie beziehen müssen.

Die LDI NRW hat in Abstimmung mit den übrigen betroffenen Aufsichtsbehörden darauf hingewirkt, dass der Datensatz zu den zusätzlich und unrechtmäßig erhobenen Daten für die Sexualstudie (45 Zusatzfragen) gelöscht und die Veröffentlichungen der Studienergebnisse – soweit dies möglich war – aus dem Internet entfernt wurden.

Eine Einwilligung in die Verarbeitung von personenbezogenen Daten zu Forschungszwecken muss informiert erfolgen und den Gegenstand der Forschung so konkret wie möglich benennen.

7.7 Informationsschreiben des Bundesministers für Gesundheit zur zweiten Auffrischungsimpfung gegen COVID-19

Durften gesetzliche Krankenkassen das Schreiben des Bundesministers für Gesundheit zur zweiten Auffrischungsimpfung gegen COVID-19 im Jahr 2022 an ihre Versicherten versenden?

Im letzten Jahr haben Millionen Menschen über 60 Jahre in Deutschland ein Schreiben des Bundesministers für Gesundheit zur zweiten Auffrischungsimpfung gegen COVID-19 erhalten. Das mir vorliegende Schreiben trägt allein den Briefkopf des Bundesministeriums für Gesundheit und ist allein durch den Bundesgesundheitsminister unterzeichnet. Dadurch ist der Eindruck entstanden, die Versichertendaten seien dem Bundesministerium übermittelt worden.

Mittlerweile ist bekannt, dass dies nicht geschehen ist. Die Schreiben wurden von der jeweiligen Krankenkasse kopiert und an die bei ihr versicherten Personen im Alter von über 60 Jahren versandt.

Gleichwohl entstand der Eindruck, die Krankenkassen würden „im Auftrag“ des Bundesministers handeln und Versandkosten im Wert von Millionen Euro für das Bundesgesundheitsministerium erbringen. Ersteres wäre wegen der Bindung der Kassen an das Sozialgeheimnis datenschutzrechtlich bedenklich. Sie dürfen die Daten der Versicherten nur für gesetzlich

festgelegte Zwecke nutzen und nicht darüber hinaus für Belange anderer Stellen, selbst wenn es sich dabei um den Bundesgesundheitsminister handelt.

Tatsächlich sei das Schreiben jedoch nach Auskunft der von uns angeschriebenen Krankenkasse entgegen des äußeren Eindrucks auch als eigenes Informationsschreiben der Krankenkasse gedacht. Die Versicherung wollte ihre eigenen Versicherten auf die Schutzimpfung aufmerksam machen, die zum damaligen Zeitpunkt insbesondere für Menschen über 60 Jahre empfohlen wurde.

Eine Nutzung der Versichertendaten für diesen Zweck ist nach § 20i Abs. 4 Satz 2 SGB V möglich: Die Krankenkassen können danach die Versicherten in geeigneter Form über fällige Schutzimpfungen und über andere Maßnahmen nach § 20i Abs. 2 und 3 SGB V, auf die sie einen Anspruch auf Leistungen haben, versichertenbezogen informieren.

Die Krankenkasse will dies zukünftig in vergleichbaren Fällen besser machen – durch Verwendung des eigenen Briefbogens oder durch Beifügung eines erklärenden Begleitschreibens. Die jetzt entstandenen Missverständnisse können damit zukünftig vermieden werden.

Die nach § 284 Abs. 1 SGB V rechtmäßig erhobenen und gespeicherten versichertenbezogenen Daten dürfen von der Krankenkasse für andere Zwecke genutzt werden, wenn dies im Sozialrecht angeordnet oder erlaubt ist – zum Beispiel zur Information der eigenen Versicherten nach § 20i Abs. 4 Satz 2 SGB V über eine COVID-Schutzimpfung.

8. Datenschutz am Arbeitsplatz

8.1 Krankheitstage, Resturlaub und Überstunden von Beschäftigten – Was dürfen Vorgesetzte wissen?

Informationen zum Arbeitsverhalten, zur individuellen Leistung, zu Fehlzeiten etc. von Beschäftigten liegen in der Regel in der personalverantwortlichen Stelle vor. Fraglich ist, ob Vorgesetzten regelmäßig Informationen zu Krankheitstagen, Überstunden und Resturlaubstagen von Beschäftigten der jeweiligen Abteilung bereitgestellt werden dürfen.

Hinter dem Wunsch, diese Daten an direkte Vorgesetzte der Beschäftigten weitergeben zu dürfen, kann zum Beispiel der Gedanke stehen, dass sie im Hinblick auf die Personalplanung oder den Personaleinsatz von erheblichem praktischem Nutzen sein können.

Generell gilt, dass Arbeitgeber*innen personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses insbesondere verarbeiten dürfen, wenn dies für dessen Durchführung erforderlich ist (§ 26 Abs. 1 Satz 1 BDSG). Die Datenverarbeitung kann zudem auch zur Wahrung der berechtigten Interessen der Verantwortlichen oder von Dritten erforderlich sein, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO).

Sofern die Abwesenheitszeiten von Beschäftigten in der personalverantwortlichen Stelle erfasst werden,

handelt es sich um eine Verarbeitung von Beschäftigtendaten zur Durchführung des Arbeitsverhältnisses im Sinne des § 26 Abs. 1 Satz 1 BDSG.

Bei Daten über krankheitsbezogene Abwesenheitszeiten in Verbindung mit der Nennung des Grundes der Erkrankung handelt es sich zudem nicht nur um vertrauliche Personaldaten, sondern auch um besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO (Gesundheitsdaten). Die Verarbeitung solcher Daten ist unter den Voraussetzungen des § 26 Abs. 3 BDSG in Verbindung mit Art. 9 Abs. 2 DS-GVO für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Krankheitstage und Arbeitsunfähigkeitsbescheinigungen

Eine Rechtsgrundlage für die Übermittlung der Anzahl von zurückliegenden Krankheitstagen an Fachvorgesetzte besteht grundsätzlich nicht. Zwar wird in der Regel eine Erforderlichkeit bestehen, Vorgesetzte über aktuelle krankheitsbedingte Ausfälle und deren voraussichtliche Dauer zu informieren, damit beispielsweise betriebliche Abläufe angepasst oder Vertretungen geregelt werden können. Die Kenntnis über die Anzahl zurückliegender Krankheitstage ist für diesen Zweck jedoch nicht notwendig. Arbeitsunfähigkeitsbescheinigungen enthalten zudem auch Angaben zur ausstellenden Arztpraxis und lassen

Rückschlüsse auf die jeweilige Fachrichtung und damit die Art der Erkrankung zu. Bei derartigen Gesundheitsinformationen handelt es sich um besondere Kategorien personenbezogener Daten, für deren Verarbeitung ein strengerer Maßstab gilt. Insoweit besteht regelmäßig keine Erforderlichkeit für eine Kenntnisnahme derartiger Informationen außerhalb der personalverantwortlichen Stelle.

Überstunden

Eine Mitteilung an Vorgesetzte kann – auch mit Blick auf die Fürsorgepflicht von Arbeitgeber*innen – in Betracht kommen, soweit bestimmte Zeitrahmen überschritten (oder unterschritten) werden. Insoweit empfehlen sich, etwa in einer Betriebsvereinbarung, konkrete Festlegungen insbesondere zu den betreffenden Zeitrahmen, also ab welchem Maß des Über- oder Unterschreitens der Sollarbeitszeit entsprechende Mitteilungen an welche Personen erfolgen können.

Urlaubstage

Die Erforderlichkeit einer Mitteilung von Resturlaubstagen an Vorgesetzte kann nicht pauschal beurteilt werden. Führungskräfte dürfen nur auf diejenigen Daten zugreifen, die zur Wahrnehmung ihrer Führungsaufgabe erforderlich sind. In Betracht kommen kann dies etwa, wenn eine Kenntnis von Resturlaubstagen für Zwecke der Personalplanung erforderlich ist. So ist es beispielsweise in Branchen mit zeitgebundenen Projektarbeiten notwendig, dass bestimmte Beschäftigte oder eine bestimmte Anzahl von Personen für ein Projekt eingeplant werden, um die Betriebsabläufe sicherzustellen. Gleichzeitig kann es vorkommen, dass sich die Zeiträume von Projekten und die

Verfallfristen für Urlaubstage der Beschäftigten überschneiden. Damit eine effektive Personalplanung für die Projekte erfolgen und zugleich sichergestellt werden kann, dass Beschäftigte den ihnen zustehenden Urlaub nehmen können, ist für Vorgesetzte insoweit die Kenntnis von den Resturlaubstagen der Beschäftigten erforderlich. Derartige Informationen sind erforderlichenfalls primär bei der betroffenen Person selbst zu erfragen.

Innerhalb einer für die Verarbeitung verantwortlichen Stelle können Beschäftigtendaten nicht frei fließen. Es dürfen immer nur die Stellen oder Personen Beschäftigtendaten erhalten, für deren Aufgabenerfüllung die Kenntnis der Daten erforderlich ist. Dabei sind die Informationen primär bei der betroffenen Person zu erheben.

8.2 Offene Listen mit 3G-Nachweisen am Arbeitsplatz

In der „heißen Phase“ der Überprüfung der 3G-Nachweise „geimpft, genesen oder getestet“ kam der Beschäftigtendatenschutz manchmal zu kurz. Beispielsweise sollten Beschäftigte ihren 3G-Status in Listen eintragen. Dabei konnten sie alle vorherigen Eintragungen der Kolleg*innen auf der Liste sehen. So funktioniert Beschäftigtendatenschutz nicht.

Bei den Daten zum Impf- und Genesenen-Status sowie negativen Testbescheinigungen handelt es sich um Gesundheitsdaten (Art. 4 Nr. 15 DS-GVO) und damit um eine besondere Kategorie personenbezogener Daten (Art. 9 Abs. 1 DS-GVO), deren Verarbeitung grundsätzlich untersagt ist. Dies bedeutet, dass Arbeitgeber*innen den Impfstatus von Beschäftigten

nur verarbeiten dürfen, soweit eine gesetzlich geregelte Ausnahme eine Verarbeitung gestattet. Derartige Ausnahmen finden sich zum Beispiel im Infektionsschutzgesetz.

Die bis zum März 2022 geltende Fassung des § 28b Abs. 3 Satz 1 IfSG verpflichtete Arbeitgeber*innen zur Nachweiskontrolle und zur Dokumentation darüber, dass Beschäftigte der Pflicht zur Mitführung oder Hinterlegung eines 3G-Nachweises (§ 28b Abs. 3 Satz 2 IfSG a. F.) nachkamen. Soweit es für eine lückenlose Erfüllung ihrer Nachweispflicht erforderlich war, durften Arbeitgeber*innen personenbezogene Daten, wie den Namen und das Vorliegen eines gültigen 3G-Nachweises inklusive der Gültigkeitsdauer, abfragen und dokumentieren (siehe Art. 28b Abs. 3 Satz 3 IfSG a. F.). Dies konnte auch in Form einer Liste geschehen. Erfasst werden durften nur die für die Aufgabe der Dokumentation erforderlichen Daten. Hierzu gehörten neben personenbezogenen Daten, die die Zuordnung zu einer Person erlaubten und Verwechslungen ausschlossen (Name, Geburtstag, Personalnummer oder Arbeitsbereich), das Vorliegen eines gültigen 3G-Nachweises inklusive der Gültigkeitsdauer und des Enddatums des nachgewiesenen Status. Details dazu, welcher Status (geimpft – genesen – getestet) konkret nachgewiesen wurde, waren nicht zu dokumentieren.

Zur Verfahrensvereinfachung sollten in einem von uns geprüften Fall die Beschäftigten selbst Eintragungen zu ihrem 3G-Status in Listen vornehmen. Damit erhielten sie nicht nur gegenseitig Einblick in die Eintragungen ihrer Kolleg*innen. Die Listen waren darüber hinaus auch für unbeteiligte Personen (im Haus

anwesende Dritte) frei einsehbar. Auch Führungskräfte konnten darauf zugreifen. Für die Preisgabe der sensiblen Gesundheitsdaten an Dritte gab es keine Rechtsgrundlage.

Nachdem die Unternehmensleitung Kenntnis von dem geschilderten Sachverhalt erhalten hatte, unterband sie nach unserer Beratung das unzulässige Auslegen von Listen mit 3G-Nachweisen von Beschäftigten umgehend.

Auch wenn die Pandemie allen viel abverlangt hat und der Wunsch nach unkomplizierten Verfahren verständlich ist, bleiben Gesundheitsdaten besonders sensible Daten und müssen vor der Einsicht durch Dritte geschützt werden.

8.3 Fragen nach psychologischen Behandlungen im Bewerbungsgespräch

„Sind Sie in psychologischer Behandlung?“ – Wer diese Frage in einem Vorstellungsgespräch gestellt bekommt, darf zu Recht entsetzt sein. In aller Regel verstoßen Arbeitgeber*innen damit gegen das Datenschutzrecht. So geschehen im Falle eines Personaldienstleistungsunternehmens, dessen Geschäftsführer genau dies von Bewerber*innen wissen wollte.

Das Unternehmen gab in einem Business-Netzwerk einen Einblick in die Praxis seiner Entscheidungsfindung bei Bewerbungsverfahren. Eine der Fragen im Vorstellungsgespräch war: „Warst/Bist Du in einer psychologischen Behandlung?“ Das Unternehmen versicherte, dass es ihm hierbei ausschließlich um die Ehrlichkeit der Kandidat*innen gehe. So arbeiteten im Unternehmen auch Beschäftigte, die auf diese

Frage mit „Ja“ oder „Darauf möchte ich nicht antworten“ geantwortet hätten.

Der aufgrund dieser Praxis öffentlich geäußerte Protest ließ nicht lange auf sich warten und führte dazu, dass wir auf diesen Fall aufmerksam wurden. Der Verantwortliche vertrat unter anderem die Auffassung, dass es die Pflicht von Arbeitgeber*innen sei, für die psychische Gesundheit ihrer Beschäftigten zu sorgen. Daher wolle man nur Persönlichkeiten beschäftigen, die dem psychologischen Druck der Tätigkeit gewachsen seien.

Dies allein rechtfertigt aber keine Fragen nach psychologischen Behandlungen.

Gesundheitsdaten, die Erkrankungen und deren Behandlung betreffen, unterliegen dem besonderen Schutz des Art. 9 Abs. 1 DS-GVO. Arbeitgeber*innen haben daher nur einen begrenzten Informationsanspruch. Nach § 26 Abs. 3 BDSG in Verbindung mit Art. 9 Abs. 2 DS-GVO ist eine solche Verarbeitung für Zwecke des Beschäftigungsverhältnisses nur dann zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist – und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Erlaubt ist die Nachfrage nach gesundheitlichen Beeinträchtigungen, die die Eignung für die vorgesehene Tätigkeit durch unzumutbare potenzielle Ausfallzeiten einschränken. Darüber hinaus darf zum Beispiel nach ansteckenden Krankheiten gefragt werden, die zwar keine Auswirkungen auf die individuelle

Leistungsfähigkeit der Bewerber*innen haben, jedoch andere Beschäftigte gefährden könnten.

Ob eine Person sich in psychologischer Behandlung befindet, geht jedoch weit darüber hinaus. Es wird damit pauschal die Belastbarkeit von Menschen in Frage gestellt, die in dieser Hinsicht Unterstützung in Anspruch nehmen, obwohl es unzählige Gründe dafür geben kann, die womöglich gar nicht in Zusammenhang mit der angestrebten Tätigkeit stehen. Ein zulässiges Kriterium für eine Eignungsaussage stellt die Frage keinesfalls dar.

Dagegen liegt ein tiefgreifender Eingriff in die Persönlichkeitsrechte vor. Im Vorstellungsgespräch auf dieses Thema angesprochen zu werden, erzeugt unter Umständen eine enorme Belastungssituation und kann Bewerber*innen massiv unter Druck setzen. Im ohnehin schon bestehenden strukturellen Ungleichgewicht zwischen Arbeitgeber*innen und Arbeitnehmer*innen werden Betroffene so zur Offenbarung persönlichster Angelegenheiten veranlasst. Ein solcher Eingriff in die Intimsphäre ist unverhältnismäßig und nicht gerechtfertigt.

Gegen das Unternehmen haben wir deswegen ein Bußgeldverfahren eingeleitet.

Arbeitgeber*innen haben ein Interesse daran, möglichst aussagekräftige Informationen über potenzielle Beschäftigte zu erhalten. Dies betrifft nicht nur die fachliche Qualifikation und den Lebenslauf, sondern auch persönliche Verhältnisse und eben auch den Gesundheitszustand. Hierbei sind jedoch datenschutzrechtliche Grenzen zu beachten und die Persönlichkeitsrechte der Betroffenen zu wahren.

8.4 Geldbußen für Datenschutzverstöße gegenüber juristischen Personen – uneinheitliche Rechtsprechung in Deutschland und Klärung durch den EuGH

Kann eine Geldbuße wegen eines Datenschutzverstoßes unmittelbar gegen juristische Personen festgesetzt werden, ohne dass eine vorwerfbare Handlung bestimmter Leitungspersonen vorliegt? Diese Frage wird von deutschen Gerichten unterschiedlich beantwortet. Sie liegt dem Europäischen Gerichtshof (EuGH) zur Beurteilung vor.

Nach Art. 83 DS-GVO sind Geldbußen für Datenschutzverstöße auch gegen Unternehmen zu verhängen. Der Erwägungsgrund 150 zur DS-GVO verweist in diesem Zusammenhang auf den europäisch geprägten funktionalen Unternehmensbegriff, der mit dem sog. Funktionsträgerprinzip verknüpft ist. Danach wird ein Unternehmen als wirtschaftliche Einheit verstanden und soll unmittelbar für Verstöße aller Personen haften, die im Rahmen ihres Arbeitsverhältnisses für das Unternehmen tätig werden – unabhängig von ihrer Funktion im Unternehmen.

In § 41 BDSG ist jedoch ergänzend geregelt, dass für Verstöße nach Art. 83 Abs. 4 bis 6 DS-GVO die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG) sinngemäß gelten. Dieses sieht gerade keine unmittelbare Unternehmenshaftung vor, sondern setzt das sog. Rechtsträgerprinzip um. Nach den §§ 30, 130 OWiG ist daher als sog. Anknüpfungstat eine Ordnungswidrigkeit oder Aufsichtspflichtverletzung einer Leitungsperson erforderlich, damit ein Verstoß von Unternehmensmitarbeiter*innen der jeweiligen juristischen Person zugerechnet werden kann.

Es bestehen hierzu unterschiedliche Rechtsauffassungen zu der Frage, ob bzw. unter welchen Voraussetzungen Geldbußen für Datenschutzverstöße unmittelbar gegen Unternehmen festgesetzt werden können – auch deutsche Gerichte sind sich uneins.

Nach Ansicht des Landgerichts Bonn (Urteil vom 11. November 2020, Az. 29 OWi 1/20) können Bußgelder auf Grundlage von Art. 83 DS-GVO unmittelbar gegen juristische Personen selbst verhängt werden, ohne dass ein konkreter Verstoß einer Leitungsperson festgestellt werden muss. Das europäische Recht stelle ein solches Erfordernis nicht auf – Gegenstand der Sanktionierung bei Art. 83 Abs. 4 bis 6 DS-GVO sei der Datenschutzverstoß als Erfolg und nicht die dafür ursächliche Handlung bestimmter natürlicher Personen. Ausreichend sei es daher, den Datenschutzverstoß zu individualisieren. Der europäische Gesetzgeber habe bei der DS-GVO das supranationale Kartellrecht mit einer unmittelbaren Verbandshaftung zum Vorbild gehabt. Eines der Grundanliegen bei der Schaffung der DS-GVO sei die gleichmäßige Rechtsanwendung und eine einheitliche sowie insbesondere auch effektive Sanktionierung von Datenschutzverstößen von Unternehmen gewesen. Die Anknüpfung der Geldbuße an ein Fehlverhalten von Organen oder Leitungspersonen gemäß § 30 OWiG lasse sich mit diesem Haftungskonzept und dem Funktionsträgerprinzip nicht sinnvoll in Einklang bringen. Die Anwendung von § 30 OWiG würde gegenüber dem europäischen Haftungsmodell zu einer erheblichen Einschränkung der Bußgeldverhängung gegen Unternehmen führen, wenn trotz Feststehens eines Datenschutzverstoßes die internen Verantwortlichkeiten aufzuklären wären; zudem be-

stünde die Gefahr einer europaweit deutlich unterschiedlichen Sanktionierungspraxis. Aufgrund des europarechtlichen Effektivitätsgebots dürfe auf nationale Bußgeldverfahren nur insoweit zurückgegriffen werden, als damit die effektive Durchsetzung und praktische Wirksamkeit der DS-GVO gewährleistet blieben. Nach der Auffassung des Gerichts besteht damit ein Anwendungsvorrang von Art. 83 Abs. 4 bis 6 DS-GVO gegenüber § 30 OWiG bzw. dieser ist unionsrechtskonform auszulegen, so dass die juristische Person unmittelbar selbst haftet und es nicht auf eine Anknüpfungstat einer Leitungsperson ankommt.

Demgegenüber vertritt das Landgericht Berlin (Beschluss vom 18. Februar 2021, Az. (526 OWi LG) 212 Js-OWi 1/20) die Auffassung, dass Bußgelder gegen juristische Personen nur verhängt werden können, wenn bei Leitungspersonen nach § 30 OWiG eine vorwerfbare Ordnungswidrigkeit festgestellt wird. Nach Art. 83 DS-GVO könnten Bußgelder zwar auch gegen juristische Personen verhängt werden. Juristische Personen handelten jedoch nicht selbst, sondern ihre Organe und Vertreter*innen täten dies für sie. Eine Ordnungswidrigkeit als vorwerfbare Handlung könne nur eine natürliche Person begehen; einer juristischen Person könne lediglich ein Handeln ihrer Organmitglieder oder Repräsentant*innen zugerechnet werden. Insoweit sei die Feststellung eines vorwerfbaren Verhaltens einer natürlichen Person die notwendige Grundvoraussetzung für die Begründung einer Verantwortlichkeit des möglicherweise pflichtigen Rechtsträgers. Nähere Bestimmungen zur Zurechnung enthalte die DS-GVO selbst nicht; zudem verbliebe den Mitgliedstaaten ein Ermessenspielraum bei der Ausgestaltung des Sanktionsregimes. Der deutsche Gesetzgeber habe sich mit der Regelung

des § 41 BDSG bewusst für eine Anwendbarkeit der §§ 30, 130 OWiG auf Datenschutzverstöße entschieden. Hintergrund sei insoweit auch das aus dem Grundgesetz folgende Schuldprinzip. Nach dieser Auffassung ergibt sich aus der DS-GVO keine unmittelbare Verbandshaftung bei Datenschutzverstößen, sondern es ist nach §§ 30, 130 OWiG immer eine Anknüpfungstat einer Leitungsperson notwendig. Mit einer vergleichbaren Rechtsauffassung sieht sich auch die LDI NRW beim Amtsgericht Düsseldorf konfrontiert.

Diese unterschiedlichen Anforderungen für Bußgeldverfahren gegenüber juristischen Personen haben Auswirkung auf die Effektivität der Bußgeldverfahren. Denn soweit trotz des Feststehens eines Datenschutzverstoßes die internen Verantwortlichkeiten von der Datenschutzaufsicht als Bußgeldbehörde aufzuklären sind, erfordert dies teils erheblichen Aufwand und mitunter kann eine Anknüpfungstat von Leitungspersonen auch gar nicht nachgewiesen werden. Insoweit können faktisch auch Benachteiligungen von Unternehmen entstehen, da ein solcher Nachweis umso schwieriger sein kann, je komplexer die Unternehmensstrukturen sich gestalten; weiterhin besteht diese Anforderung aus einer nationalen Regelung nicht einheitlich in allen Mitgliedstaaten und auch nicht einheitlich in der Rechtspraxis der Gerichte in Deutschland.

Der Fall des Landgerichts Berlin ging in die nächste Instanz; dort hat das Kammergericht Berlin (Beschluss vom 6. Dezember 2021, Az. 3 Ws 250/21) das Verfahren ausgesetzt und dem EuGH die Streitfrage zur Vorabentscheidung vorgelegt, da diese die Auslegung des Unionsrechts betrifft. Der EuGH wird

daher zu entscheiden haben, ob mit Art. 83 Abs. 4 bis 6 DS-GVO der funktionale Unternehmensbegriff und das Funktionsträgerprinzip derart festgelegt werden, dass trotz einer nationalen Regelung wie § 30 OWiG ein Bußgeldverfahren wegen eines Datenschutzverstoßes unmittelbar gegen ein Unternehmen geführt werden kann, ohne dass es der Feststellung einer Ordnungswidrigkeit durch eine bestimmte natürliche Leitungsperson bedarf.

Es ist umstritten, ob bei Datenschutzverstößen für Geldbußen gegenüber juristischen Personen das Rechtsträgerprinzip des deutschen Ordnungswidrigkeitenrechts oder das europäisch geprägte Funktionsträgerprinzip gilt. Die Befassung des EUGH mit den vorgelegten Fragen bringt hoffentlich die Rechtssicherheit, die eine einheitliche Anwendung des Art. 83 DS-GVO in Deutschland und Europa gewährleistet.

8.5 Keine Veröffentlichung von Privatadressen von Beschäftigten im Amtsblatt

Die Veröffentlichung von personenbezogenen Daten von im öffentlichen Dienst Beschäftigten ist immer wieder ein Thema, wenn der Dienstausweis verloren wurde. Die Dienststellen müssen dabei die Privatsphäre ihrer Beschäftigten schützen.

Ein Beschäftigter hat seiner Dienststelle den Verlust seines Dienstausweises gemeldet. In diesem Ausweis sind Name, Vorname und Geburtsdatum die einzigen personenbezogenen Daten, die neben einem Passfoto zum Zweck der eindeutigen Identifikation als Mitarbeiter der Behörde vermerkt sind. In der späteren Veröffentlichung der Ungültigkeitserklärung des

Ausweises im Amtsblatt für den Regierungsbezirk wurde allerdings neben diesen Daten auch die Privatanschrift des Beschäftigten aufgeführt. Das Amtsblatt ist im Internet veröffentlicht und damit für jede Person zugänglich. Informationen, die einmal ins Internet gestellt worden sind, können danach kaum mehr kontrolliert werden.

Die Veröffentlichung der Privatanschrift im Rahmen einer Ungültigkeitserklärung ist unzulässig. Personenbezogene Daten von Beschäftigten dürfen nur in einem eng begrenzten Umfang verarbeitet werden (§ 18 DSG NRW). Eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, wenn Empfänger*innen ein rechtliches Interesse darlegen, der Dienstverkehr es erfordert oder die betroffene Person eingewilligt hat. Die Veröffentlichung einer Ungültigkeitserklärung ist zwar zur Klarstellung für den Dienstverkehr erforderlich. Nicht erforderlich ist hingegen die Angabe der Privatanschrift der Person, die den Dienstausweis verloren hat, da sie zur Identifizierung des verlorenen Dienstausweises nicht benötigt wird. Der Dienstausweis weist insoweit richtigerweise lediglich den Vor- und Nachnamen, das Geburtsdatum und die Dienstbezeichnung aus ohne eine Privatadresse zu nennen. Das ist auch deswegen bedeutsam, weil viele Beschäftigte im öffentlichen Dienst, die im direkten Kontakt mit Bürger*innen stehen, zunehmend angefeindet werden und in Einzelfällen sogar konkret gefährdet sind. In diesen Fällen würde die Dienststelle die Gefahrenlage durch Veröffentlichung der Privatadresse verschärfen.

Die Behörde hat nach Aufgreifen der Beschwerde durch die LDI NRW die Ungültigkeitserklärung durch

Schwärzung der Privatanschrift und des Nachnamens korrigiert.

Bei der Veröffentlichung von Beschäftigtendaten ist darauf zu achten, dass lediglich solche personenbezogenen Daten genannt werden, die zur Erreichung des Zwecks der Veröffentlichung unbedingt erforderlich sind.

9. Wirtschaft

9.1 Bonitätsabfragen bei Wirtschaftsauskunfteien – Überprüfung des berechtigten Interesses

Sowohl anlassbezogen als auch anlasslos prüfen wir den Umgang mit Bonitätsanfragen durch die in NRW ansässigen Wirtschaftsauskunfteien. Bei allen Bonitätsabfragen muss ein berechtigtes Interesse der abfragenden Stelle vorliegen. Abfragen ohne berechtigtes Interesse können auch ein Bußgeld nach sich ziehen.

Wer eine Bonitätsabfrage über eine Person bei einer Wirtschaftsauskunftei einholt, braucht hierfür nach Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO ein berechtigtes Interesse. Ein solches ist zum Beispiel dann gegeben, wenn im Rahmen von Vertragsbeziehungen – wie einem Kauf auf Rechnung oder einer Ratenzahlungsvereinbarung – ein finanzielles Ausfallrisiko für die abfragende Stelle besteht.

Da Bonitätsauskünfte im Wirtschaftsverkehr massenweise abgefragt werden, sind standardisierte Verfahren mit Fallgruppen zu Ausfallrisiken üblich. Nach dem BDSG a. F., also der Fassung noch vor Geltung der DS-GVO, waren Wirtschaftsauskunfteien nach § 29 Abs. 2 Satz 5 in Verbindung mit § 10 Abs. 4 Satz 3 dazu verpflichtet, regelmäßige Stichprobenkontrollen zum Vorliegen eines berechtigten Interesses bei ihren Vertragspartner*innen – den abfragenden Stellen – durchzuführen. Auch im Rahmen der DS-GVO werden diese Stichprobenüberprüfungen durch die Wirtschaftsauskunfteien weitergeführt, um Missbrauch zu verhindern.

Im vergangenen Jahr haben wir den Umgang mit diesen Stichprobenkontrollen bei einer großen Wirtschaftsauskunftei für den Zeitraum der letzten drei Jahre überprüft. Diese Überprüfung hat Folgendes ergeben: Es wurden in ausreichendem Maße Stichproben gezogen. Diese Stichproben setzten sich zusammen sowohl aus Fällen, bei denen eine entsprechende Beschwerde beim Unternehmen einging, als auch aus Fällen, die nach dem Zufallsprinzip ausgewählt wurden. Im Verhältnis musste nur in wenigen Fällen festgestellt werden, dass ein berechtigtes Interesse nicht vorgelegen hatte.

Die Auskunftei ist gehalten, in diesen Fällen auf die abfragende Stelle zuzugehen, um die datenschutzrechtlichen Aspekte zu erörtern und auf vertragsrechtliche Sanktionen hinzuweisen, die bei einem erneuten Abruf ohne berechtigtes Interesse zum Ausschluss vom Abrufverfahren führen. Zudem konnten wir erreichen, dass Unternehmen nun durch verstärkte Hinweise im Abrufverfahren vor unberechtigten Abfragen gewarnt werden.

Unabhängig hiervon überprüfen wir das Vorliegen eines berechtigten Interesses bei Bonitätsabfragen regelmäßig auch im Rahmen konkreter Beschwerdefälle. Je nach Fallgestaltung kann eine missbräuchliche Abfrage einer Bonitätsauskunft für die abfragende Stelle oder Person auch zu der Verhängung eines Bußgeldes führen.

9.2 Prüfaktion zu Datenschutzbeauftragten bei Detekteien

Das Betätigungsfeld von Detekteien kann auch Observationen und andere Überwachungstätigkeiten umfassen. Detekteien, die diese Tätigkeiten umfangreich ausüben, benötigen unabhängig von der Anzahl ihrer Beschäftigten Datenschutzbeauftragte. Dazu haben wir eine Stichprobenprüfung durchgeführt.

Ob Philip Marlowe oder Georg Wilsberg – zu den klassischen Aufgaben des Detektivberufs gehören die Recherche und das Zusammentragen von Informationen. Das weiß doch jeder! Was nicht jeder weiß: Sofern auch Observationen oder andere Überwachungstätigkeiten durchgeführt werden, kann dies die Pflicht zur Benennung von Datenschutzbeauftragten auslösen. Abhängig ist das vom Umfang solcher Datenverarbeitungen.

Nach Art. 37 Abs. 1 Buchstabe b DS-GVO benennen Verantwortliche und Auftragsverarbeiter auf jeden Fall Datenschutzbeauftragte, wenn die Kerntätigkeit in einer Datenverarbeitung besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich macht.

Eine umfangreiche und regelmäßige Überwachungstätigkeit führt also zur Pflicht, eine*n Datenschutzbeauftragte*n zu benennen – und zwar unabhängig davon, ob es sich bei der Detektei um ein Ein-Personen-Unternehmen oder um ein größeres Unternehmen handelt. Darüber hinaus greift bei entsprechend großen Unternehmen die Regelung nach § 38

BDSG, wonach Stellen bei einer Anzahl von mindestens 20 Personen, die in der Regel ständig automatisiert personenbezogene Daten verarbeiten, ebenfalls Datenschutzbeauftragte benennen müssen.

Die bisherigen Ergebnisse der Prüfung lassen erkennen, dass manche Detekteien unsicher sind, ob und ab welcher Häufigkeit und Intensität der Observationen regelmäßig von einer umfangreichen Überwachung auszugehen ist, die eine Benennungspflicht begründet. Wir gehen von einer umfangreichen, regelmäßigen und systematischen Überwachung im Rahmen der Kerntätigkeit dann aus, wenn Observationen von Personen öfter als in einer niedrigen einstelligen Anzahl pro Jahr durchgeführt werden. Hierbei ist ebenso die Dauer einzelner Observationen (etwa Dauerbeobachtungen) zu berücksichtigen.

Wir beraten Detekteien, die noch keine*n Datenschutzbeauftragte*n benannt haben, und wir setzen durch, dass sie ihre Pflicht erfüllen. Das gilt auch, falls die Kontaktinformationen der Datenschutzbeauftragten noch nicht veröffentlicht oder uns als Aufsichtsbehörde noch nicht mitgeteilt sind.

Es gibt auch Detekteien, die ihre Kerntätigkeit so ausgerichtet haben, dass sie keine regelmäßige und systematische Überwachung erfordert. Dann gibt es insoweit auch keine Pflicht, zur Benennung von Datenschutzbeauftragten. Das ist zum Beispiel so bei Detekteien, die sich auf die Recherche von Wirtschaftsinformationen oder Urheberrechtsverstößen oder auf den Objektschutz spezialisieren und dafür keine Observationen oder andere Überwachungen von Personen durchführen.

Und natürlich haben wir bei unserer Stichprobenprüfung auch Detekteien gefunden, die schon seit vielen Jahren ordnungsgemäß Datenschutzbeauftragte bestellt sowie die Kontaktdaten veröffentlicht und uns gemeldet haben. Auch den rechtstreuen Verantwortlichen wollen wir mit unseren Stichproben zeigen, dass wir bei der Konkurrenz nach dem Rechten schauen.

Wir beraten und unterstützen Detekteien weiterhin bei der Umsetzung der Pflichten aus der DS-GVO.

Soweit Detekteien regelmäßig Observationen oder andere Überwachungstätigkeiten durchführen, bei denen gezielt und systematisch Personen beobachtet werden, ist von einer umfangreichen Überwachung Betroffener auszugehen, die eine Benennung von Datenschutzbeauftragten erforderlich macht. Die Landesbeauftragte unterstützt die Verantwortlichen bei der Umsetzung der Benennungspflicht.

9.3 Zertifizierung: DSK-Papier zu den Anforderungen überarbeitet

Die neue Version des Papiers „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ bringt mehr Rechtssicherheit und Transparenz für die Erstellung von Zertifizierungsprogrammen.

Art. 42 und 43 DS-GVO legen die Grundsteine für einheitliche europäische Zertifizierungs- und Akkreditierungsverfahren.

Zertifikate bedeuten für alle, deren Daten verarbeitet werden, mehr Transparenz. Sie ermöglichen betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger Produkte und Dienstleistungen. Damit einhergehend wird die klare

Botschaft formuliert, dass die zertifizierte Datenverarbeitung die Regeln der DS-GVO grundsätzlich einhält. Zertifizierung schafft Vertrauen. Eine erfolgreiche Zertifizierung als solche garantiert zwar nicht die Einhaltung der DS-GVO bei jeder einzelnen Datenverarbeitung, sie attestiert aber, dass der zertifizierte Prozess grundsätzlich datenschutzgerecht angelegt ist. Durch die regelmäßig stattfindenden Audits werden die Prozesse, die im Zertifikat benannt sind, überprüft und optimiert.

Um als Zertifizierungsstelle nach der DS-GVO tätig werden zu können, muss sich eine Stelle zunächst für diese Tätigkeit akkreditieren lassen. Für diese Akkreditierung muss eine Prüfung durchlaufen werden, die in mehreren Schritten stattfindet. Die Deutsche Akkreditierungsstelle und die jeweils zuständige Aufsichtsbehörde arbeiten dabei zusammen.

Zu den ersten Schritten gehört die Fachprüfung des Konformitätsbewertungsprogramms und der entsprechenden Zertifizierungskriterien durch die zuständige Aufsichtsbehörde anhand der ISO/IEC 17065 und der ergänzenden Anforderungen. Erfolgreich abgeschlossen wird die Fachprüfung der Aufsichtsbehörde mit der Genehmigung der Zertifizierungskriterien.

Die deutschen Aufsichtsbehörden, die sich in der DSK abstimmen, haben einheitliche Anforderungen an Zertifizierungskriterien aufgestellt. Programmeigner sowie die zu akkreditierenden Zertifizierungsstellen können sich schon bei der Erstellung ihrer Dokumente hieran orientieren. Das Papier ist überarbeitet und in der Version 2.0 veröffentlicht, um aktuelle Erfahrungen und Erkenntnisse der Aufsichtsbehörden sowie Rückmeldungen der Antragstellenden zu be-

rücksichtigen. Das Papier enthält nun konkretere Informationen zu den Anforderungen bei Drittlandtransfers und zur gemeinsamen Verantwortlichkeit. Die Anforderungen für die Auftragsverarbeitung sind überarbeitet. In einer Grafik wird außerdem der Prozess auf europäischer Ebene dargestellt.

Die LDI NRW hat bereits nationale Zertifizierungskriterien nach einer Stellungnahme durch den EDSA genehmigt. Sie ist die erste deutsche Datenschutzaufsichtsbehörde, die eine solche Genehmigung erteilt hat. Weitere Anträge liegen vor. Voraussichtlich werden in 2023 erste Zertifizierungsstellen in Deutschland datenschutzrechtliche Zertifizierungen nach der DSG-VO anbieten können.

Das Papier „Anforderungen an datenschutzrechtliche Zertifizierungsprogramme“ ist in der Version 2.0 eine weiter verbesserte Praxishilfe bei der Erstellung eines Zertifizierungsprogramms und zeigt Interessierten, worauf es bei der aufsichtsbehördlichen Überprüfung ankommt.

9.4 LDI NRW akkreditiert erste Überwachungsstelle für Verhaltensregeln in Deutschland

Im September 2022 wurde die Überwachungsstelle für die Verhaltensregeln zu den Prüf- und Löschfristen von Wirtschaftsauskunfteien akkreditiert. Viereinhalb Jahre nach Inkrafttreten der DS-GVO kommt es damit zu einer deutschlandweiten Premiere.

Die TIGGES DCO GmbH wurde als erste Überwachungsstelle in Deutschland akkreditiert, also genehmigt. Sie überwacht die Einhaltung der Verhaltensregeln der Wirtschaftsauskunfteien. Diese

Verhaltensregeln legen fest, innerhalb welcher Fristen die Speicherung personenbezogener Daten durch Wirtschaftsauskunfteien geprüft und gelöscht werden sollen. Die Überwachungsstelle hat im September 2022 ihre Arbeit aufgenommen und unterhält unter https://auskunfteien.beschwerdestelle-tigges-dco.de/ ein Beschwerdeportal, an das sich Bürger*innen wenden können.

Warum ist das so wichtig? Die Überwachungsstelle der Wirtschaftsauskunfteien ist eine zentrale unabhängige Anlaufstelle für alle Bürger*innen, die Fragen zur Speicherdauer ihrer personenbezogenen Daten durch eine Auskunftei haben. Die Stelle soll gegenüber den Auskunfteien darauf hinwirken, dass berechtigte Löschansprüche umgesetzt werden.

Die Überwachungsstelle überprüft ausschließlich die Einhaltung der Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien, vgl. Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien vom 25.05.2018 (in der Fassung vom 01.01.2020), abrufbar unter www.ldi.nrw.de.

Beschwerden über andere datenschutzrechtliche Fragen rund um Auskunfteien, werden von der Stelle nicht bearbeitet.

Verhaltensregeln, meist auch „Codes of Conduct“ (CoC) genannt, dienen im Wirtschaftsleben als verbindliche Vorgaben innerhalb einer Branche und sind damit ein wichtiger Faktor im Rahmen der Selbstregulierung. Weitere Information über Verhaltensregelungen und Akkreditierung von Überwachungsstellen: sind unter www.ldi.nrw.de abrufbar. Die LDI NRW

hatte die Verhaltensregeln für die Prüf- und Löschfristen der deutschen Wirtschaftsauskunfteien bereits 2018 genehmigt. Sie konkretisieren die allgemeinen Löschpflichten des Art. 17 DS-GVO in Bezug auf die von Auskunfteien gesammelten Daten.

Auskunfteien sammeln Daten zur finanziellen Leistungsfähigkeit von Privatpersonen und werten diese aus, um zum Beispiel vorherzusagen, ob Kund*innen ihre Rechnungen zahlen werden. Die bekannteste Auskunftei ist die Schufa (in Hessen). Daneben gibt es weitere Auskunfteien, darunter Crif Bürgel (in Bayern), Creditreform Boniversum (in NRW) und Arvato Infoscore (in Baden-Württemberg).

Die Auskunfteien geben die gesammelten und ausgewerteten Daten als Bonitätsinformationen an ihre Auftraggeber*innen weiter – jedoch nur bei einem bestätigten berechtigten Interesse. Ein berechtigtes Interesse liegt zum Beispiel vor, wenn Miet- und Kaufverträge – vor allem im Online-Handel – oder andere Verträge abgeschlossen werden, bei denen Zahlungsausfallrisiken für Unternehmen bestehen. Auskunfteien haben also einen erheblichen Einfluss darauf, in welchem Umfang Bürger*innen am Wirtschaftsleben teilnehmen können, und dienen der wirtschaftlichen Absicherung von Unternehmen.

Aus Sicht der Bürger*innen ist es wichtig, dass die über sie bei den Auskunfteien gespeicherten Daten regelmäßig auf ihre Richtigkeit geprüft und Informationen über negative Zahlungserfahrungen gelöscht werden, wenn sie keine belastbare Aussagekraft mehr für die Bonität haben.

Die nun von der LDI NRW akkreditierte Überwachungsstelle kann eine Klärung nicht nur für eine,

sondern für alle an den Verhaltensregeln beteiligten Auskunfteien herbeiführen. Die staatlichen Datenschutzaufsichtsbehörden sind daneben weiterhin zuständig, sowohl für die Datenschutzaufsicht über Auskunfteien als auch für die Überwachungsstelle.

Die Akkreditierung der Überwachungsstelle für Verhaltensregeln der Wirtschaftsauskunfteien ist ein Pilotprojekt für alle Beteiligen gewesen. Es wäre wünschenswert, dass in Zukunft auch in anderen Branchen weitere Verhaltensregeln und Akkreditierungen folgen.

9.5 Adresshandel zum Zwecke der Werbung nach der DS-GVO

Werbung von Unternehmen im Briefkasten – und die Empfänger*innen wundern sich, weil sie nie eine Geschäftsbeziehung zu dem Unternehmen hatten. Weit verbreitet ist, dass Unternehmen für ihre Werbung Adressdienstleister*innen nach ihren Vorgaben damit beauftragen, Adressdaten für die Werbung zur Verfügung zu stellen. Diese Form der Verarbeitung personenbezogener Daten wird auch als „Adresshandel“ bezeichnet.

Beim Adresshandel ist das „Lettershop-Verfahren“ eine übliche Praxis. Dabei bezieht ein Lettershop (zum Beispiel eine Druckerei) Blanko-Werbesendungen vom werbenden Unternehmen und Adressdaten von Adresshändler*innen. Der Lettershop versendet die Werbung, ohne dass das werbende Unternehmen Kenntnis von den Adressen erhält. Das reduziert den Eingriff in die schutzwürdigen Interessen der betroffenen Person, weil die Daten nur bei einer Stelle liegen

und nicht an einen größeren Kreis von Empfänger*innen zur eigenen Nutzung übermittelt werden. Durch festgelegte Auswahlkriterien (Zahl der Adressdaten, Stadt oder Region, Geschlecht, Altersgruppe, ggf. weitere bekannte Merkmale, zum Beispiel die Haushaltsgröße) sollen im Idealfall nur Personen angesprochen werden, für die die beworbenen Produkte oder Dienstleistungen potenziell interessant sind. Teilweise sind zwischen werbendem Unternehmen und Adresshändler*in noch sog. Listbroker*innen geschaltet, die das gewünschte Adressportfolio vermitteln.

Wie ist das zu bewerten? Der Umgang mit Adress- und ggf. weiteren Daten für Werbezwecke stellt eine Verarbeitung personenbezogener Daten dar. Wie jede andere personenbezogene Datenverarbeitung ist diese nur zulässig, wenn dafür eine Rechtsgrundlage besteht (Art. 5 Abs. 1 Buchstabe a, Art. 6 Abs. 1 DS-GVO). Dies kann beispielsweise eine Einwilligung gemäß Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a DS-GVO sein, die entsprechend nachzuweisen ist.

Die DS-GVO lässt aber auch das Verarbeiten personenbezogener Daten bei Erforderlichkeit und überwiegendem berechtigten Interesse des Verantwortlichen zu (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO). Dies kann auch für Werbung und Adresshandel gelten. Die Erläuterungen zur DS-GVO stellen im Erwägungsgrund 47 Satz 7 klar, dass Direktwerbung als ein berechtigtes Interesse im Sinne von Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO betrachtet werden kann. Adresshandel ist in einer durch Industrie und Dienstleistung geprägten freien Marktwirtschaft ein grundsätzlich zulässiges Geschäftsfeld, um die für postalische Werbung benötigten Adressen zu

generieren, und steht daher mit Direktwerbung in einem engen sachlichen Zusammenhang. Für die Verarbeitung von personenbezogenen Daten zum Zwecke des Adresshandels besteht das berechtigte Interesse der werbenden Unternehmen, ihre Waren und Dienstleistungen möglichst zielgerichtet anbieten zu können. Adresshändler*innen haben wiederum das berechtigte Interesse, ihre Datensätze zu diesem Zweck zur Verfügung zu stellen. Insoweit ist von einer Erforderlichkeit der Datenverarbeitung auszugehen.

Empfänger*innen der Postwerbung haben andererseits möglicherweise das Interesse, keine unbestellte Werbung zu erhalten. Im Rahmen einer Abwägung ist dann zu prüfen, ob die berechtigten Interessen der werbenden Unternehmen und Adresshändler*innen die schutzwürdigen Interessen der Empfänger*innen überwiegen. Dabei sind auch deren vernünftige Erwartungen zu berücksichtigen, die sich unter anderem daraus ableiten lassen,

- in welcher Beziehung die betroffenen Personen und die Verantwortlichen zueinanderstehen und
- ob die Daten aus öffentlich zugänglichen Quellen stammen, oder
- ob die Daten auf sonstige Weise genutzt werden dürfen, zum Beispiel indem die Person ihre Daten im Rahmen von Preisausschreiben auch für Werbezwecke zur Verfügung gestellt hat.

Bei personenbezogenen Daten, welche die betroffene Person offensichtlich selbst öffentlich gemacht hat, überwiegen grundsätzlich die berechtigten Interessen der Unternehmen. Hier gilt: Bei öffentlich gemachten personenbezogenen Daten besteht eine tendenziell geringere Schutzbedürftigkeit. Die LDI NRW orientiert

sich an § 28 Abs. 3 BDSG a. F., wonach – kurz gesagt – in öffentlichen Registern (etwa Adress-, Rufnummern-, Branchenverzeichnisse) zusammengefasste personenbezogene Daten (zum Beispiel Name, Berufs- oder Geschäftsbezeichnung, Anschrift) über Angehörige einer Personengruppe grundsätzlich für Werbezwecke verwandt werden durften (ausgenommen Pflichtveröffentlichungen wie zum Beispiel Impressumsangaben auf Internetseiten). Mit dieser Vorschrift hatten die damals zuständigen Gesetzgebungsorgane die widerstreitenden Interessen von Unternehmen an der werbenden Tätigkeit und Verbraucher*innen am Schutz vor ungewollter Werbung durch eine gesetzliche Festlegung austariert. Wir gehen davon aus, dass diese damalige gesetzliche Wertung auch unter der Geltung der DS-GVO weiterhin eine sachgerechte Interessenabwägung darstellt.

Die DS-GVO enthält keine explizite Regelung zur Verarbeitung von Adressdaten, sie widerspricht der von uns vorgenommenen Wertung aber auch nicht. Das überwiegende berechtigte Interesse des datenverarbeitenden Unternehmens (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO) ist eine gleichrangige Rechtsgrundlage für eine Datenverarbeitung wie die Einwilligung (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a DS-GVO). Nicht wenige Menschen gehen davon aus, dass für die Verarbeitung ihrer personenbezogenen Daten eine Einwilligung erforderlich ist. Diese Annahme trifft aber oft nicht zu. Unsere Interessenabwägung nach Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO bezüglich der Nutzung von Adressdaten für Werbung und Adresshandel teilen allerdings – dies soll nicht verschwiegen werden – andere Datenschutzaufsichtsbehörden in Deutschland nicht. Diese

halten in diesem Fall die Einwilligung für die einzig tragfähige Grundlage der Datenverarbeitung. Im EDSA wird an Empfehlungen für das Direktmarketing gearbeitet. Dies wird hoffentlich eine einheitliche Sicht aller Datenschutzaufsichtsbehörden auf diese Frage befördern.

Wer keine Werbung haben möchte, hat – ungeachtet dieser unterschiedlichen Rechtsauffassungen – jederzeit das Recht, der Verarbeitung seiner personenbezogenen Daten zu Werbezwecken zu widersprechen (Art. 21 Abs. 2 DS-GVO) bzw. eine erteilte Einwilligung zu widerrufen (Art. 7 Abs. 3 DS-GVO). Werbewidersprüche können sowohl bei Adresshändler*innen als auch bei dem werbenden Unternehmen geltend gemacht werden. Ein interner Sperrvermerk führt dann dazu, dass das Unternehmen bzw. die Adresshändler*innen keine Werbung mehr an die hinterlegte Adresse versenden werden. Das ist sinnvoll, um zu verhindern, dass bei zukünftigen Werbeaktionen die betroffene Person Werbung erhält, wenn deren Adresse wieder in den Adressbestand der oder des Verantwortlichen gelangt ist. Sofern die betroffene Person es verlangt, sind ihre Daten nach Art. 17 Abs. 1 Buchstabe c DS-GVO zu löschen.

Tipp: Ein Widerspruch nach Art. 21 Abs. 2 DS-GVO sollte schriftlich (möglichst auf dem Postweg) an die Unternehmen gerichtet und in jedem Fall die schriftliche Bestätigung verlangt werden. Alternativ oder zusätzlich können betroffene Personen die Eintragung in eine der sog. Robinsonlisten vornehmen, um möglichst keine unerwünschte Werbung mehr zu erhalten. In Deutschland gibt es Robinsonlisten, unter anderem des Deutschen Dialogmarketing Verbandes e. V.

(DDV) und des Interessenverbandes Deutsches Internet e. V. (I.D.I.). Einzelheiten zu den Robinsonlisten siehe unter www.ichhabediewahl.de und www.robinsonliste.de.

Darüber hinaus gibt es nach Art. 13 und 14 DS-GVO Pflichten der datenschutzrechtlich Verantwortlichen, betroffenen Personen bestimmte Informationen im Zusammenhang mit der Verarbeitung ihrer Daten mitzuteilen bzw. bereitzustellen sowie – sofern hierfür die Voraussetzungen vorliegen – das Recht auf Löschung personenbezogener Daten nach Art. 17 DS-GVO.

Auf Folgendes sei noch ergänzend hingewiesen:

Nach den Erfahrungen der LDI NRW mit Beschwerden lässt sich feststellen, dass postalische Werbung im Allgemeinen als weniger beeinträchtigend angesehen wird, insbesondere im Vergleich zur Telefon- oder E-Mailwerbung, wofür besondere Regelungen gelten (§ 7 Gesetz gegen den unlauteren Wettbewerb – UWG).

Werden Adressdaten mit weiteren personenbezogenen Kontaktinformationen angereichert, namentlich mit Telefonnummern oder E-Mail-Adressen, ist für die Anreicherung und werbliche Nutzung solcher Zusatzinformationen § 7 UWG zu beachten.

Nach § 7 Abs. 1 UWG sind Werbung per Telefon oder E-Mail gegenüber Verbraucher*innen grundsätzlich nur mit vorheriger ausdrücklicher Einwilligung der Betroffenen zulässig – ansonsten handelt es sich um eine unzumutbare Belästigung. Das bedeutet, dass

die Anreicherung und werbliche Nutzung der Zusatzinformationen nur bei Vorliegen einer Einwilligung zulässig ist.

Der Handel mit öffentlich gemachten Adressen stellt nach unserer Auffassung ein berechtigtes Interesse dar, um Direktwerbung zu ermöglichen. Betroffene haben allerdings die Möglichkeit, unerwünschter Werbung zu widersprechen. Ein solcher Widerspruch kann gegen Adresshändler*innen und/oder werbende Unternehmen gerichtet werden. Darüber hinaus gibt es Informations- und Löschungspflichten. Betroffene können sich außerdem in eine sog. Robinsonliste eintragen.

9.6 Datenverkehr in vernetzten Autos

Autos fahren mit immer mehr technischer Unterstützung. Und immer mehr Technik in den Autos sammelt Daten. Kraftfahrzeugbesitzer*innen sind oft unsicher, ob und welche Daten über sie von dem Hersteller des Fahrzeugs verarbeitet werden.

Ein in NRW ansässiger Autohersteller setzt in fast allen aktuellen Fahrzeugmodellen eine Vernetzungstechnologie ein. Ab Werk sind sie dafür mit einem verbauten Mobilfunkmodem und SIM-Karte ausgestattet. Die Nutzer*innen werden darüber in der Datenschutzerklärung der Fahrzeug-App und im Benutzerhandbuch ihres Fahrzeuges informiert. Die Daten werden in diesem Fall nur ausgelesen und an den Hersteller übermittelt, wenn Nutzer*innen oder Händler*innen entsprechende Einstellungen im Infotainment-System des Fahrzeugs vorgenommen haben.

Regelmäßig sind die von einem vernetzten Fahrzeug an den Hersteller übermittelten Informationen personenbeziehbare Daten der Nutzer*innen. Der Personenbezug lässt sich über die jedem Fahrzeug zugeordnete Fahrzeug-Identifizierungsnummer (FIN) herstellen. Diese Daten, die aufgrund der Fahrzeugnutzung entstehen, gehören den Fahrzeugnutzer*innen und können grundsätzlich nur mit deren Einwilligung übermittelt werden. Diese wird entweder beim Kauf explizit erteilt – und kann jederzeit widerrufen werden. Oder aber die Nutzer*innen willigen durch eigenes aktives Tun ein, indem sie etwa entsprechende Einstellungen im Fahrzeug vornehmen. Diese können die Nutzer*innen über das Infotainment-System im Fahrzeug jederzeit eigenständig neu konfigurieren und die Vernetzung so selbst in einem bestimmten Umfang deaktivieren.

Zu berücksichtigen ist jedoch, dass nicht alle technischen Voreinstellungen deaktiviert werden können. Es gibt auch solche, die für die Funktionalität des Kraftfahrzeugs und seine Assistenzsysteme unverzichtbar sind. Sonst würde die Verkehrssicherheit leiden. Diese sind voreingestellt und führen zu Datenübermittlungen, die auf einer gesetzlichen Grundlage erlaubt sind. Diese müssen den Kund*innen transparent gemacht werden. Daneben gibt es aber einen optionalen Teil von Datenflüssen, der (de)aktiviert werden kann. Auch hierüber müssen Händler*innen – mit Hilfe der Hersteller – aufklären. Je autonomer ein Kraftfahrzeug fahren wird, desto größer wird der notwendige Datenfluss sein. Ob und wann eine Datenübertragung stattfindet, zeigen entsprechende Symbole auf dem Display im Fahrzeug an.

Beim Kauf eines vernetzten Fahrzeuges gehört es zu den vertraglichen Pflichten der Händler*innen zu erklären, wie die Vernetzung funktioniert welche Voreinstellungen vorgenommen wurden und wie die Käufer*innen die Vernetzung eigenhändig verändern können. Insofern sind die Händler*innen auch die ersten Ansprechpartner*innen für diese Fragen. Beantworten müssen sie auch die Frage, ob bzw. in welche Datenverarbeitungen mit dem Kauf bereits einwilligt wird, was auch genau von den Händler*innen dokumentiert werden muss. Diese Dokumentation ist den Käufer*innen – und natürlich bei Nachfrage auch der zuständigen Datenschutzaufsicht – auszuhändigen.

Dass die Fahrzeugnutzer*innen über die von ihnen verursachten Daten die Hoheit haben sollen, entspricht den im Jahr 2016 aufgestellten Grundsätzen der Gemeinsamen Erklärung der DSK und des Verbandes der Automobilindustrie zu den „datenschutzrechtlichen Aspekten bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge“, aufzurufen auf unserer Homepage unter www.ldi.nrw.de/datenschutz/wirtschaft/datenschutz-im-auto.

Personenbezogene Daten aus vernetzten Fahrzeugen dürfen an die Hersteller nur bei vorheriger Einwilligung gesendet werden. Die Nutzer*innen sollten die Vernetzungseinstellungen ihres Fahrzeugs darauf hin prüfen und ihren Wünschen entsprechend ändern.

9.7 DSK positioniert sich zum Gastzugang im Online-Handel

Die deutschen Datenschutzaufsichtsbehörden fordern in einem Beschluss vom 24. März 2022, dass bei der Online-Bestellung auch ein Gastzugang, also die Bestellung ohne dauerhaftes Kund*innenkonto, möglich sein muss. Kund*innenkonten mittels verpflichtender Registrierung waren lange Zeit gängige Praxis im Online-Handel. Die Forderung der DSK hat in Fachkreisen deshalb für reichlich Diskussion gesorgt.

Die Datenschutzaufsichtsbehörden haben sich in ihrer täglichen Eingabepraxis vielfach mit der Frage auseinanderzusetzen, unter welchen Voraussetzungen bei Bestellungen im Online-Handel Gastzugänge einzurichten sind. Kund*innen müssen nach Auffassung der Aufsichtsbehörden frei entscheiden können, ob sie ihre Daten nur einmalig und für mögliche weitere Bestellungen erneut eingeben und insofern als sog. temporärer Gast geführt werden möchten oder ob sie bereit sind, eine dauerhafte Geschäftsbeziehung einzugehen, die mit Registrierungs- bzw. Zugangsdaten für ein fortlaufendes Kund*innenkonto verbunden ist.

Die eindeutige Positionierung der Datenschutzaufsichtsbehörden sorgt nun für Klarheit in der Aufsichtspraxis. Damit wird verhindert, dass Online-Shops ohne Wissen und Wollen ihrer Kund*innen die Warenkörbe früherer Einkäufe für Werbezwecke nutzen. Der Beschluss der DSK „Datenschutzkonformer Online-Handel mittels Gastzugang“ vom 24. März 2022 ist im Anhang abgedruckt.

Die vier Kernaussagen des DSK-Beschlusses lauten wie folgt:

1. Verantwortliche, die Waren oder Dienstleistungen im Onlinehandel anbieten, müssen ihren Kund*innen unabhängig davon, ob sie ihnen daneben einen registrierten Nutzungszugang (fortlaufendes Kund*innenkonto) zur Verfügung stellen, grundsätzlich einen Gastzugang (Online-Geschäft ohne Anlegen eines fortlaufenden Kund*innenkontos) für die Bestellung bereitstellen.
2. Ohne einen Gastzugang bzw. ohne eine gleichwertige Bestellmöglichkeit kann die Freiwilligkeit einer Einwilligung in ein fortlaufendes Kund*innenkonto nicht gewährleistet werden.
3. Die mit einem fortlaufenden Kund*innenkonto verbundenen Möglichkeiten der Auswertung und Verarbeitung der Vertragshistorie für Werbezwecke bedürfen einer darauf bezogenen informierten Einwilligungserklärung. Diese ist nicht bereits durch die Einwilligung zur Einrichtung und Führung des fortlaufenden Kund*innenkontos abgedeckt. Kund*innen, die ein fortlaufendes Konto ablehnen, geben damit auch zu erkennen, dass sie eine Werbeansprache ablehnen.
4. Die von den Verantwortlichen verarbeiteten Daten müssen in einer für die Kund*innen transparenten Weise verarbeitet werden.

Bei Bestellungen im Online-Handel ist Kund*innen, die keine dauerhafte Geschäftsbeziehung eingehen oder in eine Speicherung von nicht zur Geschäftsabwicklung benötige Daten nicht einwilligen wollen, ein Gastzugang zu ermöglichen. Bei Bestellungen von Waren oder Dienstleistungen im Online-Handel muss

es möglich sein, als „Gast“ nur die Daten anzugeben, die dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind (Grundsatz der Datenminimierung nach Art. 5 Abs. 1 Buchstabe c DS-GVO). Nach Vertragserfüllung nicht mehr benötigte Daten müssen grundsätzlich unverzüglich gelöscht werden. Mit der Einrichtung des Gastzugangs werden nur die für die Vertragsdurchführung und zur Erfüllung gesetzlicher Pflichten, wie insbesondere die gesetzlichen Aufbewahrungspflichten, erforderlichen Daten verarbeitet.

Wird über ein Gastkonto hinausgehend ein fortlaufendes Konto eingerichtet, ist grundsätzlich eine Einwilligung (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a DS-GVO) einzuholen. Eine Einwilligung ist nur dann freiwillig (Art. 7 Abs. 4 DS-GVO) erteilt, wenn eine mit der Einrichtung des fortlaufenden Kund*innenkontos im Sinne der EDSA-Leitlinien 05/2020 gleichwertige Bestellmöglichkeit angeboten wird, ohne dass die bestellende Person Nachteile erleidet, wie zum Beispiel die Bestellung über eine an sieben Tagen rund um die Uhr besetzte Telefonhotline. Die Kund*innen müssen also eine Wahlmöglichkeit haben.

Ausnahmen von dem Erfordernis der Einwilligung sind jedoch in Abhängigkeit vom konkreten Geschäftskonzept im Einzelfall möglich. Soweit besondere Umstände vorliegen, bei denen ein fortlaufendes Kund*innenkonto ausnahmsweise als für die Erfüllung eines Vertrages erforderlich angesehen werden kann (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe b DS-GVO, zum Beispiel für Fachhändler*innen bei bestimmten Berufsgruppen) und mithin hierfür ausnahmsweise keine Einwilligung erforderlich ist, ist dem Grundsatz der Datenminimierung Rechnung zu

tragen, indem etwa das Kund*innenkonto bei Inaktivität automatisiert nach einer kurzen Frist gelöscht wird. Abzustellen ist auf die Zweckbestimmung der Speicherung. Die Frist ist einzelfallabhängig mit Blick auf die Erforderlichkeit danach zu bemessen, um welche Dienstleistung es sich handelt und in welchen Zyklen Kund*innen typischerweise wieder bestellen. Sofern nach Anlage des Kund*innenkontos keine Bestellung innerhalb eines sehr kurzen Zeitraumes erfolgt, wie zum Beispiel innerhalb von 30 Tagen, muss das Kund*innenkonto umgehend gelöscht werden. Dem Bedürfnis von Kund*innen, Ausnahmen von kurzfristigen Löschroutinen zu ermöglichen, kann Rechnung getragen werden, indem zum Beispiel Kund*innen einen per E-Mail versandten Hinweis erhalten, dass eine Löschung unmittelbar bevorstehe, und ihnen die Möglichkeit eingeräumt wird, aktiv zu bestätigen, das fortlaufende Kund*innenkonto fortzuführen.

Sowohl für die Einwilligung gemäß Art. 7 DS-GVO, als auch bei einer für die Vertragserfüllung erforderlichen Datenverarbeitung sind die Kund*innen in verständlicher Sprache über die Einzelheiten der Datenverarbeitung zu informieren (Art. 7 Abs. 2 und Art. 12 – 14 DS-GVO). Die Datennutzung für Werbezwecke auf Grundlage berechtigter Interessen des Online-Shops (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO) ist ausgeschlossen, wenn Kund*innen einen Gastzugang wählen. Sie geben mit ihrer Wahl zugleich zu erkennen, dass sie eine Werbeansprache ablehnen.

Bei Werbung an Kund*innen mit fortlaufenden Konten ist hingegen danach zu unterscheiden, ob neben der Verwendung der für die Vertragserfüllung erhobenen

Kontaktdaten zusätzlich ein Selektionsverfahren zur Anwendung kommt. Die über die Kontaktdaten hinausgehenden personenbezogene Daten dürfen im Falle von fortlaufenden Kund*innenkonten nur auf Grundlage einer Einwilligungserklärung (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe a DS-GVO) für Werbezwecke (unter Nutzung von Selektionsverfahren, das heißt Profiling der Kundenhistorien, Zusammenführung mit Daten aus anderen Quellen) verwendet werden. Hierfür ist die Einwilligungserklärung zur Einrichtung und Führung des fortlaufenden Kund*innenkontos allein nicht hinreichend, weil die selektierte Verarbeitung zu Werbezwecken über diesen Verarbeitungszweck hinausgeht.

Die Verarbeitung personenbezogener Daten aus einer Kund*innenbeziehung mit Kund*innenkonto zum Zweck der einfachen Werbeansprache (das heißt ohne vorausgegangenes Profiling und ohne Zusammenführung mit Daten aus anderen Quellen) stellt hingegen nach Auffassung der LDI NRW zulässige Werbung an Bestandskund*innen dar. Werbung per E-Mail ist dann im Rahmen der Interessenabwägung (Art. 6 Abs. 1 Unterabsatz 1 Buchstabe f DS-GVO) unter den Voraussetzungen von § 7 Abs. 3 UWG ausnahmsweise zulässig (vgl. Orientierungshilfe der Aufsichtsbehörden zur Verarbeitung von personenbezogenen Daten für Zwecke der Direktwerbung unter Geltung der DS-GVO aus Februar 2022, abrufbar unter www.datenschutzkonferenz-online.de/orientierungshilfen). § 7 Abs. 3 UWG ist eine Ausnahme von dem Grundsatz, dass Telefon-, Fax- oder E-Mail-Werbung unzumutbare Belästigungen darstellen und daher ohne vorherige ausdrückliche Einwilligung der Betroffenen unzulässig sind (§ 7 Abs. 2 Nr. 1 und 2 UWG). Nach § 7 Abs. 3 UWG darf ein Online-Shop

demnach seinen Kund*innen Werbung per E-Mail zusenden, wenn er die E-Mail-Adressen im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten hat, er die Adressen zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet, die Kund*innen der Verwendung nicht widersprochen haben und bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass der Verwendung jederzeit widersprochen werden kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen.

Der DSK-Beschuss zum Online-Handel stärkt die Rechte der Verbraucher*innen, ihre Daten nur insoweit preisgeben zu müssen, wie es für den von ihnen gewünschten Zweck erforderlich ist, und trägt so dazu bei, das Recht auf informationelle Selbstbestimmung umzusetzen.

10. Datensicherheit

10.1 „Herrenlose“ Patient*innenunterlagen – Wer ist zuständig?

Immer häufiger werden wir um Beratung gebeten, wie mit in (Miet-)Räumen zurückgelassenen Patient*innenunterlagen umzugehen ist, wenn sich die ehemaligen Praxisinhaber*innen ins Ausland abgesetzt haben, obdachlos geworden oder verstorben sind. In diesen Fällen sind die betroffenen Patientenunterlagen zumeist faktisch „herrenlos“. Eine konkrete gesetzliche Regelung, die das Problem regelt, existiert in NRW nicht.

Patient*innendaten sind besonders sensibel, sie gehören nach Art. 9 Abs. 1 DS-GVO zu den besonderen Kategorien personenbezogener Daten. Sie sind zudem als Privatgeheimnis nach § 203 StGB sowie nach § 9 MBOÄ (Musterberufsordnung-Ärzte) geheim zu halten. Deshalb ist der Schutz von Patient*innenunterlagen nicht nur während des Betriebs einer ärztlichen Praxis, sondern auch bei Aufgabe, Übergabe, Verkauf oder Insolvenz zu gewährleisten.

Patient*innendaten sind bis zum Ablauf gesetzlicher Aufbewahrungsfristen, im Regelfall zehn Jahre nach § 630f Abs. 3 BGB, aufzubewahren. Nach Ablauf der Aufbewahrungsfristen sind die personenbezogenen Daten ordnungsgemäß zu löschen bzw. zu vernichten, Art. 17 Abs. 1 DS-GVO. Bis zum Ablauf der gesetzlichen Aufbewahrungsfristen sind demzufolge sowohl eine sichere Aufbewahrung durch technisch-organisatorische Maßnahmen nach Art. 32 DS-GVO, als auch die Erfüllung der Betroffenenrechte nach Art. 12 ff. DS-GVO zu gewährleisten.

In der Praxis kommt es allerdings insbesondere in den Fällen des Absetzens von Ärzt*innen ins Ausland, als auch in den Fällen des Versterbens zu Schwierigkeiten in der Durchsetzung der datenschutzrechtlichen Pflichten und Anforderungen.

§ 10 Abs. 4 MBOÄ regelt zwar für den Fall der Übergabe oder der Aufgabe der Praxis, dass die Patient*innenunterlagen nicht herrenlos werden dürfen, sondern weiterhin aufzubewahren sind oder „in gehörige Obhut“ gegeben werden sollen. Diese Pflicht obliegt mithin den Ärzt*innen. Allerdings kommt es in der Praxis dennoch dazu, dass die Erfüllung dieser Pflicht nicht durch diese gewährleistet ist.

Problematisch wird es folglich bei „herrenlosen“ Daten, wie in den Fällen plötzlich aufgegebener Praxen, denn dann ist meistens keine datenschutzrechtlich verantwortliche Stelle nach Art. 4 Nr. 7 DS-GVO zu ermitteln. Danach ist „Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Datenschutzrechtlich verantwortlich bleiben in den oben genannten Problemfällen demnach die Ärzt*innen selbst, auch wenn sie sich ins Ausland abgesetzt haben oder obdachlos geworden sind. Auch im Falle des Versterbens geht die datenschutzrechtliche Verantwortlichkeit nicht ohne Weiteres auf Erb*innen über. Zwar geht die zivilrechtliche Aufbewahrungspflicht im Wege der Gesamtrechtsnachfolge auf die vorhandenen Erb*innen über. Damit ist allerdings nicht zwingend ein Übergang der datenschutzrechtlichen Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO verbunden. Denn dies erfordert eine Verarbeitung nach Art. 4 Nr. 2 DS-

GVO und demnach eine Handlung bzw. die Veränderung eines Zustands. Zudem kann es auch bei Erb*innen, die durch die Verarbeitung der personenbezogenen Daten datenschutzrechtlich verantwortlich werden, dazu kommen, dass die Erfüllung der Betroffenenrechte nicht gewährleistet ist. Sind keine Erb*innen vorhanden, geht die zivilrechtliche Aufbewahrungspflicht auf den Staat über. Welche Stelle in diesem Fall allerdings die datenschutzrechtliche Verantwortung trägt, ist unklar.

Vermieter*innen von Praxisräumen werden nicht automatisch Verantwortliche, wenn bei ihnen Patient*innenunterlagen zurückgelassen werden. Mit Beschluss vom 15. Oktober 2020 hat das OVG Hamburg eine Entscheidung des VG Hamburg bestätigt, wonach eine Anordnung gegen den Gebäudeeigentümer mangels datenschutzrechtlicher Verantwortlichkeit für die Lagerung rechtswidrig war. Es liege nämlich gar keine Datenverarbeitung nach Art. 4 Nr. 2 DS-GVO vor. Das VG hat festgestellt, dass in der bloßen Lagerung der Patient*innenakten in den Räumen eines ehemaligen Krankenhauses keine Datenverarbeitung durch den Gebäudeeigentümer liege, weil eine Datenverarbeitung im Sinne der DS-GVO eine Handlung bzw. die Veränderung eines Zustands voraussetzt, die hier aber nicht vorliege. Die tatsächliche Sachherrschaft begründe für sich genommen keine rechtliche Entscheidungsgewalt und damit auch keine datenschutzrelevante Pflichtenstellung. Die Frage nach dem Verantwortlichen hat das VG offengelassen.

In den beschriebenen Fällen ist die datenschutzrechtlich verantwortliche Stelle faktisch nicht greifbar, so-

dass die Anforderungen der DS-GVO nicht durchgesetzt werden können. Auch die Ärztekammern lehnen eine Zuständigkeit ab. Die Ordnungsbehörden können nur eine Sicherung der Patient*innenunterlagen gewährleisten, die Erfüllung der Betroffenenrechte allerdings nicht.

In Rheinland-Pfalz und Baden-Württemberg ist bspw. in dem jeweiligen Heilberufsgesetz geregelt, dass eine grundsätzliche Verwahrungs- und Verwaltungspflicht der Ärztekammer besteht, wenn diese nicht durch das Kammermitglied oder dessen Rechtsnachfolger*in gewährleistet ist. Nach § 4 Heilberufe-Kammergesetz Baden-Württemberg haben die Kammern bei der Wahrnehmung ihrer Aufgaben die Interessen des Gemeinwohls und die Rechte der Patient*innen zu beachten. Deren Unterlagen haben sie für die Dauer der Aufbewahrungspflicht in Obhut zu nehmen und Patient*innen Einsicht zu gestatten, sofern dies nicht durch das verpflichtete Kammermitglied oder deren Rechtsnachfolger*innen gewährleistet ist. Gegenüber den Verpflichteten besteht in diesem Fall ein Anspruch auf Erstattung der Kosten, die im Zusammenhang mit der Aufbewahrung der Patient*innenakten entstehen. Die Kammern können andere Kammermitglieder oder Dritte mit der Erfüllung dieser Aufgabe betrauen, zudem können die Kammern gemeinsame Einrichtungen zur Erfüllung dieser Aufgabe errichten oder nutzen. In § 22 Abs. 2 Satz 2 Heilberufsgesetz Rheinland-Pfalz ist geregelt, dass die Kammer verpflichtet ist, die Unterlagen im Rahmen der Verwaltungsvollstreckung zu verwahren und zu verwalten, wenn das Kammermitglied dieser Pflicht nicht nachkommt. Eine vergleichbare Regelung ist in § 27 Abs. 2 des Heilberufe-Kammergeset-

zes Berlin vorhanden. Dort erstreckt sich die Vorschrift auch auf Nachfolger*innen und Erb*innen. In beiden Vorschriften werden auch die Verpflichtungen aus dem Datenschutzrecht miteinbezogen.

Eine solche Regelung besteht in NRW nicht. In NRW wurde lediglich im Krankenhausbereich der § 34c Krankenhausgestaltungsgesetz des Landes NRW geschaffen. Danach besteht die Pflicht, schon vor Eintreten eines Insolvenzfalles Regelungen für die Aufbewahrung von Patientenunterlagen und die Gewährleistung von Betroffenenrechten zu treffen.

Um Patient*innenunterlagen angemessen schützen und die Erfüllung der Betroffenenrechte zu gewährleisten, bedarf es einer gesetzlichen Regelung mit Zuweisung der datenschutzrechtlichen Verantwortlichkeit für die Fälle, in denen der primär datenschutzrechtlich Verantwortliche nicht greifbar ist.

10.2 Unzureichender technischer Schutz von Unterlagen einer Anwaltskanzlei

Verfahrensakten von Rechtsanwält*innen unterliegen Geheimhaltungs- und Verschwiegenheitspflichten. Daher müssen Anwält*innen besondere Sorgfalt walten lassen, wenn sie für die Verarbeitung von Verfahrensakten Dienste Dritter in Anspruch nehmen. Wir wurden mit einem Fall befasst, der die gebotenen Maßnahmen zum Schutz der Unterlagen vor unberechtigten Zugriffen vermissen ließ.

Die Kanzlei nutzte zur internen Bearbeitung und externen Weitergabe von Dokumenten den Datenraum eines externen Dienstleistungsunternehmens. Personen die berechtigt waren, auf Unterlagen zuzugreifen,

erhielten dazu jeweils einen Link mit einer zufälligen Zeichenkette, die Zugriff auf die dort gespeicherten Dokumente aus dem Internet ermöglichte. Das Generieren der Zeichenketten wurde durch das Dienstleistungsunternehmen zur Verfügung gestellt. Weitere Zugriffsbeschränkungen oder Authentifizierungsprozesse über die Zeichenketten hinaus gab es nicht.

Wir wurden aufmerksam, weil ein solcher Zugangslink mit Zahlenkette für den internen Zugriff auf Dokumente an Dritte weitergegeben wurde. Unberechtigte hatten damit aus dem Internet heraus potentiell Zugriff auf eine Vielzahl von vertraulichen Dokumenten mit teilweise hohem Schutzbedarf. Solche Zugriffsverfahren für Dokumente, die einem besonderen Schutz unterliegen, müssen einem definierten Rechte- und Rollenkonzept unterliegen, nach dem der Zugriff auf die Dokumente gesteuert wird. Allein ein aus dem Internet erreichbarer Link für die regelmäßige Einsicht in eine große Zahl von Unterlagen gewährleistet kein ausreichendes Berechtigungskonzept. Anwält*innen müssen sicherstellen und nachvollziehen können, dass die Unterlagen nur in die Hände geraten, die von den Akteninhalten Kenntnis bekommen dürfen. Bei Zugriffen auf Daten mit hohem Schutzbedarf über das Internet sollte eine Zwei-Faktor-Authentifizierung erfolgen, die es ermöglicht, den Zugriff zu personalisieren und einen Zugriff Unberechtigter wesentlich erschwert.

In dem bekannt gewordenen Fall hat die LDI NRW den Verantwortlichen kontaktiert. Der Zugang wurde daraufhin deaktiviert und ein neues, verbessertes Verwaltungssystem eingerichtet.

Anwält*innen, aber auch andere Berufsgeheimnisträger müssen bei der Auswahl von Dienstleistungsunternehmen, die sie bei der Verarbeitung personenbezogener Daten unterstützen, besonders wachsam sein. Berufsgeheimnissen unterliegende Daten haben einen hohen Schutzbedarf und sind technisch vor dem Zugriff durch Unberechtigte wirksam zu schützen. Ein Link mit einer Zeichenkette, der einen Internetzugriff ermöglicht, gewährleistet als alleinige Authentifizierungsmethode in derartigen Fällen keinen ausreichenden Schutz.

10.3 Digitale Verwaltung – Pilotierung zentraler Posteingangsscanstellen NRW

Die LDI NRW wurde im Rahmen eines Beteiligungsverfahrens vom Beauftragten der Landesregierung NRW für Informationstechnik (CIO NRW) zu der vorgesehenen Pilotierung der zentralen Posteingangsscanstellen in Kenntnis gesetzt. Im Zuge dieser Beteiligung wurde uns die Sollkonzeption dieses Prozesses vorgestellt. Weiterhin erfolgte ein Informationsbesuch der zentralen Posteingangsscanstelle Rheinland.

Im Auftrag der Landesverwaltung und unter Fachaufsicht des CIO NRW werden zentrale Posteingangsscanstellen vom Landesbetrieb Information und Technik Nordrhein-Westfalen aufgebaut. Der ersetzende Posteingangsscan ist ein Dienst zur Digitalisierung der Posteingänge im Rahmen der Digitalisierung der Verwaltungsarbeit, der den Behörden in NRW zur Verfügung gestellt wird.

In den Scanstellen werden eingehende Papierunterlagen im Sinne des E-Government-Gesetz NRW § 10

inklusive aller personenbezogener Daten digitalisiert. Anschließend ist die Vernichtung der Papier-Dokumente vorgesehen. Um dabei die Vertraulichkeit, Verfügbarkeit und Integrität der personenbezogenen Daten nach dem Stand der Technik im Sinne des Art. 32 Abs. 1 DS-GVO in den zentralen Posteingangsscanstellen zu garantieren, wurde die technische Richtlinie 03138 „Ersetzendes Scannen“ (RESISCAN) des Bundesamts für Sicherheit in der Informationstechnik zu der Umsetzung der technischen und organisatorischen Maßnahmen herangezogen und eine entsprechende Zertifizierung der Posteingangsscanstellen nach dieser Richtlinie vorgesehen. Der Gegenstand der Zertifizierung umfasst jedoch nicht alle Verarbeitungsvorgänge personenbezogener Daten, die in den Posteingangsscanstellen erfolgen. Ergänzend zu dieser technischen Richtlinie ist somit unter anderem der konkrete Prozess zur abschließenden sicheren Vernichtung der Unterlagen zu definieren. Daher überführen die Posteingangsscanstellen die Dokumente nach Ablauf der qualitätssichernden Aufbewahrungsfristen in einen Vernichtungsprozess, der gemäß der technischen Norm DIN66399 umgesetzt ist. Damit wird eine datenschutzkonforme Entsorgung sichergestellt, sodass anschließend keine weitere Verarbeitung der erhaltenen Daten durch die Posteingangsscanstellen erfolgt.

Zur Klärung verschiedener Fragen haben wir einen Katalog mit Anmerkungen und Fragestellungen an den CIO NRW übermittelt. Parallel zur Beantwortung der Fragestellungen hat die LDI NRW das Angebot eines Informationsbesuchs der Scanstelle Rheinland wahrgenommen. Hierbei wurden die einzelnen Stationen der Scanstelle und einzelne Prozesse exempla-

risch präsentiert. Die Anmerkungen und Fragestellungen des übermittelten Katalogs wurden mit der Stellungnahme des CIO weitgehend abschließend adressiert. Allerdings ist jede Behörde als Kundin der Scanstelle für ihre dort durchgeführten Scanprozesse selbst datenschutzrechtlich Verantwortliche. Deshalb muss sie einen Vertrag mit der Scanstelle schließen, die nur im Auftrag der jeweiligen Behörde Daten verarbeiten kann. Da der CIO NRW kein Verantwortlicher ist, kann er diese Aufgabe nicht selbstständig für die Kundenbehörden vornehmen. Hilfreich wäre, wenn der CIO NRW einen Muster-Auftragsverarbeitungsvertrag über die Prozesse erstellen würde, den die Kundenbehörden an ihre Gegebenheiten anpassen können. Dies wurde ihm empfohlen.

Die ersetzende Digitalisierung der Posteingänge stellt eine integrale Komponente der elektronischen Verwaltungsarbeit dar, welche eine umfängliche Verarbeitung von personenbezogenen Daten in den zentralen Scanstellen erfordert. Die technische Richtlinie RESISCAN ist eine sinnvolle Grundlage, um einen strukturierten Scanprozess zu realisieren, der die sicherheitsrelevanten technischen und organisatorischen Maßnahmen abdeckt. Weil die Scanstelle zukünftig ein Nadelöhr für die vielfältigen analog eingehenden personenbezogenen Daten sein wird, die von der digitalen Verwaltung bearbeitet werden sollen, ist die vom CIO NRW vorgesehene Konformitätsprüfung der Posteingangsscanstellen nach dieser technischen Richtlinie zu begrüßen.

10.4 Alarmierungsbenachrichtigungen von Feuerwehren und Rettungsdiensten im Internet

BOS-Funk-Benachrichtigungen von Leitstellen – zumeist Alarmierungsbenachrichtigung von Feuerwehren und Rettungsdiensten – wurden im Internet frei und in Echtzeit veröffentlicht. Es gab verschiedene Wege, wie sie dort hingelangt sind.

Behörden und Organisationen mit Sicherheitsaufgaben (BOS) – zum Beispiel Feuerwehren – setzen zur Alarmierung ihrer operativen Einheiten im Rahmen des sog. BOS-Funk verschiedene Formen von Kurznachrichten, sog. Telegramme, ein. BOS-Funk-Benachrichtigungen enthalten regelmäßig personenbezogene Daten wie Adressen und Namen sowie Gesundheitsdaten, um die alarmierten Stellen über die Art des Einsatzes zu informieren. Über (zum Teil kostenfreie) Software können diese Telegramme des BOS-Funk dekodiert, aufbereitet und auf einer Webseite dargestellt werden. Solche Software wird zum Teil auch von Leitstellen eingesetzt. Je nach Konfiguration steht auch ein Gast-Zugang zur Verfügung, über den ohne weitere Authentifizierung auf die Alarmierungsbenachrichtigungen zugegriffen werden kann.

Mit sog. Computer-Suchmaschinen kann das Internet gezielt nach Webservern durchsucht werden, auf denen eine solche Software eingesetzt wird. Auch Alarmierungsbenachrichtigungen von Leitstellen in NRW waren ungeschützt im Internet veröffentlicht und konnten so gefunden werden. Einige Leitstellen haben uns die Veröffentlichung als Datenpanne gemeldet.

Bereits im Jahr 2020 wurde über die zugrundeliegende Problematik in den Medien berichtet. Das Innenministerium hatte daraufhin die Leitstellen über die Bezirksregierung auf einen datenschutzkonformen Umgang mit BOS-Funkdaten hingewiesen. Die uns bekanntgewordenen Fälle zeigen jedoch, dass die zugrundeliegenden Probleme noch nicht flächendeckend gelöst wurden.

Die Alarmierungsbenachrichtigungen umfassen unterschiedlich sensible Informationen. Jedenfalls enthalten sie Angaben zum Alarmierungszeitpunkt, zur alarmierten Einheit, zur Adresse des Einsatzortes und zur Art des Einsatzes. Gerade bei der Alarmierung von Rettungsdiensten enthalten die Benachrichtigungen regelmäßig auch Gesundheitsdaten und neben der Adresse des Einsatzortes auch den Namen und in Einzelfällen das Alter der betroffenen Person. Somit wurden auch besonders sensible personenbezogene Daten in den bekanntgewordenen Fällen im Internet veröffentlicht.

Bei der Untersuchung der Ursache für die Veröffentlichung haben sich drei verschiedenen Fallgruppen ergeben.

1. **Betrieb eines unsicher konfigurierten Webservers durch die Leitstelle**

   In einzelnen Fällen setzten Leitstellen selbst unsicher konfigurierte Webserver ein. Aufgrund einer fehlenden Anpassung der Konfiguration der Software war der Zugang auf die Alarmierungsbenachrichtigungen über ein Gastkonto ohne weitere Zugangsbeschränkung möglich. Nach dem Bekanntwerden der Sicherheitslücke haben die

Leitstellen die Konfiguration unverzüglich angepasst.

Systeme zur Verarbeitung von BOS-Funk-Benachrichtigungen sollten zum Schutz vor unbefugten Zugriffen möglichst in einem vom Internet getrennten bzw. abgeschotteten Netz betrieben werden. Ist aus dienstlichen Gründen eine Erreichbarkeit der Systeme über das Internet erforderlich, müssen die Server so konfiguriert werden, dass nur befugte und geeignet authentifizierte Personen Zugang zu den Daten erhalten. Insbesondere muss ein angemessenes Schutzniveau hinsichtlich der verarbeiteten Gesundheitsdaten gewährleistet werden.

2. Abhören unverschlüsselter BOS-Funkbenachrichtigungen

In den anderen Fällen wurden durch Dritte Alarmierungsbenachrichtigungen abgehört und auf Webservern unbefugt veröffentlicht. In einem Teil der Fälle war das unbefugte Abhören möglich, da die Alarmierungsbenachrichtigungen unverschlüsselt übermittelt wurden. Nach dem Stand der Technik und unter Berücksichtigung des Risikos für die Rechte und Freiheiten natürlicher Personen müssen BOS-Funkdaten auf dem gesamten Kommunikationsweg verschlüsselt übertragen werden. Um dies sicherzustellen, sollte eine flächendeckende Umstellung auf den Digitalfunk BOS angestrebt werden. Dieser sieht eine Ende-zu-Ende-Verschlüsselung zwischen den an der Kommunikation beteiligten Endgeräten vor.

Die betroffenen Leitstellen haben zugesichert, Endgeräte zu beschaffen, über die eine verschlüsselte Kommunikation personenbezogener Daten gewährleistet werden kann, sobald die entsprechenden Haushaltsmittel zur Verfügung stehen. In der Zwischenzeit sollen sensible personenbezogene Daten nicht über die Alarmierungsbenachrichtigungen selbst, sondern über einen getrennten, sicheren Kanal an die Einsatzkräfte mitgeteilt werden.

3. Abhören verschlüsselter BOS-Funkbenachrichtigungen

In anderen Fällen fand die Übermittlung der Alarmierungsbenachrichtigungen verschlüsselt statt, jedoch war es Dritten möglich, die verschlüsselten Benachrichtigungen abzuhören und zu entschlüsseln, um sie dann zu veröffentlichen.

Die digitalen Schlüssel zur verschlüsselten Kommunikation sind meist auf dem Endgerät bzw. einer Chipkarte (auch Sicherheitskarte genannt) gespeichert, die in das Endgerät eingelegt wird. Durch geeignete Maßnahmen muss sichergestellt werden, dass die digitalen Schlüssel nicht in den Besitz von Unbefugten kommen bzw. zu unbefugten Zwecken eingesetzt werden. Die Endgeräte dürfen daher nur befugten Personen zu dienstlichen Zwecken zur Verfügung gestellt werden. Weiterhin müssen Prozesse zur Aushändigung, Rückgabe, Aussonderung und für den Fall des Verlustes eines Endgeräts bzw. einer Sicherheitskarte festgelegt, umgesetzt und überwacht werden. Die mit der Nutzung des BOS-Funks betrauten Personen sind zudem hinsichtlich eines

datenschutzkonformen Einsatzes und Umgangs mit den Endgeräten zu unterweisen.

Das unbefugte Abhören ist unabhängig von der Frage der Verschlüsselung gemäß § 27 TTDSG strafbar. Die strafrechtlichen Ermittlungen gegen diejenigen, die die Meldungen abgehört haben, erfolgt durch die Polizei bzw. die Staatsanwaltschaften.

BOS-Funk-Benachrichtigungen müssen nach dem Stand der Technik verschlüsselt übertragen werden. Server, über die BOS-Funk-Benachrichtigungen verarbeitet werden, sollten nur dann über das Internet erreichbar sein, wenn dies zwingend erforderlich ist und sie so abgesichert sind, dass nur befugte Personen Zugriff auf die Daten erhalten.

10.5 Beratung der Kassenärztlichen Vereinigung zum E-Rezept

In den Regionen der Kassenärztlichen Vereinigung Westfalen-Lippe (KVWL) und der Kassenärztliche Vereinigung Schleswig-Holstein wurde am 1. September 2022 die Pilotphase des E-Rezepts eingeleitet. Die KVWL hat die LDI NRW in dieser Pilotphase um Beratung zu alternativen Umsetzungsmethoden gebeten, da der von der Gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) zur digitalen Übermittlung des E-Rezepts vorgesehene Token nur lückenhaft verfügbar ist.

Das E-Rezept soll den Prozess der Verordnung und des Einlösens von Rezepten papierlos ermöglichen. Dazu sollen Ärzt*innen das Rezept im zentralen E-

Rezept-Fachdienst der Telematik-Infrastruktur hinterlegen. Für die so hinterlegten Informationen werden E-Rezept-Token generiert, die einen 2D-Code zur erleichterten optischen Erfassung aufweisen. Diese können anschließend in einer Apotheke vorgelegt werden, die damit auf die im E-Rezept-Fachdienst hinterlegten Informationen zugreift und das Rezept einlösen kann.

Die hierfür vordefinierten Prozesse der Gematik sehen vor, dass die E-Rezept-Token vom betroffenen Versicherten mittels der offiziellen E-Rezept-App abgerufen werden können, sobald sie im E-Rezept-Fachdienst vorliegen. Alternativ kann der Versicherte ebenfalls einen Ausdruck des E-Rezept-Tokens von der verordnenden Stelle erhalten, was aber das Ziel einer durchgehend digitalen Lösung verfehlt. Versicherte können entweder den Ausdruck oder den digitalen Token mittels E-Rezept-App vor Ort in der Apotheke vorzeigen und so das E-Rezept einlösen. Des Weiteren entwickelte die Gematik eine Spezifikation, die den Apotheken einen Abruf der E-Rezepte eines Versicherten ermöglicht, wenn dieser seine elektronische Gesundheitskarte vor Ort in ein Lesegerät steckt. Eine PIN ist dabei allerdings bisher nicht erforderlich. Dadurch können bei Entwendung oder Verlust der Karte Unberechtigte auf sensible Gesundheitsdaten zugreifen oder gar Rezepte einlösen. Hinsichtlich der Spezifikation dieser Schnittstelle sind daher aus Sicht der zuständigen Aufsichtsbehörde zusätzliche Maßnahmen zu Basisabsicherung der IT-Lösung zu treffen.

Da die Infrastruktur für die so vorgesehenen digitalen Übermittlungsmethoden der E-Rezept-Token nach wie vor nur lückenhaft zur Verfügung steht, ist die

KVWL vorerst aus dem E-Rezept-Rollout ausgestiegen. Bei ihrer Suche nach Möglichkeiten, den Ärzt*innen in Westfalen-Lippe eine digitale Übermittlung der Token an die Patient*innen auch ohne Rückgriff auf die Gematik-App oder analoge Dokumente datenschutzkonform zu ermöglichen, steht die LDI NRW der KVWL beratend zur Seite. Dabei ist zu berücksichtigen, dass auch die E-Rezept-Token selbst gesetzlich besonders geschützte Gesundheitsdaten enthalten, bei denen ein Bruch der Vertraulichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellen würde. Hinsichtlich eines von der KVWL angedachten möglichen Versands der E-Rezept-Token per E-Mail wies die LDI NRW daher auf die Notwendigkeit einer Ende-zu-Ende-Verschlüsselung hin.

Die von der Gematik bereitgestellte Infrastruktur zur digitalen Übermittlung der E-Rezept-Token steht nicht flächendeckend zur Verfügung, sodass alternative digitale Methoden von der KVWL geprüft werden. Durch eine datenschutzkonforme und allgemein zugängliche Bereitstellung der von der Gematik vorgesehenen Strukturen könnte eine bundesweit einheitliche Systematik etabliert werden und die Notwendigkeit zur Suche geeigneter Alternativen entfallen. Wir begrüßen die konstruktive Zusammenarbeit mit der KVWL und werden auch im weiteren Prozess beratend mitwirken.

10.6 Recht mit dem Standard-Datenschutzmodell (SDM) Version 3.0 technisch umsetzen

Mit dem Standard-Datenschutzmodell (SDM) stellt die DSK Verantwortlichen, Auftragsverarbeitern, Datenschutzbeauftragten und Aufsichtsbehörden ein Hilfsmittel zur Auswahl, Umsetzung und Prüfung von datenschutzrechtlich geforderten technischen und organisatorischen Maßnahmen bereit. Die Version 3.0 rückt die einzelnen Verarbeitungsphasen (zum Beispiel Erhebung, Nutzung, Übermittlung, Löschung) stärker in den Fokus. In einem so genannten SDM-Würfel, werden die Ziele, die den Datenschutz gewährleisten, technische Ebenen und Verarbeitungsphasen grafisch verbunden. Das ermöglicht für jede Phase, die relevanten Fragen im Blick zu behalten und die passenden technisch-organisatorischen Maßnahmen zu bestimmen.

Die LDI NRW ist an der Fortschreibung des SDM beteiligt, sie hat auch an der Version 3.0 mitgearbeitet.

Die Version 3.0 liefert zusätzliche Unterstützung bei der Beschreibung und Untersuchung einer Verarbeitungstätigkeit. Dies umfasst die Aufbereitung einer Verarbeitung in ihre Schritte bzw. Phasen und den dabei beteiligten Komponenten (Daten, Systeme und Dienste sowie Prozesse) auf den unterschiedlichen Ebenen (Geschäftsprozessebene, Fachapplikationsebene und Infrastrukturebene). Diese Aufbereitung kann dann systematisch hinsichtlich der Umsetzung der datenschutzrechtlichen Anforderungen bzw. der Gewährleistungsziele und den mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen untersucht werden. Auf Basis dieser Untersuchung können gezielt technische und

organisatorische Maßnahmen abgeleitet werden, um datenschutzrechtliche Anforderungen umzusetzen und die Risiken abzumildern.

Um die Auswahl der technischen und organisatorischen Maßnahmen zu unterstützen, zählt das SDM generische Referenzmaßnahmen (zum Beispiel „Implementierung eines sicheren Authentifizierungsverfahrens“, „Trennung nach Organisations-/Abteilungsgrenzen“, „Schaffung notwendiger Datenfelder zum Beispiel für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen“, „Festlegung und Umsetzung eines Löschkonzepts“) auf. Das SDM wird durch einen sukzessiv erweiterten Maßnahmenkatalog ergänzt, in dem die Referenzmaßnahmen konkretisiert werden (zum Beispiel Trennen, Löschen und Vernichten, Einschränken der Verarbeitung). Die Referenzmaßnahmen sowie die Maßnahmen aus den Maßnahmenkatalogen müssen jeweils auf die konkrete Verarbeitung angepasst und ggf. durch zusätzliche Maßnahmen ergänzt werden.

Die mit der Version 3.0 des SDM eingeführten Vorgangsgruppen und Phasen eines Datenlebenszyklus erlauben eine systematische Beschreibung und Untersuchung einer Verarbeitungstätigkeit. Der „SDM-Würfel“ setzt die zentralen Sichten auf eine Verarbeitungstätigkeit zueinander in Beziehung und unterstützt damit eine systematische und umfassende Analyse einer Verarbeitungstätigkeit. Dies erlaubt schließlich die Auswahl und Umsetzung angemessener und geeigneter technischer und organisatorischer Maßnahmen.

Verantwortliche, Auftragsverarbeiter und Datenschutzbeauftragte erhalten mit der neuen Version des SDM eine verbesserte Hilfestellung, an der sie sich bei der Untersuchung von Verarbeitungstätigkeiten sowie der Auswahl, Umsetzung und Prüfung der datenschutzrechtlich geforderten technischen und organisatorischen Maßnahmen orientieren können.

2.Teil: Informationsfreiheitsbericht

1. Gerichtsentscheidungen zur Informationsfreiheit

- Das Verwaltungsgericht Düsseldorf hat sich zum einen ausführlich mit der Bereichsausnahme der in **§ 2 Abs. 3 IFG NRW** aufgeführten **„Forschungseinrichtung“** auseinandergesetzt (Urteil vom 14. Mai 2021, Az. 29 K 7636/18). Eine solche setze einen organisatorischen Rahmen voraus, innerhalb dessen die Forschungstätigkeit stattfindet. Zum anderen enthält das Urteil Ausführungen dazu, wann ein Informationszugangsanspruch wegen **unverhältnismäßigen Verwaltungsaufwands** ausgeschlossen sein kann.

  Die Klägerin hatte Zugang zu diversen, sich über einen Zeitraum von sechs Jahren erstreckenden Unterlagen der Ethik-Kommission der Ärztekammer Nordrhein zu prospektiven Datenerhebungen und nichtinterventionellen Studien beantragt. Obwohl die von der Klägerin begehrten Informationen den Bereich der Forschung betrafen, stellte das Gericht fest, dass die Ethik-Kommission der Beklagten keine Forschungseinrichtung im Sinne des § 2 Abs. 3 IFG NRW und damit grundsätzlich zur Auskunft verpflichtet sei. Weder die beklagte Ärztekammer noch ihre Ethik-Kommission nähmen Forschungsaufgaben wahr. Auch die Aufgabe der Ethik-Kommission, nämlich die Beratung von Kammerangehörigen der Beklagten in berufsrechtlichen und berufsethischen Fragen stelle keine solche Forschung dar.

  Gescheitert ist die Klage aber daran, dass das Gericht den Verwaltungsaufwand für unverhältnismäßig befand, der mit der Erfüllung des Anspruchs für die Ärztekammer bzw. deren Ethik-Kommission verbunden gewesen wäre. Einen Ablehnungsgrund eines unverhältnismäßigen Verwaltungsaufwands enthält

das IFG NRW an sich nicht. Das Gericht sah in dem Fall aber ein so außergewöhnliches Missverhältnis zwischen Nutzen der Information für die Antragstellerin und Aufwand für die informationspflichtige Stelle, dass es eine institutionelle Überforderung und eine Beeinträchtigung der Funktionsfähigkeit der Ärztekammer sah.

- In dem aktuellsten Urteil zur Informationsfreiheit hat sich das OVG NRW mit **rechtsmissbräuchlicher Antragstellung** auseinandergesetzt (Urteil vom 6. Oktober 2022, Az. 15 A 760/20). Ein Antrag auf Informationszugang kann nur in besonders gelagerten Ausnahmefällen und unter engen Voraussetzungen unter Hinweis auf seine Rechtsmissbräuchlichkeit abgelehnt werden. Im vorliegenden Fall – dem ein Antrag auf Zugang zu dem senatsinternen Geschäftsverteilungsplan eines Oberlandesgerichts zugrunde lag – hat das OVG NRW zu dieser von der Rechtsprechung äußert selten bemühten ultima ratio gegriffen. Das Urteil beschreibt einen Extremfall, was in den Entscheidungsgründen, die es lohnt, zu lesen, sehr deutlich wird. Das Gericht hat es sich hier nicht leichtgemacht und begründet sehr detailliert und ausführlich seine Entscheidung.

  Grundsätzlich sind die Motive des Antragstellenden für seine Anspruchsberechtigung unerheblich und ein Anspruch nach dem IFG NRW muss deswegen auch nicht begründet werden.

  Das Gericht sah das Antragsbegehren des Klägers in diesem speziellen Fall allerdings als rechtmissbräuchlich an, da damit ersichtlich rein schikanöse oder belästigende Ziele verfolgt würden. Der Kläger hatte rund 350 Eingaben innerhalb von vier Jahren im

Zusammenhang mit gerichtlichen Geschäftsverteilungsplänen in NRW sowie zahlreicher anderer an die Justiz adressierte Anträge gestellt. Nach der Überzeugung des Gerichts ergab das Gesamtbild „eine schikanöse Zielrichtung des Klägers, Vergeltung für eine von ihm empfundene ungerechte Behandlung durch die Justiz dadurch zu nehmen, dass er diese mit vielfachen Anträgen und Einwendungen überzieht und beschäftigt und hierzu die Möglichkeiten, die ihm im Grundsatz voraussetzungslose bzw. niedrigschwellige Ansprüche gewähren, als Mittel nutzt“.

Unabhängig von dieser Feststellung des Rechtsmissbrauchs hatte das OVG NRW bereits den Anwendungsbereich des IFG NRW als nicht eröffnet angesehen, da der Inhalt von gerichtlichen Geschäftsverteilungsplänen keine Verwaltungstätigkeit, sondern justizielle Tätigkeit sei.

2. 2022: 20 Jahre Informationsfreiheit in NRW

Mit seinen mittlerweile 20 Jahren ist das IFG NRW etwas in die Jahre gekommen. Eine Weiterentwicklung hin zu einem modernen Transparenzgesetz wäre wünschenswert. Auf der gemeinsam mit dem Landtag veranstalteten Jubiläumsfeier haben wir darüber mit Vertreter*innen aus Politik, Zivilgesellschaft, Justiz und Verwaltung diskutiert.

Das 20-jährige Bestehen des IFG NRW haben wir zusammen mit zahlreichen Gästen am 19. Oktober 2022 im Landtag gefeiert. Auf dem Programm standen Vorträge zur Geschichte, Gegenwart und Zukunft des IFG NRW. Hierfür konnten wir Referent*innen vom OVG NRW, von den Kommunalen Spitzenver-

bänden sowie von Transparency International gewinnen. Im Anschluss fand eine kontroverse Diskussion unter Beteiligung des Publikums statt.

Die wesentlichen Aussagen und Erkenntnisse der Veranstaltung lassen sich folgendermaßen zusammenfassen: Das IFG NRW war zu seiner Geburtsstunde sehr modern. Es hat sich bewährt und über die Jahre die Kultur im Umgang mit Informationen positiv verändert. Die mittlerweile lang geübte Praxis hat gezeigt, dass das IFG NRW imstande ist, gegenläufige Interessen von Auskunftsbegehrenden, öffentlichen Stellen und betroffenen Dritten in Ausgleich zu bringen und sachgerechte Ergebnisse zu liefern. Gleichwohl wünschten sich die Kommunalen Spitzenverbände bessere Möglichkeiten einer ausufernden und aufwändigen Inanspruchnahme in Einzelfällen entgegenzuwirken.

Einigkeit bestand darin, dass das IFG NRW ein gutes Instrument für Bürger*innen ist, um der Verwaltung „auf den Zahn zu fühlen“. Es liefert damit einen wichtigen Beitrag für eine starke Demokratie. Inzwischen ist das einst sehr moderne IFG NRW in puncto „proaktiver Veröffentlichungen“ nicht mehr auf der Höhe der Zeit. Die Weiterentwicklung zu einem Transparenzgesetz ist – nicht zuletzt mit Blick über die Landesgrenzen hinaus – auch in NRW angekommen. Gerade dort, wo die Verwaltung wichtige Entscheidungen trifft oder öffentliche Gelder verausgabt, müssen wir weg von der Holschuld der Bürger*innen und hin zu einer Bringschuld des Staates. Amtliche Informationen müssen öffentlich und kostenlos im Internet zugänglich gemacht werden. Ein wesentliches Charaktermerkmal einer gut funktionierenden Demokratie

ist es, dass sich staatliches Handeln durch Nachvollziehbarkeit legitimiert.

Wir freuen uns über 20 Jahre Informationsfreiheit und blicken erwartungsvoll in die Zukunft. Sehr gerne würden wir uns schon bald zu der nächsten Festveranstaltung zusammenfinden, wenn es heißt: „Adieu IFG – willkommen Transparenzgesetz!“

3. Wer hat mit wem und wann zur Bewältigung der Hochwasserkatastrophe kommuniziert? Das geht uns alle an!

Die Hochwasserkatastrophe war schlimm, in erster Linie für die unmittelbar Betroffenen. Die Kommunikation verantwortlicher Stellen während einer solchen Krise steht besonders im Fokus und wird von der Bevölkerung ganz genau verfolgt. Informationen dazu, wer wann mit wem kommuniziert hat, sind dabei von hohem öffentlichen Interesse. Für die Offenlegung ist das IFG NRW ein geeignetes Instrument.

Ein Antragsteller beantragte bei der Staatskanzlei Zugang zu der Kommunikation während der Hochwasserkatastrophe für die Tage 14. und 15. Juli 2021 mit zwei betroffenen Gemeinden bzw. einem Kreis. Bei dem Antragsteller handelt es sich um einen Journalisten, der ausdrücklich keine Anfrage nach dem Landespressegesetz NRW, sondern einen Antrag nach dem IFG NRW gestellt hatte. Innerhalb der Monatsfrist und auch nach einer Erinnerung erhielt er jedoch keine Antwort. Weshalb der Antrag nicht innerhalb der Monatsfrist bearbeitet wurde, war schnell klar: Im Rahmen der Koordination der Hilfen musste schnell

gehandelt werden. Regierung und Verwaltung wurden hier an ihre Grenzen gebracht. Eine solche Katastrophe ist ein außergewöhnliches Ereignis und die Bearbeitung von IFG-Anfragen für informationspflichtige Stellen hat dann nicht erste Priorität.

Der Antragsteller wandte sich schließlich an uns, und wir griffen den Fall gegenüber der Staatskanzlei auf. In der Antwort wies diese darauf hin, dass sich die Beantwortung wegen der Hochwasserkatastrophe und deren Folgenbeseitigung verzögert habe. Die Prüfung des IFG-Antrags werde gleichzeitig mit der Sichtung der Unterlagen für den parlamentarischen Untersuchungsausschuss zur Hochwasserkatastrophe erfolgen. Diese Prüfung dauerte dann allerdings noch weitere vier Monate. Am Ende erhielt der Journalist die beantragten Informationen erst ein Dreivierteljahr nachdem er den Antrag gestellt hatte. Zu diesem Zeitpunkt hatte der Ausschuss auch schon längst getagt. Auch wenn es hier nachvollziehbar war, dass im Moment der Katastrophe Dringenderes zu tun war, wäre für den Journalisten ein früherer Informationszugang wichtig gewesen, um objektiv über das Handeln der betroffenen Stellen berichten zu können.

Informationen von hohem öffentlichen Interesse sollten von formationspflichtigen Stellen zeitnah offengelegt werden. Das hat auch bei der Krisenbewältigung große Bedeutung: So kann das Vertrauen in Verwaltung und Politik und damit in unsere Demokratie gestärkt werden. Eine informierte Öffentlichkeit ist eher bereit, die mit der Krise verbundenen Einschränkungen zu tragen.

4. Staatskanzlei macht Kunst zum Staatsgeheimnis

Informationen zu Kunstwerken, die sich im Eigentum des Landes NRW befinden, sind vor einem Bekanntwerden zu schützen, da hierdurch die öffentliche Sicherheit beeinträchtigt würde – ist diese Ablehnungsbegründung etwa ernst gemeint?

Ein Antragsteller hatte uns in einem Fall um Vermittlung gebeten, in dem es ihm um eine Auflistung der Kunstwerke im Bestand der Staatskanzlei NRW ging. Unter anderem wollte er wissen, wann welche Kunstwerke zu welchem Kaufpreis erworben worden waren und wo sie sich aktuell befänden. Die Staatskanzlei lehnte seinen Antrag unter Bezugnahme auf § 6 Satz 1 Buchstabe a IFG NRW ab: Die Offenbarung der Informationen würde die öffentliche Sicherheit beeinträchtigen, da eine konkrete Gefahr bestünde, dass die Informationen zur Begehung von Eigentumsdelikten verwendet würden.

In unserem Auskunftsersuchen gaben wir zu bedenken, dass bereits lange Zeit vor dem Antrag auf Informationszugang Informationen veröffentlicht worden seien, die Hinweise zum Bestand an Kunstwerken geben, etwa zu der im Kabinettsaal hängenden Fotografie „Rhein II“ von Andreas Gursky https://www.land.nrw/media/image/fotografie-rhein-ii-von-andreas-gursky. Diese über die Homepage der Staatskanzlei selbst erhältliche Information, in Verbindung mit der etwa unter https://artinfo24.com/kunstmarkt/news-840.html öffentlich zugänglichen Information zum Wert der Fotografie (ca. 4,3 Millionen US-Dollar), könne bereits jetzt dazu missbraucht werden, gegen die Rechtsordnung zu verstoßen, folgte man

den Ausführungen der auskunftspflichtigen Stelle. Von einer konkreten, erstmalig durch die Offenbarung der beantragten Informationen geschaffenen Gefahr für das Schutzgut der öffentlichen Sicherheit könne also nicht ohne Weiteres ausgegangen werden.

Die Staatskanzlei hielt an ihrer Auffassung fest, dass der Informationserteilung Sicherheitsbedenken entgegenstünden. Ergänzend teilte sie mit, dass sich die exemplarisch erwähnte Fotografie aufgrund umfangreicher Renovierungsarbeiten am und im Landeshaus und dadurch bedingter Anwesenheit einer Vielzahl nicht hausangehöriger Personen im Gebäude derzeit nicht in den hiesigen Räumlichkeiten befände.

Antragstellende dürfen nicht mit widerlegbaren Begründungen vom Informationszugang abgehalten werden. Die Verweigerungsgründe des IFG NRW sind eindeutig, eng auszulegen und nicht unendlich dehnbar.

5. Informationsfreiheit hilft gegen Fake News

Rund um die COVID-19-Pandemie kursierten unzählige Falschmeldungen, Fehlinformationen und Verschwörungsmythen. Im Zentrum vieler Desinformationen standen Gerüchte über angebliche Folgen der Impfungen – und vor allem über deren Ausmaß.

Nach dem Infektionsschutzgesetz ist „der Verdacht einer über das übliche Ausmaß einer Impfreaktion hinausgehenden gesundheitlichen Schädigung“ meldepflichtig. In Kenntnis dieser Meldepflicht wollte ein Antragsteller von verschiedenen Gesundheitsämtern in NRW die Anzahl der seit Beginn der COVID-19-Impfkampagne gemeldeten Verdachtsfälle genannt

bekommen. Auch wenn das Interesse an der Information keine Rolle für den Antrag nach dem IFG NRW spielt, ging es ihm nach eigener Aussage dabei vor allem darum, den oben beschriebenen Desinformationen durch belegbare Zahlen entgegen zu wirken.

Wir wurden auf die Anfragen aufmerksam, weil der Antragsteller uns in drei seiner über die Plattform „FragDenStaat“ adressierten Anträge um Vermittlung bat. In allen uns bekannten Fällen erhielt er die beantragten Zahlen von den Gesundheitsämtern; in der Mehrheit auch ohne unsere Vermittlung. Alle angefragten Gesundheitsämter offenbarten die Information und lieferten damit einen wichtigen Beitrag zur Aufklärung und Versachlichung der öffentlichen Diskussion.

Die Informationsfreiheit ist ein probates Mittel zur Abwehr und Entlarvung von Falschmeldungen.

6. Stadt lässt es auf Klage ankommen

Öffentliche Stellen sollten nicht darauf spekulieren, dass Antragstellende das Prozessrisiko scheuen und klaglos auf ihr Recht verzichten. Zum einen widerspricht dies dem Grundsatz der Bindung der Verwaltung an die Gesetze, zum anderen zahlt es sich nicht aus, Antragstellende zu unterschätzen.

In einem konkreten Fall hatte die auskunftspflichtige Stadt zunächst ein ganzes Jahr nicht auf einen Antrag auf Informationszugang reagiert – trotz mehrfachen Nachfragens durch den Antragsteller. Nachdem wir eingeschaltet wurden, reagierte die Stadt zwar endlich, lehnte den Antrag jedoch ab: Dieser sei zu unkonkret.

Der Antragsteller erhob daraufhin Klage auf Informationszugang vor dem Verwaltungsgericht. Binnen zwei Monaten nach Zustellung der Klageschrift stellte die beklagte Stadt den Antragsteller klaglos, indem sie ihm die beantragte Information zukommen ließ. Daraufhin wurde die Klage übereinstimmend für erledigt erklärt, und die Stadt hatte sämtliche Kosten des Verfahrens zu tragen. Dieser Umweg über das Verwaltungsgericht und damit auch die entstandenen Kosten für die Steuerzahler*innen wären durchaus vermeidbar gewesen.

Für Antragstellende ist es unbefriedigend, wenn sie den Eindruck gewinnen müssen, dass sie ihren gesetzlichen Informationsanspruch nur mit Druck durchsetzen können. Eine zeitnahe Bearbeitung von Informationszugangsanträgen auch ohne Klageerhebung ist nicht nur rechtlich geboten, sondern schont auch die knappen Ressourcen der Verwaltungen sowie der Verwaltungsgerichte.

7. Wenn das IFG NRW die Frist von einem Monat setzt, aber die Bearbeitung des Antrags trotzdem ein Jahr dauert…

Urlaubsbedingte Verzögerungen, personelle Umstrukturierungen, Nachfragen bei anderen Stellen im Haus..., dies alles kann dazu führen, dass ein Antrag auf Informationszugang nach dem IFG NRW nicht fristgerecht beantwortet wird. Das sollte jedoch nicht bedeuten, dass die vom Gesetzgeber vorgegebene Monatsfrist grundsätzlich nicht mehr eingehalten werden muss.

Dass informationspflichtige Stellen die gesetzlich vorgeschriebene Monatsfrist für die Bearbeitung eines

Antrags nach dem IFG NRW nicht einhalten, kann viele Gründe haben. Der Gesetzgeber hat in § 5 Abs. 2 IFG NRW aber vorgesehen, dass die beantragte Information „unverzüglich, spätestens innerhalb eines Monats nach Antragstellung“, zugänglich gemacht werden soll. Daher müssen Behörden und andere informationspflichtige Stellen diese Frist grundsätzlich auch einhalten: Im begründeten Ausnahmefall besteht das Recht, hiervon abzuweichen, beispielsweise, wenn die Einwilligung von betroffenen Personen einzuholen ist, eine Nachfrage bei Antragstellenden erforderlich ist oder die zu sichtenden Informationen sehr umfangreich sind. Wenn jedoch die begehrte Information letztlich erst nach mehr als einem Jahr zugänglich gemacht wird und das auch nur, weil wir eine Beanstandung ausgesprochen haben, dann ist das nicht mehr von den gesetzlichen Ausnahmetatbeständen gedeckt.

Im konkreten Fall hatte der Antragsteller bei einem Studierendenwerk den Zugang zu Informationen über den Betrieb der bargeldlosen Kartenaufladung (AUTOLOAD-Verfahren) für den Mensabetrieb beantragt. Obwohl er nach einem Monat an seinen Antrag erinnerte, erhielt er keine Reaktion von der informationspflichtigen Stelle. Er wandte sich daher an uns. Die informationspflichtige Stelle teilte uns im Rahmen eines Auskunftsersuchens und zweier Erinnerungen zwar mit, dass die Bearbeitung aufgrund personeller Wechsel bzw. urlaubsbedingt nicht erfolgen konnte, die erbetenen Informationen bekamen der Antragsteller und wir dennoch nicht. Erst nachdem wir den Vorgang gegenüber der Behörde beanstandeten, erhielt der Antragsteller seine Auskunft.

Eine derart extensive Überschreitung der Monatsfrist zulasten von Antragssteller*innen ist rechtswidrig. Antragstellende können in vergleichbaren Fällen Untätigkeitsklage erheben.

Die Monatsfrist nach dem IFG NRW ist keine bloße Empfehlung. Eine Überschreitung darf nicht die Regel, sondern muss eine Ausnahme bleiben.

8. Wo Verschlusssache draufsteht, ist nicht immer Verschlusssache drin!

Polizeiliche Dienstanweisungen sind häufig als Verschlusssache deklariert. Anträge nach dem IFG NRW können behilflich sein, eine solche Einstufung kritisch zu überdenken, damit polizeiliche Arbeit für Bürger*innen nachvollziehbarer wird.

Ein Antragsteller beantragte gegenüber einem Polizeipräsidium den Zugang zu einer Dienstanweisung zu Kontrollen im ruhenden Verkehr und Verfahren bei Abschleppvorgängen. Der Zugang wurde unter Hinweis auf § 6 IFG NRW abgelehnt. Nach dieser Regelung ist der Antrag auf Informationszugang unter anderem abzulehnen, soweit und solange das Bekanntwerden der Information die öffentliche Sicherheit oder Ordnung, insbesondere die Tätigkeit der Polizei, beeinträchtigen würde (§ 6 Buchstabe a IFG NRW). Die Behörde argumentierte, dass Dienstanweisungen beim Polizeipräsidium als Verschlusssachen NUR FÜR DEN DIENSTGEBRAUCH deklariert seien und das Bekanntwerden demnach die Tätigkeit der Polizei beeinträchtigen könnte. Aus diesem Grund könne die beantragte Information nicht zur Verfügung gestellt werden.

Verschlusssachen sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform (§ 6 Abs. 1 Satz 1 Sicherheitsüberprüfungsgesetz NRW). Die Verschlusssache NUR FÜR DEN DIENSTGEBRAUCH ist nach § 7 Nr. 4 der allgemeinen Verwaltungsvorschrift des Innenministeriums NRW zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung) einzustufen, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann. In der VS-Anweisung werden vier unterschiedliche Geheimhaltungsgrade aufgeführt: 1. STRENG GEHEIM, 2. GEHEIM, 3. VS-VERTRAULICH und 4. VS-NUR FÜR DEN DIENSTGEBRAUCH. Von einer Einstufung als Verschlusssache ist nur der notwendige Gebrauch zu machen (§ 1 VS-Anweisung). In der Anlage 1 zur VS-Anweisung wird zudem darauf verwiesen, dass kritisch zu prüfen ist, ob eine Einstufung als Verschlusssache tatsächlich notwendig ist. Im Falle einer VS-Einstufung muss schlüssig dargelegt werden, welche Gefährdungen, Schäden oder Nachteile für die Bundesrepublik Deutschland oder eines ihrer Länder konkret entstehen können, wenn Unbefugte von den Informationen Kenntnis erhalten. Bereits mit Urteil vom 29. Oktober 2009 hatte das Bundesverwaltungsgericht zu einem Antrag nach dem IFG des Bundes entschieden: „der Anspruch auf Zugang zu einer Information ist nicht allein deshalb nach § 3 Nr. 4 IFG des Bundes ausgeschlossen, weil die Information formal als Verschlusssache eingestuft ist. Vielmehr kommt es darauf an, ob die materiellen Gründe für eine solche Einstufung vorliegen“ (Az. 7 C 21.08).

Im vorliegenden Fall hatte das Polizeipräsidium bei der Ablehnung des Zugangs zu der Dienstanweisung lediglich den Hinweis auf die Verschlusssache angeführt, wonach durch das Bekanntwerden die Tätigkeit der Polizei beeinträchtigt werden könnte. Der Antragsteller wandte sich daraufhin an uns. In unserem Auskunftsersuchen hakten wir nach und wiesen darauf hin, dass eine Ablehnung auf der Grundlage des IFG NRW begründet werden muss und ein Hinweis auf eine Verschlusssache für die Ablehnung allein noch keine ausreichende Begründung sei. Antragstellende müssen nachvollziehen können, weshalb der Zugang zu den begehrten Informationen abgelehnt wird.

Das Polizeipräsidium prüfte aufgrund unseres Auskunftsersuchens die Einstufung der Dienstanweisung als Verschlusssache erneut und kam zu dem Ergebnis, dass die Einstufung als Verschlusssache aufzuheben sei. Der Antragsteller konnte daraufhin die beantragte Information erhalten.

Der Hinweis auf die Einstufung als Verschlusssache allein rechtfertigt nicht die Ablehnung eines Informationszugangs. Diese kann nur auf der Grundlage des IFG NRW erfolgen und ist im konkreten Fall zu prüfen.

9. Umweltinformationen – weil Informationen manchmal nicht gleich Informationen sind!

Die LDI NRW ist für das Umweltinformationsgesetz NRW (UIG NRW) weiterhin nicht zuständig. Da es in NRW jedoch auch keine andere Stelle gibt, die die Bürger*innen in ihrem Informationsrecht nach dem UIG NRW unterstützen kann, versucht die LDI NRW in diesem Bereich zumindest

zwischen Bürger*innen und Behörden zu vermitteln, wenn Antragstellende von informationspflichtigen Behörden keine oder unzureichende Antworten bekommen.

Wir erhalten immer wieder Eingaben von Bürger*innen, die Ansprüche nach dem UIG NRW betreffen. Für das UIG NRW hat die LDI NRW – anders als beim IFG NRW – keine gesetzlich zugewiesene Aufsichtskompetenz. Das bedeutet, dass der LDI NRW die im IFG NRW vorgesehenen Befugnisse beim UIG NRW nicht zur Verfügung stehen. Trotzdem stehen wir grundsätzlich auch in UIG-Fällen Bürger*innen unterstützend zur Seite.

So begehrte ein Antragsteller gegenüber einer Stadt ein Gutachten, das die Ursache für ein großes Fischsterben ermitteln sollte. Da er hierzu trotz mehrfacher Erinnerung keine Antwort erhalten hatte, wandte er sich an uns mit der Bitte um Vermittlung. Der Begriff der Umweltinformation ergibt sich aus § 2 Abs. 3 UIG Bund. Dieser Begriff ist sehr weit auszulegen, wie das Bundesverwaltungsgericht bereits mit Urteil vom 21. Februar 2008 feststellte (Az. 4 C 13.07). Besteht ein grundsätzliches Zugangsrecht nach dem UIG NRW, findet das IFG NRW daneben keine Anwendung.

Im vorliegenden Fall war es offensichtlich, dass mit dem Antrag auf Zugang zu dem Gutachten Umweltinformationen betroffen sind. Unsere Anfrage und mehrfache Nachfragen an die Stadt ergaben schließlich nach über einem Jahr, dass das Gutachten gar nicht vollständig vorlag. Auch wenn der Antragsteller kein Gutachten erhielt, bekam er durch unsere Vermittlung jedenfalls die Auskunft, dass das Gutachten noch nicht fertiggestellt war.

Auf die Lücke der fehlenden Zuständigkeit hatte die Konferenz der Informationsfreiheitsbeauftragten in Deutschland in ihrer Entschließung „Informationsfreiheit – Lücken schließen!“ vom 23. Mai 2011 aufmerksam gemacht. Der Bund und eine Reihe von Ländern haben inzwischen eine gesetzlich zugewiesene Kompetenz für die Gewährleistung des Zugangs zu Umweltinformationen erhalten, jedoch fehlt diese in NRW nach wie vor. Zuletzt berichteten wir im 24. Bericht unter „8. Reformbedarf“, dass für die LDI NRW keine Zuständigkeit in Bezug auf das UIG NRW besteht. In diesem Bereich gibt es seit Bestehen des Gesetzes im Jahr 2007 keine unabhängige Aufsichtsbehörde.

Für Antragstellende ist es letztlich einerlei, welches Recht den Zugang zu den beantragten Informationen regelt. Es wäre daher sinnvoll, eine einheitliche Aufgabenkompetenz für beide Gesetze, das IFG NRW und das UIG NRW, bei der LDI NRW zu verankern. Eine einheitliche Aufgabenwahrnehmung durch die LDI NRW würde die Rechtsanwendung für die auskunftspflichtigen Behörden und für die Anspruchsberechtigten erleichtern. Siehe hierzu 23. Bericht unter „16.2 Transparenzgesetz NRW?“.

Bürger*innen brauchen eine Ombudsstelle auch für die Umweltinformationsfreiheit, damit die LDI NRW sie auch in diesem Bereich effektiv bei der Wahrnehmung ihres Rechts auf Informationszugang unterstützen kann.

10. Unterschiedliches Dateiformat = unterschiedliche Information?

Wurde die beantragte Information Antragsteller*innen bereits zur Verfügung gestellt, kann der Antrag abgelehnt werden. So sieht es das IFG NRW in § 5 Abs. 4 vor. Gilt dieser Ablehnungsgrund auch noch, wenn die Information in einem anderen Dateiformat zugänglich gemacht wurde?

Diese Frage wurde in einem Fall aufgeworfen, in dem wir um Vermittlung gebeten wurden: Eine Stadt hatte den Antrag auf Zugang zu einem Verkehrsplan im CAD-Dateiformat abgelehnt und dies damit begründet, dass derselbe Antragsteller die Information zuvor schon als PDF-Datei erhalten hatte. Um diese Begründung überprüfen zu können, war zunächst eine Beleuchtung der technischen Seite des Falls erforderlich: Worin besteht der Unterschied zwischen einer CAD- und einer PDF-Datei?

Beide Dateiformate unterscheiden sich sowohl hinsichtlich des Verwendungszwecks als auch der Darstellung grundlegend voneinander: CAD steht für „Computer Aided Design“ und bezeichnet die Erstellung von Designs am Computer. Das Zeichnen von Hand wird dabei durch einen automatisierten Prozess ersetzt. Es gibt zweidimensionale und dreidimensionale Dateiformate.

PDF steht für „Portable Document Format" und ist ein vom Gerät sowie Betriebssystem unabhängiges Dateiformat, das in erster Linie für den sicheren Austausch von Dokumenten bestimmt ist.

Die entscheidende Frage in dem konkreten Fall: Handelt es sich bei dem Verkehrsplan – einmal als CAD-,

einmal als PDF-Datei – um ein und dieselbe Information, so dass der zweite Antrag zu Recht nach § 5 Abs. 4 IFG NRW abgelehnt werden konnte? Die Stadt ging zunächst davon aus, dass der Antragsteller die beantragten Informationen zum Inhalt der Verkehrsplanung durch vorherige Übermittlung von PDF-Dateien bereits erhalten habe. Der Antragsteller hielt dagegen: Beide Dateien enthielten nicht dieselbe Information, da die CAD-Datei Markierungen sowie exakte Flächenmaße enthalte und eine Bearbeitung durch zum Beispiel. technische Zeichnungen ermögliche, wohingegen die PDF-Datei über all diese Eigenschaften nicht verfüge.

In dem geschilderten Fall sind wir davon ausgegangen, dass beide Dateien aufgrund der großen Unterschiede der beiden Dateiformate in Bezug auf die optische Darstellung, die Bearbeitbarkeit und den Detailgrad auch inhaltlich unterschiedlich sind und wir es folglich nicht mit einer identischen Information zu tun hatten.

In jedem Einzelfall, dem ein vergleichbarer Sachverhalt zugrunde liegt, dürfte die Frage nach der Unterscheidung zweier Dateiformate zwar eine technische Prüfung nach sich ziehen. Zu berücksichtigen ist dabei, dass das in § 5 Abs. 2 Satz 3 IFG NRW geregelte Recht zur Bestimmung der Art des Informationszugangs auch das Wahlrecht des Dateiformats umfasst.

Anderes Format – andere Information? Die Antwort ist immer abhängig vom Informationsgehalt der zu vergleichenden Dateien. Bleiben am Ende Zweifel über die Identität zweier Informationen, sollte zugunsten des Informationszugangs entschieden werden.

11. Eine teilweise Ablehnung muss begründet werden

Werden in einem Dokument, das im Rahmen eines Antrags auf Informationszugang zugänglich gemacht wird, einzelne Passagen geschwärzt, ist das eine teilweise Ablehnung des IFG-Antrags. Eine solche ist generell nach § 5 Abs. 2 Satz 3 IFG NRW begründungspflichtig.

In unserer Praxis können wir mitunter beobachten, dass auskunftspflichtige Stellen versäumen, eine Ablehnung zu begründen. Dies kann insbesondere dann schnell geschehen, wenn der Anspruch grundsätzlich gewährt wird und etwa ein Dokument, das herausgegeben wird, nur einige wenige Schwärzungen enthält. Solche Schwärzungen, zum Beispiel personenbezogener Daten, bedeuten eine teilweise Ablehnung des Antrags. Für einen solchen Fall sieht das IFG NRW in § 5 Abs. 2 Satz 3 Folgendes vor: „Die Ablehnung eines Antrages nach Abs. 1 oder die Beschränkung des beantragten Zugangs zu einer Information ist schriftlich zu erteilen und zu begründen“.

Auch eine eventuell nur minimale Beschränkung des Antrags muss begründet werden. Hierfür möchten wir auskunftspflichtige Stellen sensibilisieren, die eine Begründung oftmals versehentlich unterlassen.

12. Ein anhängiges Gerichtsverfahren ist kein Ablehnungsgrund

Bei flüchtiger Lektüre des § 6 IFG NRW könnte man zu dem Schluss kommen, ein anhängiges Gerichtsverfahren könnte ein Grund sein, einen Antrag auf Informationszugang abzulehnen. Das ist allerdings nicht so.

Erreicht eine auskunftspflichtige Stelle ein Antrag auf Informationszugang und steht die angefragte Information in Zusammenhang mit einem laufenden Gerichtsverfahren, mag der erste Reflex sein, diesen Antrag abzulehnen. Verstärkt wird dieser Reflex, wenn Antragstellende selbst Partei im Gerichtsverfahren sind und durch die Offenbarung der Information womöglich einen Vorteil im Prozess erlangen könnten.

Schnell ist dann der Ablehnungsgrund des § 6 IFG NRW zur Hand, der den Schutz „öffentlicher Belange und der Rechtsdurchsetzung“ im Titel führt. Gerade der letztgenannte Schutzbereich könnte nach seinem Wortlaut darauf hindeuten, dass ein Ablehnungsgebot auch im Falle einer zu befürchtenden Beeinträchtigung eines anhängigen Rechtsstreits besteht. Liest man jedoch den kompletten Text des § 6 IFG NRW, ist dort unter Satz 1 Buchstabe b die Rede vom Schutz verschiedener Verfahren. Die abschließende Aufzählung umfasst etwa anhängige Verwaltungs- oder Ordnungswidrigkeitenverfahren, jedoch gerade keine Gerichtsverfahren. Dabei ist davon auszugehen, dass es sich bei der Beschränkung auf Verwaltungsverfahren um eine bewusste Entscheidung bei der Gesetzgebung handelte, denn erst durch einen Antrag im parlamentarischen Verfahren wurde das Wort „Verfahren“ zu „Verwaltungsverfahren“ ergänzt.

Abgesehen davon, dass ein anhängiges Gerichtsverfahren nicht von § 6 IFG NRW erfasst ist, gibt es auch keinen anderen Ablehnungsgrund im IFG NRW, den die auskunftspflichtige Stelle hätte heranziehen können. Ein Antrag darf gerade nicht nur deshalb abgelehnt werden, weil er dazu dient, die erhaltenen Informationen in einem Rechtsstreit gegen die auskunftspflichtige Stelle zu verwenden. Im Gegenteil dienen sowohl das IFG NRW als auch ein Rechtsstreit demselben Ziel, nämlich der Überprüfung der Rechtmäßigkeit staatlichen Handelns.

Ein anhängiger Rechtsstreit ist nur auf den ersten Blick ein Ablehnungsgrund. Diese spontane Fehleinschätzung dürfte vor allem dem Impuls geschuldet sein, prozessrelevante Informationen, die zum eigenen Nachteil gereichen könnten, nicht der gegnerischen Partei offenbaren zu wollen. Die abschließenden Ablehnungsgründe in den §§ 6 bis 9 IFG NRW bieten aber keine Grundlage mit dem Verweis auf einen Rechtsstreit eine Information zu verweigern.

13. Warum nicht gleich so? Informationszugang nur über Klageweg

Eine öffentliche Stelle lässt es bei einem Informationsanspruch auf ein Klageverfahren ankommen, obwohl wir sie in einem vergleichbaren Fall bereits darauf hingewiesen hatten, dass das IFG NRW hier Anwendung findet.

Ein Antragsteller beantragte Präsentationsmaterialien zu einem bestimmten Fachseminar des Zentrums für schulpraktische Lehrerausbildung. Der Antrag wurde von der zuständigen Bezirksregierung mit dem Hinweis abgelehnt, dass die begehrten Materialien nicht

auf eine Verwaltungsentscheidung hinführten und sie lediglich in der internen Ausbildung von Lehrkräften am Zentrum für schulpraktische Lehrerausbildung zum Einsatz kämen. Auf den ersten Blick erschien es nachvollziehbar, dass das IFG NRW vorliegend keine Anwendung findet, schließlich gilt es für Verwaltungstätigkeit der im Gesetz genannten Stellen.

Die Bezirksregierung hatte genau den gleichen Antrag schon einmal abgelehnt. Im Vermittlungsverfahren hatten wir darauf hingewiesen, dass nach der Rechtsprechung der Begriff „Verwaltungstätigkeit“ weit auszulegen ist und die Verwaltung sowohl im formellen als auch im materiellen Sinne umfasst. Das OVG NRW stellte in seinem Urteil vom 7. Oktober 2010, Az. 8 A 875/09, Rdnr. 38 klar: „… Darunter wird die gesamte Tätigkeit der Exekutive verstanden, unabhängig davon, ob es sich um eine Tätigkeit materiell verwaltender Art handelt. Entscheidend ist die Einordnung des Handelnden in den Staatsaufbau. Ausgehend davon liegt eine Verwaltungstätigkeit dann vor, wenn eine Stelle aus dem Bereich der Exekutive und nicht der Legislative oder Judikative tätig wird. …“. Wir wiesen die Bezirksregierung darauf hin, dass es nicht darauf ankommt, dass die begehrte Information zu einer Verwaltungsentscheidung hinführt. Ausreichend sei, dass die Stelle, die über die Information verfügt, der Exekutive zugeordnet ist. Unbeachtlich war, dass es sich um Informationen handelte, die lediglich in der internen Ausbildung von Lehramtskräften am Zentrum für schulpraktische Lehrerausbildung zum Einsatz kommen.

Dennoch blieb die Bezirksregierung bei ihrer Auffassung. Sie lehnte den gleichlautenden Antrag erneut ab. Der Antragsteller erhob daraufhin Klage mit Hilfe

der Plattform Fragdenstaat.de vor dem Verwaltungsgericht. Die öffentliche Stelle schaltete in dem Verfahren eine Anwaltskanzlei ein. Offensichtlich wurde der Sachverhalt daraufhin anders bewertet, da die Bezirksregierung noch vor einer Verhandlung durch eine Übersendung der Präsentationsmaterialien den Antragsteller klaglos stellte.

Der Antragsteller hat zwar die begehrten Informationen erhalten, jedoch wurden aufgrund der Verweigerungshaltung der informationspflichtigen Stelle unnötige Kosten verursacht. Leider müssen wir häufiger feststellen, dass zweifellos bestehende gesetzliche Informationsansprüche nur unter Druck, nämlich im Klageverfahren durchgesetzt werden können. Hierzu hatten wir bereits im 26. Bericht, 2.Teil Informationsfreiheitsbericht unter 10. berichtet („Stadt lässt es auf Klage ankommen“).

Bei eindeutiger, gerichtlich bestätigter Rechtslage ist nicht nachzuvollziehen, weshalb gesetzliche Informationsansprüche erst verweigert und im Klageverfahren dann doch erfüllt werden. Dies alles geschieht letztlich auf Kosten der Allgemeinheit.

14. Gebühren – alles andere als simpel

Ist die Bereitstellung von Informationen mit einem umfangreichen Verwaltungsaufwand verbunden, sieht § 11 IFG NRW in Verbindung mit der Verwaltungsgebührenordnung zum IFG NRW hierfür eine Gebühr vor. Allerdings lauern rund um das Thema „Gebühren“ einige Fallstricke. Hier noch einmal die wichtigsten Hinweise, um diese Fallstricke zu vermeiden:

1. Bevor ein Gebührenbescheid erlassen wird, müssen Antragstellende nach § 28 Abs. 1 VwVfG NRW angehört werden.
2. Für die Berechnung der Stundensätze können die im Runderlass des Ministeriums für Inneres und Kommunales vom 8. August 2016 „Richtwerte für die Berücksichtigung des Verwaltungsaufwandes bei der Festlegung der nach dem Gebührengesetz für das Land NRW zu erhebenden Verwaltungsgebühren“ (MBl. NRW. Ausgabe 2016 Nr. 22 vom 26.8.2016 Seite 491 bis 510 | /RECHT.NRW.DE) genannten Werte zugrunde gelegt werden.
3. Die Struktur der Gebührenziffern ist komplex. Die Gebühr wird in einem zweistufigen Verfahren ermittelt. Zuerst wird der Gebührenrahmen bestimmt, anschließend die konkrete Gebühr innerhalb des Rahmens. Die Festsetzung der Gebührenhöhe innerhalb des Gebührenrahmens ist eine Ermessensentscheidung, die immer dann notwendig wird, wenn im Gebührenrahmen nicht lediglich die Mindestgebühr festgesetzt wird (vgl. Beschluss des OVG NRW vom 12. April 2017, Az. 9 B 384/17). Der Bescheid muss konkrete

und nachvollziehbare Ausführungen zum Gebührenrahmen und zur Gebührenhöhe enthalten: Weshalb etwa handelt es sich um einen umfangreichen Verwaltungsaufwand? Wie wurde die Gebühr konkret berechnet? Welcher Aufwand ist wofür in welcher Zeit entstanden? Welche einzelnen Arbeitsschritte waren erforderlich? Siehe zur Vertiefung das Urteil des Verwaltungsgerichts Arnsberg vom 4. Mai 2020, Az. 11 K 1503/19 und 26. Bericht 2. Teil Informationsfreiheit unter Nr. 7.

4. Wie hoch die Gebühr im konkreten Fall ist, bestimmt sich auch nach dem sog. Äquivalenzprinzip. Danach muss ein angemessenes Verhältnis zwischen der Gebühr und dem Wert der von der Behörde erbrachten Leistung bestehen. Für die Ermittlung der Höhe der festzusetzenden Gebühren darf der Verwaltungsaufwand nicht der alleinige Maßstab sein.
5. Die Erstattung von Auslagen nach § 11 Abs. 2 IFG NRW in Verbindung mit § 3 VerwGebO IFG NRW ist nicht verfassungsgemäß (siehe Urteil des Bundesverwaltungsgerichts vom 20. Oktober 2016, Az. 7 C 6.15). Allerdings hat der nordrhein-westfälische Gesetzgeber den Mangel bislang noch nicht behoben, obwohl die LDI NRW bereits im 24. Bericht, 2. Teil Informationsfreiheit unter Nr. 6 darauf hingewiesen hatte.
6. Grundsätzlich dürfen im Zusammenhang mit Informationszugangsanträgen keine Gebühren im Voraus erhoben werden.

Aus der zu IFG-Gebühren vorliegenden Rechtsprechung geht einheitlich hervor, dass der mit der Bearbeitung des Antrags entstandene Aufwand konkret und nachvollziehbar darzulegen ist.

Anhang zum Datenschutzbericht

Veröffentlichungen der Datenschutzkonferenz 2022

Neben den hier abgedruckten Entschließungen und Beschlüssen der Datenschutzkonferenz sind alle weiteren Veröffentlichungen auf der Homepage der Datenschutzkonferenz www.datenschutz-konferenz-online.de abrufbar.

Entschließungen der Datenschutzkonferenz 2022

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

- **24.11.2022 – Petersberger Erklärung zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung**

  Vorbemerkung

  Die wissenschaftliche Forschung mit Gesundheitsdaten, also mit Informationen über den Gesundheitszustand von Personen, kann dazu dienen, Erkenntnisse über die Ursachen von Krankheiten zu gewinnen, effiziente Therapien zu entwickeln und Behandlungsmöglichkeiten zu verbessern.

  Damit steht sie im essentiellen Interesse der Allgemeinheit und sollte gerade bei der Verfolgung dieser Ziele bestmöglich gefördert werden. Allerdings ist dabei zu beachten, dass die hierfür relevanten Datenkategorien von der europäischen Datenschutz-Grundverordnung (DSGVO) in besonderer Weise geschützt werden und einem besonders hohen Schutzbedarf unterliegen. Eine unsachgemäße Verwendung sensibler Gesundheitsdaten kann zu gravierenden Folgen führen, wie z. B. soziale Stigmatisierung

oder sogar Diskriminierung für die betroffenen Personen etwa auf dem Arbeits- und Versicherungsmarkt.

Datenverarbeitung für Zwecke der wissenschaftlichen Forschung genießt schon heute in der Datenschutz-Grundverordnung und den nationalen Datenschutzgesetzen eine weitgehende Privilegierung. Es ist daher eine wichtige Herausforderung, Wege und Lösungen zu finden, um die Verarbeitung von Gesundheitsdaten zu im öffentlichen Interesse liegenden wissenschaftlichen Forschungszwecken zu ermöglichen und ihre Vorzüge nutzbar zu machen. Gleichzeitig ist den damit verbundenen Risiken konsequent zu begegnen, um den Betroffenen einen adäquaten Grundrechtsschutz zu gewähren.

Mit begründetem Vertrauen der betroffenen Personen in die Einhaltung ethischer, rechtlicher und technischer Standards wächst ihre Motivation, die Forschung zu unterstützen. Deshalb ist es für Bürgerinnen und Bürger unerlässlich, darauf vertrauen zu können, dass ihre personenbezogenen Daten im Einklang mit den sie schützenden datenschutzrechtlichen Vorgaben und unter Wahrung ihrer informationellen Selbstbestimmung verarbeitet werden. Auch deshalb ist Datenschutz eine Voraussetzung für eine menschenzentrierte wissenschaftliche Forschung mit Gesundheitsdaten.

Grundlage für eine solche datenschutzkonforme effektive Gesundheitsdatenforschung ist neben einer weitreichenden Transparenz vor allem eine hohe Rechtsklarheit für alle Beteiligten sowie die Sicherstellung eines nachhaltigen Schutzes personenbezogener Daten, wie bereits in ihrer Entschließung vom 23. März 2022 „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz“ von der DSK gefordert.

In Konkretisierung dieser Forderungen hat sich die DSK auf die folgenden Empfehlungen im Zusammenhang mit der Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung verständigt:

- **Die Menschen stehen im Mittelpunkt der Forschung. Sie dürfen nicht zum bloßen Objekt der Datenverarbeitung gemacht werden. Entsprechende Verarbeitungsprozesse müssen daher rechtmäßig sowie für betroffene Personen stets transparent und nachvollziehbar sein. Auch wenn eine Verarbeitung ihrer Daten im öffentlichen Interesse gesetzlich erlaubt und nicht auf ihre Einwilligung gestützt wird, sind die betroffenen Personen in geeigneter Form einzubinden. Digitale Managementsysteme sollen Informations-, Kontroll- und Mitwirkungsmöglichkeiten sicherstellen. Gesetzliche Regelungen müssen wirksam den Schutz des Rechts auf informationelle Selbstbestimmung der betroffenen Personen gewährleisten und die datenschutzrechtlichen Anforderungen des europäischen und nationalen Datenschutzes erfüllen.**
- **Es gilt der Grundsatz: Je höher der Schutz der betroffenen Personen durch geeignete Garantien und Maßnahmen, desto umfangreicher und spezifischer können die Daten genutzt werden.**
- **Zu den grundlegenden Garantien und Maßnahmen gehören die Verschlüsselung, die Pseudonymisierung durch eine Vertrauensstelle und die frühestmögliche Anonymisierung. Zusätzlich sind besondere Anforderungen bei Verarbeitungen in Drittländern zu beachten. Anonyme Datensätze, die die Re-Identifikation auch für Personen mit Zusatzwissen irreversibel ausschließen, können Forschende umfassend nutzen.**
- **Auswertungen anhand von Falldaten greifen insbesondere dann besonders tief in die Rechte und Freiheiten der betroffenen Personen ein, wenn Datensätze aus verschiedenen Quellen verknüpft werden. Daher müssen die Art und der Umfang der Bereitstellung, der Zweck der Auswertung und die Forschenden persönlich besondere Schutzanforderungen erfüllen. Geeignete Verfahren**

müssen gewährleisten, dass rechtliche und technische Voraussetzungen für den Datenzugang erfüllt sind. Die datenschutzrechtliche Verantwortlichkeit ist lückenlos festzulegen, damit betroffene Personen ihre Datenschutzrechte ausüben können.

- **Mit einem zentralen Registerverzeichnis sollten die Nutzung der in den verschiedenen Registern gespeicherten Daten für alle Beteiligten transparent gestaltet und mehrfache Datensammlungen vermieden werden. Dabei sind Qualitätsanforderungen verbindlich vorzugeben, zu prüfen und auszuweisen. Zudem sollte eine zentrale koordinierende Stelle mit Lotsenfunktion geschaffen werden, die Datennutzungsanträge veröffentlicht und die Nutzenden zur Publizierung der Forschungsergebnisse in anonymer Form verpflichtet. Dies schafft sowohl Wissen im Allgemeininteresse als auch Schutz für die betroffenen Personen.**
- **Durch eine gesetzliche Regelung des Forschungsgeheimnisses ist der Umgang mit personenbezogenen medizinischen Forschungsdaten für wissenschaftlich Forschende auch in strafrechtlicher und prozessualer Sicht klarzustellen und damit ein wichtiger Beitrag zum Schutz dieser Daten zu leisten.**
- **Die Datenschutzbehörden müssen die Einhaltung datenschutzrechtlicher Anforderungen umfassend und effektiv überwachen und durchsetzen können. Hierfür ist auch erforderlich, gegenüber öffentlichen Stellen den sofortigen Vollzug von Maßnahmen anordnen zu können. Zur Erleichterung der Kontrolle sollten standardisierte Anforderungen u.a. an die Dokumentation der Datenverarbeitungsprozesse festgelegt werden.**

Grundlage für die Datenverarbeitung

Generell gilt: Die Einzelperson darf nicht zum bloßen Objekt der Datenverarbeitung gemacht werden.

Ungeachtet der gesondert zu führenden Diskussionen zum europäischen Gesundheitsdatenraum und zur Nutzung von Gesundheitsdaten zu Forschungszwecken auf europäischer Ebene, besteht nach Auffassung der DSK auch auf nationaler Ebene Bedarf, die Regelungen für die Nutzung von Forschungsdaten näher zu spezifizieren und kohärent auszugestalten. Ziel dabei sollte eine länderübergreifende, einheitliche Regelung zur Verarbeitung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken sein, die Forschungsverbünden mit Partnern in unterschiedlichen Bundesländern das Einhalten der datenschutzrechtlichen Anforderungen erleichtert.

Soweit Ärztinnen und Ärzte und andere Berufsgeheimnisträger ermächtigt werden sollen, personenbezogene Daten zu Forschungszwecken zu übermitteln, muss die Regelung mit dem Berufsrecht in Einklang stehen.

Die datenschutzrechtliche Einwilligung als Grundlage für die Datennutzung kann dem hohen Gut des Rechts auf informationelle Selbstbestimmung unmittelbar Ausdruck verleihen. Sie muss freiwillig erfolgen, setzt eine umfassende Information voraus und ist jederzeit widerruflich.

Es ist Aufgabe des Gesetzgebers, im Allgemeininteresse liegende Forschung mit Gesundheitsdaten zu ermöglichen, aber auch ihre Grenzen festzulegen und die Interessen der betroffenen Personen zu wahren. Der Gesetzgeber darf diese komplexen Fragestellungen nicht vollständig auf die betroffenen Personen und die Forschenden verlagern.

Sofern eine gesetzliche Regelung Rechtsgrundlage einer Datenverarbeitung zu Forschungszwecken sein soll, muss sie in jedem Fall normenklar wirksam den Schutz des Rechts auf informationelle Selbstbestimmung der betroffenen Personen gewährleisten und die datenschutzrechtlichen Anforderungen des europäischen und nationalen Datenschutzes erfüllen. Eine solche Regelung

kann bei der Nutzung von Daten aus anderen Quellen, beispielsweise Behandlungsdaten aus Krankenhäusern, aus medizinischen Registern oder auch aus anderen Forschungsprojekten (sog. Sekundärnutzung) datenschutzkonforme Forschung ermöglichen oder erleichtern, wenn das Einholen einer ausdrücklichen Einwilligung nicht durchführbar wäre oder das Forschungsvorhaben ernsthaft beeinträchtigen würde.

Zweck der wissenschaftlichen Forschung

Eine gesetzliche Grundlage für die Nutzung von Gesundheitsdaten zu wissenschaftlichen Forschungszwecken muss einen Ausgleich insbesondere zwischen den verfassungsrechtlich geschützten Interessen schaffen: dem Recht der betroffenen Personen auf Kontrolle über ihre Daten (sog. „informationelles Selbstbestimmungsrecht“) einerseits und der Forschungsfreiheit der Wissenschaftler und wissenschaftlichen Einrichtungen andererseits.

Eine gesetzliche Grundlage für die Verarbeitung personenbezogener Daten zu Forschungszwecken sollte im Rahmen der Interessenabwägung u.a. Gemeinwohlinteressen – insbesondere das öffentliche Interesse an den Erkenntnissen und den Nutzen für die Allgemeinheit – berücksichtigen. Es bedarf der näheren Bestimmung durch den Gesetzgeber, was inhaltlich der 6

Forschung im Gemeinwohlinteresse entspricht und welche weiteren Anforderungen an das Verfahren und die Durchführung der Forschung gestellt werden.

Geeignete Garantien für die Rechte und Freiheiten betroffener Personen

Eine gesetzliche Grundlage für die Verarbeitung von Gesundheitsdaten muss angemessene Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen enthalten.

Die Privilegierung der Forschung als Zweck der Verarbeitung personenbezogener Daten in der Datenschutz-Grundverordnung wird flankiert von zusätzlichen Anforderungen, vor allem zur Datenminimierung und zur frühestmöglichen Anonymisierung. Da die Anonymisierung den besten Schutz für die Rechte und Freiheiten der betroffenen Personen bietet, ist die Umsetzung dieser Schutzmaßnahme immer vorrangig zu prüfen.

Soweit der Forschungszweck mit anonymisierten Daten erreicht werden kann, dürfen nur anonymisierte Daten verarbeitet werden. Dabei bestehen hohe Anforderungen an die Anonymisierung personenbezogener Daten. Soweit zur Erreichung des Forschungszwecks eine vollständige Anonymisierung nicht möglich ist, sind effektive Maßnahmen der Pseudonymisierung vorzusehen. Darüber hinaus sind technische und organisatorische Schutzmaßnahmen entsprechend dem für die bei Gesundheitsdaten gesteigerten Anforderungen gemäß dem Stand der Technik zu treffen, darunter solche zur Pseudonymisierung und Verschlüsselung der Daten.

Falls Datenverarbeitungen auch in Ländern außerhalb des Europäischen Wirtschaftsraums stattfinden sollen, entstehen dadurch Risiken, denen mit besonderen Garantien zu begegnen ist. Dies ist nach der DSGVO gewährleistet mit Beschlüssen nach Art. 45 DSGVO und bei Garantien nach Art. 46 DSGVO einschließlich gebotener ergänzender Maßnahmen. Auch in allen anderen Fällen sollten Pseudonymisierungen oder Verschlüsselungen ausschließen, dass die Daten im Drittland einer spezifischen Person zugeordnet werden können.

Pseudonymisierung durch Vertrauensstellen

Die Aufgabe der Pseudonymisierung der Gesundheitsdaten sollte gesetzlich an unabhängige und eigenverantwortliche Vertrauensstellen übertragen werden. Dafür ist entscheidend, diese Stellen völlig unabhängig auszugestalten und insbesondere Weisungen

von wissenschaftlich Forschenden bzgl. der von den Vertrauensstellen verarbeiteten Daten auszuschließen. Die konkreten Aufgaben, Rechte und Pflichten der Vertrauensstellen sind zu definieren. Je nach Ausgestaltung ist zudem die eigene Verantwortlichkeit dieser Stellen für die Datenverarbeitung im Interesse der Wahrung der Betroffenenrechte festzulegen.

Kontrolle durch die betroffenen Personen: Mitwirkung und Widerspruch

Will der Gesetzgeber die Verarbeitung zu Forschungszwecken nicht auf eine Einwilligung, sondern auf eine gesetzliche Grundlage stellen, sollte er die Einbindung der betroffenen Personen vorsehen. Dabei ist zumindest sicherzustellen, dass die betroffene Person in der Regel einer Verarbeitung der personenbezogenen Daten zu Forschungszwecken voraussetzungslos widersprechen kann. Ausnahmen können nur für gesetzlich konkret bestimmte Einzelfälle vorgesehen werden, wenn dieses Recht den Forschungszweck unmöglich macht oder ernsthaft beeinträchtigt. Das Verfahren ist so auszugestalten, dass der Widerspruch möglichst unkompliziert ausgeübt werden kann.

Die betroffenen Personen müssen über die Verarbeitungsschritte informiert werden sowie Gelegenheit erhalten, sich leicht zu informieren. Digitale Methoden oder Managementsysteme, wie Datencockpit, Dashboard oder Portal, sollen dabei Information, Kontrolle und Mitwirkung vereinfachen, indem sie Nachrichten übermitteln und digitale Einwilligungserklärungen zulassen. Durch entsprechende Vorgaben sollten Lösungen erreicht werden, die Bürgerinnen und Bürgern einheitliche und leicht zugängliche Wege bieten, ihre Kontrollrechte auszuüben.

Sichere Datenbereitstellung

Zunächst ist ein Verfahren festzulegen, in dem zuverlässig überprüft werden kann, ob ein Zugriff auf die Daten datenschutzrecht-

lich zulässig ist (Use-and-Access-Verfahren). Bei der Bereitstellung von personenbezogenen Daten für Forschende müssen besondere technische und organisatorische Anforderungen vorgeschrieben werden. So sollte ein Zugang zu den Daten vorrangig in einer sicheren Umgebung der Zugangsstelle vorgesehen werden. Ein Zugriff oder Abruf sollte nur dann möglich sein, wenn Forschende zuvor nachweisen, dass sie angemessene technische und organisatorische Maßnahmen implementiert haben und den Stand der Technik einhalten.

Um den Verantwortlichen Hilfestellung zur Beachtung einheitlicher Mindeststandards zu geben, sollten generelle Risiken der Verarbeitung im Wege einer gesetzlichen Datenschutz-Folgenabschätzung ermittelt und berücksichtigt sowie grundlegende Maßnahmen zur Risikominimierung unmittelbar gesetzlich geregelt werden. Unabhängig davon ist von den Verantwortlichen eine Datenschutz-Folgenabschätzung für jeweils bevorstehende Forschungsvorhaben durchzuführen.

Verknüpfung von Datensätzen

Sofern eine gesetzliche Grundlage geschaffen werden sollte, um Datensätze aus verschiedenen Quellen, beispielsweise aus medizinischen Registern, zu verknüpfen, sind besondere Sicherheits- und Schutzmaßnahmen vorzusehen. Die Verknüpfung erhöht das Risiko für die Rechte und Freiheiten natürlicher Personen, wenn sie anhand der zusammengeführten Informationen leichter zu identifizieren sind. Sie verstärkt darüber hinaus das Risiko, dass Zweckbindungen nicht eingehalten werden, dass zusätzliche, nicht zur Erreichung des Forschungszwecks erforderliche Informationen in einer für die betroffenen Personen wenig überschaubaren Weise generiert oder auch unrichtige Informationen erzeugt werden. Es sind besondere Record-Linkage-Verfahren vorzusehen, die nur eine anlassbezogene und temporäre Zusammenführung zulassen sollten. Die betroffenen Personen sollten über ein Einwilligungsmanagementsystem die Gelegenheit haben, in Kenntnis der Risiken der Zusammenführung

aktiv zuzustimmen. Alternativ müssen technische Methoden oder Maßnahmen sicherstellen, dass die Reidentifizierung der betroffenen Person trotz der Verkettung ausgeschlossen ist.

Bei der Verarbeitung von Daten zu Forschungszwecken muss stets unter Beachtung der vorliegenden Risiken geprüft werden, ob und inwieweit Daten zentral oder dezentral gespeichert oder verarbeitet werden. Soweit dies vom Forschungszweck her möglich ist, sollten die Daten am Ort der Speicherung ausgewertet werden, so dass den Ort der sicheren Speicherung nur anonyme Ergebnisse der Datenauswertung verlassen. Dabei ist eine Mehrfachspeicherung zu vermeiden.

Partizipation und Teilnahme

Im Zusammenhang mit der Gesundheitsforschung gibt es bereits vielfältige Ansätze zur Partizipation der betroffenen Personen. Einige Forschungsvorhaben und Register ermöglichen den betroffenen Personen, sich über Vorhaben und daraus resultierende Erkenntnisse z. B. zu Behandlungsalternativen oder Therapien zu informieren, darüber zu diskutieren und sich bestimmte Forschungsthemen zu wünschen. Diese Partizipation sollte gesetzlich verankert werden.

Denkbar sind Webportale mit weiterführenden Informationen über konkrete Forschungsprojekte sowie einzelne darauf bezogene Krankheitsbilder und in diesem Zusammenhang stehende Therapieziele, Diskussionsforen, Newsletter oder Veröffentlichungen von Datenauswertungen.

Klare Verantwortlichkeiten

Die DSK empfiehlt, gesetzlich zu bestimmen, wer datenschutzrechtlich für einzelne Verarbeitungsschritte verantwortlich ist. Die datenschutzrechtliche Verantwortlichkeit ist lückenlos zu regeln, insbesondere bei der Übermittlung zwischen Forschungseinrichtungen, um sicherzustellen, dass die betroffenen

Personen ihre Datenschutzrechte ausüben können. Es sind rechtsklare Regelungen zur Aufbewahrungsdauer und Löschung von Forschungsdaten festzulegen, die sowohl das Recht auf informationelle Selbstbestimmung der betroffenen Personen als auch das Interesse der wissenschaftlichen Forschung an einer späteren Überprüfbarkeit der Forschungsergebnisse berücksichtigen. Die aus Sicht des Datenschutzes besonders relevanten Instrumente der Verschlüsselung, Pseudonymisierung und Anonymisierung sollten vom Gesetzgeber präzisiert werden. 10

Daten aus medizinischen Registern

Eine gesetzliche Regelung zur Nutzung von personenbezogenen Daten für Forschungszwecke sollte zudem spezifische Vorgaben für medizinische Register schaffen. Sie sollte einheitliche Anforderungen für die Datenverarbeitung in den Registern enthalten.

Hierzu sollte zunächst ein laufendes, zentrales Verzeichnis der bestehenden Register im Gesundheitsbereich errichtet werden, um eine strukturierte Übersicht über vorhandene Daten zu bieten. Dies schafft für die betroffenen Personen ebenso wie für die Forschenden Transparenz. Zugleich vermeidet dies mehrfache Datensammlungen mit gleichen Inhalten und fördert so den Grundsatz der Datenminimierung.

Weiter sind Standards für die Qualität medizinischer Register und der dortigen Verarbeitung festzulegen, die auch Vorgaben zum Datenschutz und zur Datensicherheit enthalten müssen. So sollten die von den Registern einzuhaltenden technisch-organisatorischen Maßnahmen harmonisiert werden. Zugleich sollte ein Verfahren vorgesehen werden, mit dem die Einhaltung dieser Standards – in regelmäßigen Abständen wiederholt – geprüft und nachgewiesen wird.

Eine Datenverarbeitung in den Registern ist stets nur zulässig, wenn die Einhaltung der datenschutzrechtlichen Vorgaben ge-

währleistet ist. Eine Befugnis zur Übermittlung von personenbezogenen Daten, insbesondere Patientendaten, in ein Register setzt dabei mindestens die normenklare Definition des Datenkranzes und die Erforderlichkeit der Erfassung aus medizinisch-fachlicher Sicht voraus. Eine ausdrückliche Meldepflicht ist nur in besonderen Ausnahmefällen denkbar und muss aus verfassungsrechtlichen Gründen gesetzlich festgelegt sein.

Sollte eine zentrale, koordinierende Stelle vorgesehen werden, könnte diese hinsichtlich der Betroffenenrechte eine Beratungs- und Lotsenfunktion wahrnehmen. Um die zuverlässige Durchführung dieser Aufgaben zu gewährleisten, ist eine öffentliche Stelle hiermit zu betrauen und die datenschutzrechtliche Verantwortlichkeit der Stelle ebenso wie die datenschutzrechtliche Aufsicht eindeutig festzulegen.

Normenklare Regelung eines Forschungsgeheimnisses

Bereits mit ihrer Entschließung im Jahr 2004 hat die 67. DSK die Einführung eines Forschungsgeheimnisses gefordert und diese Forderung im März 2022 bekräftigt. Hierdurch sollte die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe gestellt, deren Beschlagnahme verboten und ein Zeugnisverweigerungsrecht für wissenschaftlich Forschende und ihre Berufshelfer geschaffen werden. Die DSK erinnert eindringlich an diese Forderung und ist bereit, entsprechende Vorhaben beratend zu begleiten.

Überwachung und Aufsicht

Die unabhängigen Datenschutz-Aufsichtsbehörden müssen die Einhaltung der datenschutzrechtlichen Regelungen zur Verarbeitung personenbezogener Gesundheitsdaten im Forschungskontext lückenlos überwachen und durchsetzen können. Sie müssen auch gegenüber öffentlichen Stellen mit Befugnissen ausgestattet werden, erforderliche Anordnungen durchsetzen zu können. Dazu gehört auch die - europarechtlich ohnehin gebotene und in

Deutschland bisher ausgeschlossene - Möglichkeit, sofortigen Vollzug von Maßnahmen anordnen zu können.

Um eine effektive und konstruktive Aufsicht zu gewährleisten, sind konkrete Anforderungen an die prüffähige Dokumentation der Verarbeitungsschritte und die zu implementierenden technischen und organisatorischen Maßnahmen vorzusehen. Ebenso sind die forschenden Einrichtungen mit ausreichendem datenschutzrechtlichen Sachverstand auszustatten.

- **29.04.2022 – Die Zeit für ein Beschäftigtendatenschutzgesetz ist „Jetzt“!**

  Die voranschreitende technische Entwicklung ermöglicht eine immer weitergehende Überwachung von Beschäftigten. Deshalb forderte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) bereits 2014 die Schaffung eines Beschäftigtendatenschutzgesetzes.[1]

  Die sich dynamisch entwickelnde Digitalisierung führt zu tiefgreifenden Veränderungen in der Arbeitswelt. Auch vor diesem Hintergrund hat das Bundesministerium für Arbeit und Soziales (BMAS) den interdisziplinären Beirat Beschäftigtendatenschutz eingesetzt, der seinen Abschlussbericht im Januar 2022 fertiggestellt hat. Auch er kommt darin zu dem Schluss, dass – neben weiteren Maßnahmen – ein eigenständiges Beschäftigtendatenschutzgesetz notwendig ist.[2]

  Das europäische Recht ermöglicht es den Mitgliedstaaten spezifischere Regelungen für die Verarbeitung von Beschäftigtendaten zu schaffen. Eine erste Regelung hat der deutsche Gesetzgeber

[1] Entschließung vom 27. März 2014, abrufbar unter: https://www.datenschutzkonferenz-online.de/me-dia/en/20140327_en_Beschaeftigtendatenschutzgesetz.pdf..
[2] Beiratsbericht, S. 6, 9, abrufbar unter: https://www.bmas.de/SharedDocs/Downloads/DE/Arbeitsrecht/ergeb-nisse-beirat-beschaeftigtendatenschutz.pdf;jsessionid=0A2E14EA95F12CD2F926680929CDC8C5.delivery2-mas-ter?__blob=publicationFile&v=3).

mit Erlass des § 26 Bundesdatenschutzgesetz (BDSG) getroffen und sich zugleich weitergehende Regelungen ausdrücklich vorbehalten (BT-Drs. 18/11325, S. 97). Die DSK begrüßt, dass sich im Koalitionsvertrag auf Bundesebene explizit zur Schaffung von Regelungen zum Beschäftigtendatenschutz bekannt wird (Koalitionsvertrag „Mehr Fortschritt wagen“, S. 17).

Die DSK ist der Auffassung, dass weitergehende Regelungen notwendig und überfällig sind: § 26 BDSG ist nicht hinreichend praktikabel, normenklar und sachgerecht[1]. Die Norm ist als Generalklausel formuliert und eröffnet weite Interpretationsspielräume. Dadurch führt sie zu Unklarheiten über die Zulässigkeit von Verarbeitungen personenbezogener Daten im Beschäftigungskontext für Arbeitgeberinnen und Arbeitgeber, Beschäftigte, Bewerberinnen und Bewerber, Personalvertretungen oder Gerichte.

Gerade im Zeitalter der Digitalisierung muss ein Beschäftigtendatenschutzgesetz hinreichend flexibel sein, ein hohes Datenschutzniveau gewährleisten sowie Rechtsklarheit für alle Akteure der Arbeitswelt ermöglichen. Zudem hat es insbesondere vor dem Hintergrund der Risiken technischer Entwicklungen einen angemessenen Ausgleich zwischen den grundrechtlich geschützten Interessen der Arbeitgeberinnen und Arbeitgeber sowie dem Recht auf informationelle Selbstbestimmung der Beschäftigten zu schaffen.

Daher fordert die DSK den Gesetzgeber auf, im Rahmen eines eigenständigen Beschäftigtendaten-schutzgesetzes mindestens in den folgenden Bereichen gesetzliche Regelungen zu schaffen:

- **Einsatz algorithmischer Systeme einschließlich Künstlicher Intelligenz (KI)**

[1] S. Stellungnahme der DSK zur Evaluierung des BDSG vom 2.3.2021, S. 8 f., abrufbar unter: https://www.daten-schutzkonferenz-online.de/media/st/20210316_DSK_evaluierung_BDSG.pdf .

Die Grenzen und Rahmenbedingungen des Einsatzes algorithmischer Systeme im Beschäftigungs- und Bewerbungskontext sollten gesetzlich geregelt werden. Dabei spielt die Schwere, Tiefe und Breite der Grundrechtseingriffe, die der Einsatz algorithmischer Systeme im Beschäftigungskontext typischerweise verursacht, eine wesentliche Rolle. Zudem sind die Hambacher Erklärung der DSK[1] und die von der Datenethikkommission entwickelte „Kritikalitätspyramide“[2] zu berücksichtigen. Je höher die „Kritikalität“, also das Schädigungspotential eines algorithmischen Systems ist, desto strenger sind demnach die Anforderungen an dessen Einsatz. Im Beschäftigungs- und Bewerbungsverhältnis fallen zahlreiche aussagekräftige Daten an. Die Beschäftigten sowie Bewerberinnen und Bewerber sind wegen ihres Abhängigkeitsverhältnisses besonders schutzbedürftig. Zugleich sollen alle Beteiligten von den Chancen des KI-Einsatzes profitieren können. Korrektur- und Kontrollinstrumente wie Zulassungsverfahren, Vorabprüfungen, Antidiskriminierungs- oder Transparenzvorgaben sowie verbesserte Möglichkeiten der Rechtsdurchsetzung bedürfen daher gesetzlicher Normierung. Besonders eingriffsintensive Datenverarbeitungen sollten verboten werden: So fordert die DSK, auch im Beschäftigungskontext die Profilbildung als solche dem Verbot mit Erlaubnisvorbehalt des Artikels 22 der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO) zu unterstellen. Es hat sich gezeigt, dass Artikel 22 DS-GVO, dessen Wortlaut nur automatisierte Entscheidungen verbietet, im Beschäftigungskontext nicht ausreichend Schutz gewährleistet. Zum Schutz der betroffenen Bewerberinnen und Bewerber sowie Beschäftigten ist darüber

[1] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklae-rung.pdf.
[2] Gutachten der Datenethikkommission, S. 177 ff., abrufbar unter: https://www.bmi.bund.de/Shared-Docs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommis-sion.pdf?__blob=publicationFile&v=6.

hinaus regelmäßig der Einsatz von KI im Beschäftigungskontext auf der Grundlage einer Einwilligung zu untersagen.

- **Grenzen der Verhaltens- und Leistungskontrolle**

Die Grenzen der Verhaltens- und Leistungskontrolle bedürfen gesetzlicher Eckpunkte.

Heimliche Kontrollen im Beschäftigungsverhältnis oder Dauerüberwachungen des Verhaltens der Beschäftigten sollten grundsätzlich, im Betrieb ebenso wie im „Home Office“, verboten sein. Die Einzelfallkasuistik der arbeitsgerichtlichen Rechtsprechung und § 26 Absatz 1 Satz 2 BDSG sind im Rahmen einer normenklaren Ausnahmeregelung zu berücksichtigen. Dabei bedarf die Frage, ob § 26 Absatz 1 Satz 2 BDSG auch bei groben Pflichtverletzungen entsprechend Anwendung finden darf, einer gesetzlichen Klarstellung. Gesetzliche Eckpunkte, die z. B. auch Transparenz- und Zertifizierungsanforderungen für technische Anwendungen vorgeben können, sind insbesondere zu folgenden Aspekten nötig: Grenzen des Zugriffs auf und der Auswertung von E-Mails, Internetdienstdaten und weiteren IT-Daten der Beschäftigten durch Arbeitgeberinnen und Arbeitgeber, Regelungen zum Einsatz von Video-überwachungssystemen sowie Grenzen des Einsatzes von Geoinformationssystemen (GPS-Tracking) und biometrischen Verfahren im Beschäftigungsverhältnis. Hintergrund ist, dass der Einsatz und die Auswertung von Informations- und Kommunikationstechnologie gerade bei computergebundenen Arbeitsplätzen weitreichende Möglichkeiten der Leistungsüberwachung der Beschäftigten eröffnet, die durch gesetzliche Regelungen beschränkt werden müssen. Auch die Auswertung und Analyse von mit GPS ausgestatteten Fahrzeugen hat hohes Überwachungspotential und bedarf einer Regulierung. Besonders schützenswerte persönliche Merkmale wie biometrische Daten von Beschäftigten dürfen nur in Ausnahmefällen, die der Gesetzgeber definieren sollte, für Zwecke des Beschäftigungsverhältnisses genutzt werden.

● Ergänzungen zu den Rahmenbedingungen der Einwilligung

Die DSK befürwortet eine Ergänzung der Regelungen des § 26 Absatz 2 BDSG unter Berücksichtigung der Leitlinien des Europäischen Datenschutzausschusses zur Einwilligung, wonach die Einwilligung im Beschäftigungsverhältnis wegen des bestehenden Machtungleichgewichts grundsätzlich kritisch zu sehen ist[1]. Zudem sollte die entsprechende Regelung die Formulierung von Regelbeispielen bzw. Bedingungen enthalten, in welchen Fällen Einwilligungen im Beschäftigungs- und Bewerbungsverhältnis unzulässig sein sollen.

● Regelungen über Datenverarbeitungen auf Grundlage von Kollektivvereinbarungen

Die DSK fordert den Gesetzgeber auf klarzustellen, ob und inwieweit mit Kollektivvereinbarungen einschließlich Betriebsvereinbarungen zusätzliche Rechtsgrundlagen für Datenverarbeitungen im Beschäftigungsverhältnis geschaffen werden können. Der Wortlaut von Artikel 88 Absatz 1 DS-GVO und § 26 Absatz 1 Satz 1 BDSG ist in dieser Hinsicht unklar.

● Regelungen zum Verhältnis zwischen § 22 und § 26 BDSG sowie zu Artikel 6 und 9 DS-GVO

Die DSK empfiehlt, eindeutige konkretisierende Regelungen für die Verarbeitung von besonderen Kategorien personenbezogener Daten, wie z. B. Gesundheitsdaten, im Beschäftigungsverhältnis zu schaffen. Denn die Anwendungsbereiche der Regelungen des § 22 BDSG und des § 26 BDSG überschneiden sich:

[1] Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. 5. 2020, Rdnr. 21 ff., abrufbar unter: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guide-lines_202005_consent_de.pdf .

Unklar ist, welcher der beiden Paragraphen den Vorrang genießt. Nach § 22 Absatz 1 Nummer 1 Buchstabe b BDSG ist beispielsweise die Verarbeitung besonderer Kategorien personenbezogener Daten „für die Beurteilung der Arbeitsfähigkeit des Beschäftigten“ zulässig. Dieser steht hinsichtlich des Anwendungsbereiches nicht im Einklang mit § 26 Absatz 3 BDSG, der die Verarbeitung besonderer Kategorien von personenbezogenen Daten im Beschäftigungsverhältnis an weitere Bedingungen knüpft.

Unklar ist darüber hinaus auch das Verhältnis zu Artikel 6 Absatz 1 und Artikel 9 Absatz 2 DS-GVO hinsichtlich der Frage, inwiefern auf die Ermächtigungsgrundlagen aus der DS-GVO zurückgegriffen werden darf, wenn die Verarbeitung gemäß § 26 BDSG ausgeschlossen ist. Es ist hinsichtlich der neu zu schaffenden bereichsspezifischen Rechtsgrundlagen daher notwendig, ihr Verhältnis zu den Rechtsgrundlagen der DS-GVO klarzustellen.

● Beweisverwertungsverbote

Die DSK befürwortet die gesetzliche Normierung eines Beweisverwertungsverbots für rechtswidrig verarbeitete Beschäftigtendaten. Diese Regelung sollte klare Kriterien für das Vorliegen eines Beweisverwertungsverbotes enthalten.

● Datenverarbeitung bei Bewerbungs- und Auswahlverfahren

Die DSK ist der Ansicht, dass gesetzliche Regelungen zur Datenverarbeitung in der Bewerbungsphase erforderlich sind. Geregelt werden sollten die Möglichkeiten und Grenzen der Verarbeitung von direkt bei Bewerberinnen und Bewerbern sowie bei Dritten oder aus öffentlich zugänglichen Quellen in Bezug auf die Bewerberinnen und Bewerber erhobenen Daten. Darunter fallen insbesondere die folgenden Themenkomplexe: Fragerecht der Arbeitgeberinnen und Arbeitgeber, Anforderung polizeilicher

Führungszeugnisse, ärztliche Untersuchungen und Eignungstests, Datenerhebung aus Drittquellen (z. B. bei vorherigen Arbeitsstellen), Umgang mit sozialen Netzwerken oder das sog. Active Sourcing. Wesentlich sind in dieser Phase auch Regelungen zur Transparenz und klare Löschfristen.

- **23.03.2022 – Wissenschaftliche Forschung – selbstverständlich mit Datenschutz**

  Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) unterstreicht, dass wissenschaftliche Forschung und Datenschutz miteinander vereinbar sind.

  Auch der europäische Verordnungsgeber hat die Bedeutung der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung gesehen. So privilegiert die Datenschutz-Grundverordnung (DSGVO) die wissenschaftliche Forschung an vielen Stellen. Dazu gehört beispielsweise die Regelung in Artikel 5 Absatz 1 Buchstabe b DSGVO, wonach Forschungszwecke vereinbar mit dem ursprünglichen Zweck sein können, zu dem die Daten einmal erhoben wurden.

  Dies entspricht dem politischen Ziel der Europäischen Union, den wissenschaftlichen Fortschritt zu fördern sowie ihre wissenschaftlichen und technologischen Grundlagen dadurch zu stärken, dass ein europäischer Forschungsraum geschaffen wird.

  Die DSGVO zielt daher darauf ab, einen Ausgleich zwischen der Forschungs-freiheit auf der einen Seite und dem Recht des Einzelnen auf Achtung seines Grundrechts auf Datenschutz zu schaffen. So weist Artikel 89 DSGVO darauf hin, dass Verarbeitungen von personenbezogenen Daten für die wissenschaftliche Forschung geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen im Sinne der DSGVO unterliegen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet werden muss. Die DSK unterstützt daher

nachdrücklich die Förderung und Erforschung von Methoden, Forschungsdaten so zu verarbeiten, dass Persönlichkeitsrechte der Bürgerinnen und Bürger bestmöglich geschützt werden. Soweit ein Zugriff auf identifizierende Angaben nicht durch geeignete innovative Methoden ausgeschlossen werden kann, sollten Anonymisierung, Pseudonymisierung, Datentreuhänderschaften und andere Instrumente vorgesehen werden.

Die DSK begrüßt die Überlegungen der Bundesregierung, ein allgemeines Forschungsdatengesetz auf den Weg zu bringen, das das Recht auf informationelle Selbstbestimmung wahrt. Flankiert werden sollte dieses allgemeine Forschungsdatengesetz durch Forschungsregelungen in einzelnen Bereichen. Insbesondere erkennt die DSK die Pläne der Bundesregierung an, ein datenschutz-gerechtes Gesundheitsdatennutzungsgesetz auf den Weg zu bringen, um die Besonderheiten bei der wissenschaftlichen Forschung mit Gesundheitsdaten zu berücksichtigen. Die Erschließung von Gesundheitsdaten in medizinischen Registern für die wissenschaftliche Forschung durch ein geplantes Registergesetz kann allerdings nur unter Beachtung der datenschutzrechtlichen Anforderungen erfolgen.

Insoweit weist die DSK vor allem auf ihre Entschließung vom 25./26. März 2004[1] hin und fordert den Gesetzgeber auf sicherzustellen, dass auch bei und nach der Übermittlung geschützter personenbezogener medizinischer Daten ein strafrechtlicher Schutz vor Offenbarung und Beschlagnahmeschutz im Strafverfahren gewährleistet ist.

Aus diesem Grund hält sie es insbesondere für erforderlich,

[1] vgl. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DSK/DSKEntschliessun-gen/67DSK-EinfuehrungEinesForschungsgeheimnissesFuerMedizinischeDaten.pdf

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forschende und ihre Berufshelfenden zu schaffen und
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die DSK bietet eine konstruktive Beratung bei der Weiterentwicklung der Nationalen Forschungsdateninfrastruktur an, sofern dabei personenbezogene Daten betroffen sind. Dies gilt auch im europäischen Kontext, soweit etwa im Bereich des Europäischen Gesundheitsdatenraums personenbezogene Daten, insbesondere Gesundheitsdaten, für die wissenschaftliche Forschung bereitgestellt werden sollen.

Die DSK beabsichtigt zeitnah weitere Vorschläge zum Thema Forschungsdaten zu veröffentlichen. Ziel ist es, neben der Rechtsklarheit für die Nutzung von Forschungsdaten insbesondere auch den nachhaltigen Schutz für die personenbezogenen Daten der Bürgerinnen und Bürger zu gewährleisten.

- **23.03.2022 – Parlamentarische Untersuchungsausschüsse und Löschmoratorien: Datenschutz durch klare Vorgaben und Verarbeitungsbeschränkungen für Behörden**

  In den vergangenen Jahren gab es zahlreiche Parlamentarische Untersuchungsausschüsse im Bundestag und in den Landtagen, die das Handeln von Polizei- und Sicherheitsbehörden untersucht haben. Prominente Beispiele sind die Untersuchungsausschüsse zur „Terrorgruppe nationalsozialistischer Untergrund“ (sog. NSU).

  Die Untersuchungsausschüsse möchten eine für die Aufklärung notwendige Datengrundlage sicherstellen. Deshalb fordern sie

die Behörden regelmäßig auf, sämtliche personenbezogenen Daten weiterhin zu speichern, die in irgendeinem Bezug zum Untersuchungsgegenstand stehen können (etwa zum Thema „Rechtsextremismus“). Diese Daten sind dann für die Arbeit des Untersuchungsausschusses vorzuhalten. Dies soll auch solche Daten umfassen, die nach den gesetzlichen Regeln eigentlich zu löschen wären (so genanntes Löschmoratorium).

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hält das Interesse der Parlamentarischen Untersuchungsausschüsse an dem Erhalt personenbezogener Daten für nachvollziehbar und gewichtig, um den Untersuchungsauftrag umzusetzen. Es ist ihr insbesondere bewusst, dass dem parlamentarischen Informationsinteresse ein besonders hohes Gewicht zukommt, soweit es um die Aufdeckung möglicher Rechtsverstöße und vergleichbarer Missstände geht. Gleichzeitig gilt es allerdings zu berücksichtigen, dass dadurch erheblich in Grundrechte der betroffenen Personen eingegriffen wird, insbesondere dann, wenn diese Personen tatsächlich in keinerlei Bezug zum Untersuchungsgegenstand stehen bzw. gesetzliche Löschungsverpflichtungen suspendiert werden.

Um parlamentarischen Kontrollrechten und Grundrechten betroffener Personen gleichermaßen Geltung zu verschaffen, weist die Konferenz auf folgende Punkte hin:

- Ohne die förmliche Einsetzung eines Untersuchungsausschusses und Anforderungen von Beweisunterlagen gibt es keine Rechtsgrundlage dafür, die gesetzlich vorgeschriebene Löschung personenbezogener Daten zu suspendieren.

  Hierzu gehört, dass der Untersuchungsgegenstand klar definiert ist und die Beweisbeschlüsse hinreichend bestimmt formuliert sind (BVerfG, Beschluss vom 17.6.2009 – 2 BvE 3/07). Zudem müssen die Ausnahmen zeitlich auf die Arbeit des Untersuchungsausschusses begrenzt sein. Nur auf diese

Weise können unnötige Datenspeicherungen und die damit verbundenen Risiken für die Rechte der betroffenen Personen vermieden werden.

- „Löschreife“ Daten, die die Behörden für Zwecke eines Untersuchungsausschusses zur Verfügung halten, dürfen sie im weiteren Verwaltungsvollzug nicht nutzen. Die DSK hält es daher für erforderlich, diese Daten in Anlehnung an § 58 Abs. 3 BDSG in ihrer Verarbeitung zu beschränken. Hierfür sollte der jeweilige Gesetzgeber Voraussetzungen und Grenzen präzise beschreiben. Einige Landesgesetzgeber haben dies bereits umgesetzt.

Die DSK appelliert deshalb an die Gesetzgeber des Bundes und der Länder, den Sicherheitsbehörden klare gesetzliche Vorgaben zum Umgang mit zu löschenden Daten zu machen. Diese müssen den Untersuchungsausschüssen den Zugriff auf die Daten sichern. Gleichzeitig ist sicherzustellen, dass die Daten dem Verwaltungsvollzug der Behörden entzogen sind. So werden das Untersuchungsinteresse der Parlamentarischen Untersuchungsausschüsse und die Grundrechte der betroffenen Personen gewahrt.

Beschlüsse der Datenschutzkonferenz 2022

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

- **29.11.2022 – Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht (Stand: Oktober 2022)**

  Der deutsche Gesetzgeber hat zur Umsetzung der europäischen Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen (DI-RL) in das Bürgerliche Gesetzbuch (BGB) neue Vorschriften zu Verbraucherverträgen über digitale Produkte aufgenommen. Diese sind am 1.1.2022 in Kraft getreten. In den neuen zivilrechtlichen Verbraucherschutzvorschriften über digitale Produkte wird in § 312 Abs. 1a BGB und § 327q BGB „Vertragsrechtliche Folgen datenschutzrechtlicher Erklärungen des Verbrauchers“ ein eindeutiger Bezug zum Datenschutzrecht hergestellt.

  § 312 Abs. 1a BGB lautet:

  „Die Vorschriften der Kapitel 1 und 2 dieses Untertitels sind auch auf Verbraucherverträge anzuwenden, bei denen der Verbraucher dem Unternehmer personenbezogene Daten bereitstellt oder sich hierzu verpflichtet. Dies gilt nicht, wenn der Unternehmer die vom Verbraucher bereitgestellten personenbezogenen Daten ausschließlich verarbeitet, um seine Leistungspflicht oder an ihn gestellte rechtliche Anforderungen zu erfüllen, und sie zu keinem anderen Zweck verarbeitet.“

  Nunmehr wird in der Praxis stark diskutiert, welche datenschutzrechtlichen Auswirkungen diese Vorschriften auf das sog. Geschäftsmodell „Bezahlen mit Daten“ haben. Insbesondere im Internet wird dieses Geschäftsmodell seit langem praktiziert, wenn werthaltige Inhalte, wie z.B. Zeitungsartikel, oder Dienstleistun-

gen, wie die Bereitstellung von Plattformen zur sozialen Vernetzung oder Suchmaschinen, von den Nutzer:innen nicht mit Geld bezahlt werden. Die vermeintlich kostenlosen Inhalte und Dienstleistungen werden regelmäßig über personalisierte Werbung finanziert. Zu diesem Zweck, wird das Verhalten der Nutzer:innen häufig nachverfolgt und die so gewonnenen Daten werden zu detaillierten Nutzerprofilen zusammengeführt und ausgewertet, um auf dieser Grundlage Werbung darzustellen und dadurch die Werbeeinnahmen zu generieren.

Die Verarbeitung personenbezogener Daten im Rahmen dieser Geschäftsmodelle muss auf eine der gesetzlichen Erlaubnistatbestände gemäß Art. 6 Abs. 1 Buchstabe a, b oder f DS-GVO gestützt werden können und auch den sonstigen Anforderungen der Datenschutz-Grundverordnung gerecht werden. Die neuen Verbraucherschutzvorschriften des BGB stellen keine eigene Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten dar.

Die DSK beurteilt die datenschutzrechtlichen Auswirkungen der neuen Verbrauchervorschriften wie folgt:

1. Die §§ 327 ff. BGB sind nur anwendbar, wenn ein Vertrag über digitale Produkte geschlossen wurde.

Ob zwischen Nutzer:innen und Betreiber:innen einer Website, deren Angebote durch personalisierte Werbung (teilweise) finanziert werden, tatsächlich ein Vertrag über digitale Produkte zustande kommt, hängt insbesondere davon ab, inwiefern die Parteien den Willen haben, sich rechtlich zu binden. Eine verallgemeinernde Auslegung dahingehend, dass jeder Aufruf einer Webseite, deren Angebot die Verarbeitung personenbezogener Daten beinhaltet, oder jede Interaktion mit einem Einwilligungsbanner zum Abschluss eines Verbrauchervertrages führt, verbietet sich vor dem Hintergrund der Anforderungen der §§ 133, 157 BGB. Insbesondere kann allein die Bereitstellung

der personenbezogenen Daten nicht als konkludente Willenserklärung der Betroffenen zum Abschluss eines Vertrages über digitale Produkte gewertet werden. In der Praxis wird es maßgeblich darauf ankommen, in jedem konkreten Fall zu untersuchen, ob zwei übereinstimmende Willenserklärungen mit entsprechendem Rechtsbindungswillen vorliegen. Nur in diesem Fall kommen die §§ 327 ff. BGB überhaupt zum Tragen.

2. Wurde zwischen dem Unternehmen und dem Verbraucher ein Vertrag über digitale Produkte geschlossen, ist jede Verarbeitung von personenbezogenen Daten im Zusammenhang mit dem geschlossenen Vertrag nur rechtmäßig, wenn sie auf eine Rechtsgrundlage der Datenschutz-Grundverordnung gestützt werden kann.

Die zivilrechtlichen Vorschriften über den Verbrauchervertrag stellen keine eigene Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten dar. Für die Datenverarbeitung im Rahmen des Verbrauchervertrages über digitale Inhalte kommen grundsätzlich Art. 6 Abs. 1 Buchstabe a, b und f DS-GVO in Betracht. Sofern besondere Kategorien personenbezogener Daten verarbeitet werden sollen, ist zusätzlich Art. 9 DS-GVO zu berücksichtigen. Die Erwägungsgründe Nr. 37 und 38 DI-RL halten ausdrücklich fest, dass die DS-GVO von der Richtlinie unberührt bleibt und die Vorgaben der DS-GVO für alle personenbezogenen Daten gelten, die im Zusammenhang mit den von dieser Richtlinie erfassten Verträgen verarbeitet werden. Eine Verarbeitung personenbezogener Daten im Zusammenhang mit einem Vertrag, der in den Anwendungsbereich der Richtlinie fällt, ist daher nur rechtmäßig, wenn sie mit den Bestimmungen der DS-GVO im Einklang steht. Gleiches gilt für die neuen Verbraucherschutzvorschriften im BGB, die der Umsetzung der DI-RL dienen.

3. § 327q BGB trifft keine Aussage zu den Auswirkungen der zivilrechtlichen Verbraucherschutzvorschriften auf das Datenschutzrecht. Es werden nur umgekehrt die zivilrechtlichen Auswirkungen auf den Verbrauchervertrag festgelegt

wenn Verbraucher von ihren datenschutzrechtlichen Rechten Gebrauch gemacht haben, eine Einwilligung zu widerrufen oder einer Datenverarbeitung, die auf Art. 6 Abs. 1 Buchstabe f DS-GVO gestützt wird, gemäß Art. 21 DS-GVO zu widersprechen.

§ 327q BGB regelt die vertragsrechtlichen Folgen datenschutzrechtlicher Erklärungen des Verbrauchers. In Absatz 1 wird festgestellt, dass die Ausübung von datenschutzrechtlichen Betroffenenrechten und die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers

nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Im Falle des Widerrufs der von einem Verbraucher erteilten datenschutzrechtlichen Einwilligung oder des Widerspruchs gegen eine weitere Verarbeitung seiner personenbezogenen Daten wird dem Unternehmen unter den Voraussetzungen des § 327q Abs. 2 BGB ein außerordentliches Kündigungsrecht des Verbrauchervertrages zuerkannt. Absatz 3 stellt ergänzend klar, dass die Ausübung von Datenschutzrechten oder die Abgabe datenschutzrechtlicher Erklärungen durch den Verbraucher keine Ersatzansprüche des Unternehmers gegen diesen begründen können.

4. Die neuen Verbraucherschutzvorschriften im BGB haben keine Auswirkungen auf die Anwendung von § 25 TTDSG.

Wurde zwischen dem Unternehmen und dem Verbraucher ein Vertrag über digitale Produkte geschlossen, hat dies keine Auswirkungen auf die Anwendung § 25 TTDSG. Das Unternehmen muss prüfen, ob für Vorgänge der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, eine Einwilligung erforderlich oder eine Ausnahme einschlägig ist. Wie oben geschildert, kommen die §§ 327 ff. BGB überhaupt erst zur Anwendung, wenn ein Verbrauchervertrag geschlossen

wird. Die Qualitätsanforderungen, die § 327e BGB aufstellt, können den „objektiv geschuldeten Funktionsumfang“ eines Telemediendienstes mithin erst beeinflussen, wenn mit Nutzer:innen ein Vertrag über digitale Produkte zustande kommt. Selbst dann ist weiterhin im Einzelfall zu prüfen, ob die Vorgänge unbedingt erforderlich sind, um den von Nutzer:innen gewünschten Dienst (mangelfrei) zur Verfügung zu stellen. Weitere Ausführungen hierzu können der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien (letzte Fassung vom 24. November 2022) entnommen werden.

- **13.04.2022 – Zur Verarbeitung personenbezogener Daten im Zusammenhang mit der einrichtungsbezogenen Impfpflicht**

  Für gesetzlich bestimmte Einrichtungen und Unternehmen aus dem Gesundheitsbereich gilt seit dem 15. März 2022 eine einrichtungsbezogene Impfpflicht, § 20a Absatz 1 IfSG. Seit diesem Zeitpunkt dürfen in diesen nur Personen tätig sein, die gegen das Coronavirus SARS-CoV-2 geimpft oder von diesem genesen sind oder bei denen eine medizinische Kontraindikation hinsichtlich einer Impfung gegen das Coronavirus SARS-CoV-2 vorliegt.

  Für die genannten Personen besteht eine Nachweispflicht über ihre Impfung, Genesung oder das Vorliegen einer medizinischen Kontraindikation, § 20a IfSG.

  - **Für wen genau gilt die einrichtungsbezogene Impfpflicht?**

  Die einrichtungsbezogene Impfpflicht gilt für alle Personen, die in den in § 20a IfSG benannten Einrichtungen/Unternehmen tätig sind. Dies sind nicht allein die unmittelbaren Beschäftigten, sondern auch weitere vor Ort tätige Personen, wie Handwerker, Leiharbeitnehmerinnen und Leiharbeitnehmer, Praktikantinnen und Praktikanten usw.

Der Wortlaut der gesetzlichen Regelung lässt offen, ob diese auch auf Arbeitskräfte Anwendung findet, die sich nur kurze Zeit im Gebäude aufhalten. Bitte wenden Sie sich in Zweifelsfällen an die für die Anwendung des Infektionsschutzgesetzes für Sie zuständige jeweilige öffentliche Stelle.

- **Was gilt als Nachweis über eine Impfung, Genesung oder medizinische Kontraindikation?**

Was im Einzelnen als Nachweis für die Impfung und Genesung gilt, ist wiederum in § 22a Absatz 1 und Absatz 2 IfSG geregelt. Der vorgelegte Nachweis muss den genannten Regelungen entsprechen, § 20a Absatz 2 Nummer 1 und 2 IfSG.

Als Nachweis über eine medizinische Kontraindikation gilt ein ärztliches Zeugnis darüber, dass die betroffene Person auf Grund einer medizinischen Kontraindikation nicht gegen das Coronavirus SARS-CoV-2 geimpft werden kann, § 20a Absatz 2 Nummer 4 IfSG. Nach dem Wortlaut des Gesetzes ist es ausreichend, dass in dem ärztlichen Zeugnis das Vorliegen einer medizinischen Kontraindikation an sich bestätigt wird. Konkrete Gesundheitsdaten, wie Diagnosen, dürfen seitens der Leitung der unter § 20a IfSG fallenden Einrichtung/des Unternehmens nicht gefordert werden.

Sollte es sich bei den medizinischen Kontraindikationen lediglich um vorübergehende handeln, wird in dem Zeugnis voraussichtlich auch ein Enddatum für das Vorliegen der medizinischen Kontraindikation benannt sein.

Alternativ können schwangere Personen, die in den in § 20a IfSG benannten Einrichtungen/Unternehmen tätig sind, ein ärztliches Zeugnis darüber vorlegen, dass sie sich im ersten Schwangerschaftsdrittel befinden, § 20a Absatz 2 Nummer 3 IfSG.

- **Gegenüber wem ist der Nachweis über eine Impfung, Genesung oder medizinischen Kontraindikation zu erbringen?**

Der Nachweis ist gegenüber der Leitung der Einrichtung/des Unternehmens zu erbringen, § 20a Absatz 2 IfSG. Zum Begriff der „Leitung“ siehe auch § 2 Nummer 15a, b IfSG.

Auch Personen, die nicht unmittelbar in einem Arbeitsverhältnis zu den unter § 20a IfSG fallende Einrichtungen/Unternehmen stehen, in diesen aber, zum Beispiel als Handwerker, tätig sind, müssen den Nachweis nur gegenüber den genannten Leitungen erbringen.

Delegationsmöglichkeiten werden im Folgenden behandelt.

- **Können die Leitungen der Einrichtungen/Unternehmen die Pflicht zur Entgegennahme des Nachweises auf andere Personen übertragen?**

In der Praxis bestimmen die Leitungen der jeweiligen Einrichtungen/Unternehmen oftmals intern Beschäftigte, zum Beispiel aus der Personalabteilung, denen der Nachweis vorzulegen ist. Dies ist grundsätzlich datenschutzrechtlich möglich (siehe auch § 2 Nummer 15a Buchstabe a und § 2 Nummer 15b Buchstabe a IfSG; Deutscher Bundestag, Drucksache 20/250, Seite 60). An dieser Stelle muss allerdings insbesondere darauf geachtet werden, dass die Nachweise tatsächlich nur von den hierfür bestimmten Beschäftigten eingesehen werden und diese auf ihre Verschwiegenheitspflicht hingewiesen werden.

Darüber hinaus kann die Leitung der in § 20a IfSG genannten Einrichtungen/Unternehmen die Entgegennahme des Nachweises alternativ an geeignete Dritte, wie zum Beispiel externe Personalverwaltungen, delegieren. Zu diesem Zweck müssten sie mit diesen einen Auftragsverarbeitungsvertrag schließen bezie-

hungsweise einen bereits mit diesen geschlossenen Auftragsverarbeitungsvertrag gegebenenfalls aktualisieren, Artikel 28 DS-GVO.

- **Datenschutzkonformer Umgang mit dem Nachweis**

Die genannten Personen müssen den Nachweis nur vorlegen. Das bedeutet, in den Nachweis darf zunächst nur Einsicht genommen werden. Dieser Nachweis darf daraufhin geprüft werden, ob er den oben genannten gesetzlichen Bestimmungen entspricht.

Bei allen in den Einrichtungen/Unternehmen tätigen Personen darf nur jeweils notiert werden, dass ein Nachweis entsprechend § 20a IfSG vorgelegt worden ist und gegebenenfalls das Ablauf-/Enddatum dieses Nachweises, zum Beispiel bei den Genesenennachweisen sowie digitalen Impfnachweisen oder auch den Nachweisen über eine temporäre Kontraindikation. Darüber hinaus sieht das Gesetz in § 22a Absatz 1 IfSG bei bestimmten Impfnachweisen als Ablaufdatum den 30. September 2022 vor, zum Beispiel bei Personen bei denen nur zwei Einzelimpfungen nachweislich vorliegen. Auch dieses Ablaufdatum darf notiert werden.

Denn nach Ablauf des jeweiligen Nachweises, muss ein dann gültiger Nachweis vorgelegt werden. Sofern dies nicht binnen Monatsfrist erfolgt, haben die Leitungen der in § 20a IfSG genannten Einrichtungen/Unternehmen dies an das jeweils für sie zuständige Gesundheitsamt zu melden und die personenbezogenen Daten der betroffenen Person an dieses zu übermitteln, § 20a Absatz 4 IfSG. Der vorgelegte Nachweis darf nicht kopiert oder eingescannt und aufbewahrt werden.

Bei Personen, die keine unmittelbaren Beschäftigten der genannten Einrichtungen/Unternehmen sind, dürfen darüber hinaus natürlich auch der Vor- und Zuname und deren Kontaktdaten erhoben werden.

Mangels Erforderlichkeit dürfen weitere Daten wie zum Beispiel Impfmittel, das Datum der einzelnen Impfung usw. nicht notiert werden.

- **Wie oft muss der Nachweis vorgelegt werden?**

Personen, die bereits in den genannten Einrichtungen tätig sind, mussten den Nachweis einmalig bis zum 15. März 2022 vorlegen. Hat der Nachweis ein Ablauf-/Enddatum, siehe oben, muss nach dessen Ablauf ein aktueller Nachweis ebenso einmalig vorgelegt werden und zwar innerhalb eines Monats nach Ablauf der Gültigkeit des bisherigen Nachweises, § 20a Absatz 4 Satz 1 IfSG. Die Leitung der unter § 20a IfSG fallenden Einrichtungen und Unternehmen dürfen die betroffenen Personen vor Ablauf der eben genannten Monatsfrist auffordern, den jeweiligen Nachweis vorzulegen. Die betroffenen Personen müssen aber vor Fristende der Aufforderung nicht nachkommen.

Personen, die erst nach dem 15. März 2022 ihre Tätigkeit aufnehmen, haben den Leitungen der genannten Einrichtungen/Unternehmen oder den von diesen bestimmten Personen vor Aufnahme ihrer Tätigkeit den Nachweis vorzulegen.

- **Was passiert wenn ein Nachweis nicht fristgerecht vorgelegt wird oder aber Zweifel an der Gültigkeit eines Nachweises bestehen?**
  - **Personen, die bereits in den Einrichtungen/Unternehmen tätig sind:**

    Die Leitungen der genannten Einrichtungen/Unternehmen oder von diesen hierfür bestimmte Personen müssen unverzüglich das für die Einrichtung/das Unternehmen zuständige Gesundheitsamt informieren und dürfen zu diesem Zweck personenbezogene Daten der Person, die keinen Nachweis vorgelegt hat oder aber bei der Zweifel an der Echtheit oder inhaltlichen Richtigkeit ihres Nachweises bestehen, an dieses übermitteln, § 20a Absatz 2 Satz 2 IfSG.

In diesem Zusammenhang dürfen auf der Grundlage des § 20a IfSG neben dem Übermittlungsanlass (Nichtvorlage/Echtheits- oder Richtigkeitszweifel) personenbezogene Daten höchstens im Umfang des § 2 Nummer 16 IfSG (insbesondere Vor- und Zuname, Kontaktdaten) an das Gesundheitsamt übermittelt werden. Der Grundsatz der „Datenminimierung“ (Artikel 5 Absatz 1 Buchstabe c DS-GVO) ist zu beachten.

Darüber hinaus besteht auf der Basis einer Einwilligung die Möglichkeit, Informationen über bereits vereinbarte Impftermine durch die Einrichtungen/Unternehmen zu erheben und an das zuständige Gesundheitsamt weiterzuleiten, sofern sich dies im weiteren Verfahren zugunsten der betroffenen Personen auswirken kann. Die weiteren Voraussetzungen für die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten aufgrund einer Einwilligung sind stets zu beachten.

Auf Anforderung des zuständigen Gesundheitsamtes haben diese Personen den jeweiligen Nachweis diesem vorzulegen, § 20a Absatz 5 Satz 1 IfSG. Bei Zweifeln an der Echtheit oder inhaltlichen Richtigkeit eines Nachweises kann das zuständige Gesundheitsamt eine Untersuchung der betroffenen Person anordnen, ob eine medizinische Kontraindikation betreffend die Impfung gegen das Coronavirus SARS-CoV-2 vorliegt, § 20a Absatz 5 Satz 2 IfSG. Legt die betreffende Person dem Gesundheitsamt ihren Nachweis nicht vor oder leistet gegebenenfalls einer Anordnung einer ärztlichen Untersuchung nicht Folge, kann das Gesundheitsamt der betreffenden Person das Betreten der Einrichtung/des Unternehmens oder das Tätigwerden in dieser/diesem untersagen, § 20a Absatz 5 Satz 3 IfSG.

- **Personen, die in den Einrichtungen/Unternehmen nach dem 15. März 2022 tätig sein sollen:**

Legen Personen, die nach dem 15. März 2022 in einer Einrichtung/einem Unternehmen tätig werden sollen, vor Beginn ihrer Tätigkeit keinen Nachweis vor, dürfen sie in der Einrichtung/dem Unternehmen nicht tätig werden, § 20a Absatz 3 Satz 4 IfSG.

Bestehen Zweifel an der Gültigkeit des Nachweises ist seitens der Leitungen der Einrichtungen/Unternehmen wie oben dargestellt zu verfahren.

- **Meldepflicht der Pflegeeinrichtungen über den prozentualen Anteil geimpfter Personen (Impfquoten) an das Robert-Koch-Institut (RKI)**

§ 20a Absatz 7 Satz 1 IfSG enthält eine weitere gesetzliche Meldepflicht: Es sind monatlich Impfquoten an das RKI zu melden.

  - **Für wen gilt diese Meldepflicht?**

    Nicht alle in § 20a IfSG benannten Einrichtungen/Unternehmen sind zur Meldung von Impfquoten an das RKI verpflichtet. Vielmehr gilt diese Meldepflicht nur für die voll- oder teilstationäre Einrichtungen zur Betreuung und Unterbringung älterer, behinderter oder pflegebedürftiger Menschen oder vergleichbare Einrichtungen, die zugelassene Pflegeeinrichtungen im Sinne des § 72 des Elften Buches Sozialgesetzbuchs sind.

  - **Ausnahme von der Meldepflicht**

    Bevor die Leitungen der genannten Einrichtungen Daten für die Erfüllung der Meldepflicht nach § 20a Absatz 7 Satz 1 IfSG verarbeiten, sollte geprüft werden, ob für die Einrichtung eine Ausnahme von der Meldepflicht nach § 20a Absatz 7 Satz 1 IfSG vorliegt. Denn wenn die nachfolgenden Voraussetzungen erfüllt sind, entfällt die Meldepflicht, § 20a Absatz 7 Satz 5 IfSG:

- Es gibt **landesrechtliche Meldeverfahren**, die bereits vor/am 19. März 2022 bestanden und
- auf Bundesrecht beruhen und
- die zu den durch das RKI zu erhebenden Daten über die Impfquoten anschlussfähig sind und
- die Bundesländer nach Kreisen und kreisfreien Städten aufgeschlüsselte Daten direkt an das RKI übermitteln.

Zur Feststellung, ob Sie von der Meldepflicht nach § 20a Absatz 7 Satz 1 IfSG befreit sind, wenden Sie sich in Zweifelsfällen an die für die Anwendung des Infektionsschutzgesetz für Sie zuständige jeweilige öffentliche Stelle.

- **Welche Daten dürfen zur Erfüllung der Meldepflicht wie verarbeitet werden?**

Wenn keine Ausnahme von der Meldepflicht vorliegt, müssen die in § 20a Absatz 7 Satz 1 IfSG benannten Einrichtungen an das RKI folgende Impfquoten übermitteln:

Anteil der Personen, die gegen das Coronavirus SARS-CoV-2 geimpft sind, jeweils bezogen auf die Personen,

- die in der Einrichtung beschäftigt sind,
- behandelt, betreut oder gepflegt werden oder
- untergebracht sind.

In § 20a Absatz 7 Satz 1 IfSG ist ausdrücklich geregelt, dass an das RKI Daten nur in anonymisierter Form übermittelt werden dürfen.

Um die Meldepflicht gegenüber dem RKI zu erfüllen, dürfen die in § 20a Absatz 7 Satz 1 IfSG benannten Einrichtungen den jeweiligen Impfstatus der

- Beschäftigten oder,
- Behandelten, Betreuten, Gepflegten oder
- Untergebrachten

verarbeiten.

Diesbezüglich dürfen die in § 20a Absatz 7 Satz 1 IfSG benannten Einrichtungen zur Erfüllung ihrer Meldepflicht den jeweiligen Impfstatus ihrer Beschäftigten, Behandelten, Betreuten, Gepflegten oder Untergebrachten bei diesen abfragen und für den Zweck „Erfüllung der Meldepflicht gegenüber dem RKI“ speichern, § 20a Absatz 7 Satz 2 IfSG.

- **Beurteilung der Gefährdungslage anhand von Impfdaten**

  Besteht eine Meldepflicht und werden für deren Erfüllung bereits Impfdaten nach § 20a Absatz 7 Satz 2 verarbeitet, dürfen diese – soweit erforderlich – durch die Leitungen der in § 20a Absatz 7 Satz 1 IfSG benannten Einrichtungen zur Beurteilung der Gefährdungslage in der Einrichtung im Hinblick auf die Coronavirus-Krankheit-2019 (COVID-19) verarbeitet werden, § 20a Absatz 7 Satz 3 IfSG.

- **Technische und Organisatorische Maßnahmen**

  Die Einrichtungen gemäß § 20a Absatz 7 Satz 1 IfSG müssen bei der Verarbeitung der Impfdaten für die Erfüllung ihrer Meldepflicht sowie für ihre Beurteilung der Gefährdungslage in der Einrichtung im Hinblick auf COVID-19 angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen treffen, § 20a Absatz 7 Satz 4 IfSG in Verbindung mit § 22 Absatz 2 BDSG.

- **Wann sind die Daten spätestens zu löschen?**

Grundsätzlich haben die Leiterinnen und Leiter der genannten Einrichtungen/Unternehmen beziehungsweise deren Auftragsverarbeiter alle Daten zu löschen, wenn der Zweck für die Verarbeitung der personenbezogenen Daten entfällt, Artikel 17 Absatz 1 Buchstabe a DS-GVO.

Unabhängig von einer Löschpflicht nach Artikel 17 Absatz 1 Buchstabe a DS-GVO sieht § 20a Absatz 7 Satz 7 IfSG für die im Zusammenhang mit der Meldepflicht und Beurteilung der Gefährdungslage anhand von Impfquoten verarbeiteten Daten vor, dass diese spätestens am Ende des sechsten Monats nach ihrer Erhebung gelöscht werden müssen. Jedenfalls muss eine Löschung aller auf Grundlage des § 20a IfSG verarbeiteten Daten spätestens mit Ablauf der Rechtsgrundlage am 31. Dezember 2022 erfolgen.

- **24.03.2022 – Hinweise der DSK – Datenschutzkonformer Online-Handel mittels Gastzugang (Stand 24. März 2022)**

  Auch im Online-Handel gilt der Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchstabe c) DS-GVO). Danach sind nur die Daten zu erheben, die für die Abwicklung eines einzelnen Geschäfts erforderlich sind. Die zulässige Verarbeitung der personenbezogenen Daten hängt im Einzelfall insbesondere davon ab, ob Kund*innen einmalig einen Vertrag abschließen wollen oder eine dauerhafte Geschäftsbeziehung anstreben. Dazu müssen Kund*innen jeweils frei entscheiden können, ob sie ihre Daten für jede Bestellung eingeben und insofern als sogenannter temporärer Gast geführt werden möchten oder ob sie bereit sind, eine dauerhafte Geschäftsbeziehung einzugehen, die mit einem fortlaufenden Kund*innenkonto verbunden ist.

  Daraus ergibt sich Folgendes:

  1. Verantwortliche, die Waren oder Dienstleistungen im Onlinehandel anbieten, müssen ihren Kund*innen unabhängig davon, ob sie ihnen daneben einen registrierten Nutzungszugang (fortlaufendes Kund*innenkonto) zur Verfügung stellen, grundsätzlich einen Gastzugang (Online-Geschäft ohne Anlegen eines fortlaufenden Kund*innenkontos) für die Bestellung bereitstellen.

Im Online-Handel ist das **fortlaufende Kund*innenkonto** regelmäßige Praxis. Es wird unter Vergabe von Zugangsdaten (z.B. Benutzername/Passwort) eingerichtet, um sich gegenüber dem Verantwortlichen eindeutig zu identifizieren. Kund*innen können damit auf ein bei dem Verantwortlichen geführtes Kund*innenkonto selbst und aktiv zugreifen, um ggf. ihre Daten zu ändern oder Bestellungen zu prüfen. Fortlaufende Kund*innenkonten werden über den erstmaligen Geschäftsabschluss hinaus im Aktivdatenbestand gepflegt. Sie dienen den Kund*innen zur vereinfachten wiederkehrenden Bestellmöglichkeit ohne die nochmalige Eingabe aller personenbezogenen Daten. Darüber hinaus kann ein fortlaufendes Kund*innenkonto eine Bestell- oder Geschäftshistorie vorsehen, die dem Verantwortlichen eine Auswertung zur Profilbildung und für Werbezwecke ermöglicht.

Nach Art. 6 Abs. 1 Satz 1 Buchstabe b) DS-GVO ist nur die Verarbeitung der personenbezogenen Daten zulässig, die für die Erfüllung des einzelnen Vertrages erforderlich sind. Bei einer erstmaligen Bestellung kann der Verantwortliche nicht per se unterstellen, dass er Daten von Kund*innen für mögliche, aber ungewisse zukünftige Geschäfte auf Vorrat vorhalten darf. Für die Einrichtung eines fortlaufenden Kund*innenkontos ist eine entsprechende bewusste Willenserklärung der Kund*innen erforderlich. Für Kund*innen, die keine dauerhafte Geschäftsbeziehung eingehen wollen oder eine Verarbeitung von nicht zur Geschäftsabwicklung benötigten Daten ablehnen, ist daher regelmäßig ein **Gastzugang** zu ermöglichen. Ein solcher Zugang verzichtet auf Registrierungs- bzw. Zugangsdaten (z.B. Benutzername/Passwort) für eine erneute Nutzung. Über diesen Zugang dürfen nur die zur Durchführung des Vertrages und zur Erfüllung gesetzlicher Pflichten erforderlichen personenbezogenen Daten und Informationen der Kund*innen erfasst werden. Nach Vertragserfüllung nicht mehr benötigte Daten müssen gemäß Art. 17 Abs. 1 Buchstabe a) DS-GVO unverzüglich gelöscht werden. Werden die Daten im Übrigen nur noch im Rahmen spezialgesetzlich geregelter Aufbewahrungsplichten verarbeitet, z.B. aus

dem Handels- oder Steuerrecht, sind technisch-organisatorische Maßnahmen zu ergreifen, um diese Daten von den Daten im operativen Zugriff zu trennen (Datensperrung). Ein Zugriff der Kund*innen auf die Daten oder das Hinzuspeichern von weiteren Daten durch die Verantwortlichen sind bei einem Gastzugang nicht vorgesehen.

Soweit im Einzelfall besondere Umstände vorliegen, bei denen ein fortlaufendes Kund*innenkonto ausnahmsweise als für die Erfüllung eines Vertrages erforderlich angesehen werden kann (Art. 6 Abs. 1 Buchstabe b DS-GVO, z.B. für Fachhändler bei bestimmten Berufsgruppen) und mithin hierfür ausnahmsweise keine Einwilligung erforderlich ist, ist dem Grundsatz der Datenminimierung Rechnung zu tragen, indem z.B. das Kund*innenkonto bei Inaktivität automatisiert nach einer kurzen Frist gelöscht wird.

2. Ohne einen Gastzugang bzw. ohne eine gleichwertige Bestellmöglichkeit kann die Freiwilligkeit einer Einwilligung nicht gewährleistet werden.

Damit eine für die Einrichtung eines fortlaufenden Kund*innenkontos erforderliche Einwilligung nicht gegen die in Art. 7 Abs. 4 DS-GVO erwähnte Konditionalität verstößt, müssen die Kund*innen im Online-Shop auch die gleichen Angebote auf anderem gleichwertigen Wege als über das fortlaufende Kund*innenkonto bestellen können (vgl. Rn. 37 f. der Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 des Europäischen Datenschutzausschusses vom 04.05.2020). Gleichwertig ist eine Bestellmöglichkeit, wenn keinerlei Nachteile entstehen, also Bestellaufwand und Zugang zu diesen Möglichkeiten, wie bei einem Gastzugang, denen eines laufenden Kund*innenkontos entsprechen und technisch organisatorische Maßnahmen getroffen werden, die ein angemessenes Datenschutzniveau gewährleisten.

3. Die mit einem fortlaufenden Online-Konto verbundenen Möglichkeiten der Auswertung der Vertragshistorie für Werbezwecke so wie die Speicherung von Informationen über Zahlungsmittel bedürfen einer informierten Einwilligung.

Sollen in einem fortlaufenden Kund*innenkonto die über die Kontaktdaten hinausgehenden personenbezogenen Daten, ggf. einschließlich der Vertragsdaten der Bestellungen, für Werbezwecke (Profiling der Kundenhistorien, Zusammenführung mit Daten aus anderen Quellen) ausgewertet und verarbeitet werden, sind darauf bezogen Einwilligungen der Kund*innen nach Art. 6 Abs. 1Satz 1 Buchstabe a) DS-GVO einzuholen. Da dies eine Verarbeitung ist, die über die bloße Einrichtung und Führung eines fortlaufenden Kund*innenkontos hinausgeht, ist diese nicht bereits durch eine Einwilligung zur Einrichtung und Führung des fortlaufenden Kund*innenkontos abgedeckt. Da Kund*innen, die einen Gastzugang wählen, damit regelmäßig zugleich zu erkennen geben, dass sie eine Werbeansprache ablehnen, ist eine andere Rechtsgrundlage für diese Datennutzung nicht ersichtlich. Gleiches gilt für das Speichern etwaiger Zahlungsmittel wie Kreditkarten. Siehe dazu die Empfehlungen des EDSA 02/2021 zur Rechtsgrundlage für die Speicherung von Kreditkartendaten ausschließlich zum Zweck der Erleichterung weiterer Online-Transaktionen.

4. Die von den Verantwortlichen verarbeiteten Daten müssen in einer für die Kund*innen transparenten Weise verarbeitet werden.

Verantwortliche haben sowohl bei Einrichtung eines Gastzugangs als auch bei Einrichtung des fortlaufenden Kund*innenkontos ihre Informationspflichten bei erstmaliger Datenerhebung zu erfüllen. Die Einrichtung des fortlaufenden Kund*innenkontos im Wege einer Einwilligung nach Art. 6 Abs. 1 S. 1 Buchstabe a) DS-GVO setzt zusätzlich voraus, dass diese in informierter Weise erfolgt.

Sowohl für die Einwilligung gemäß Art. 7 DS-GVO, als auch bei einer für die Vertragserfüllung erforderlichen Datenverarbeitung sind die Kund*innen in verständlicher Sprache über die Einzelheiten der Datenverarbeitung zu informieren (Art. 7 Abs. 2 und Art. 12 – 14 DS-GVO).

- **23.03.2022 – Zur Task Force Facebook-Fanpages**

  Die DSK nimmt das von der Taskforce Facebook-Fanpages erstellte Kurzgutachten zur Frage der datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages vom 18.03.2022 zur Kenntnis und stimmt der Bewertung zu.

  Es bildet für die Mitglieder der DSK eine wichtige Grundlage ihrer aufsichtsbehördlichen Tätigkeit gegenüber öffentlichen und nichtöffentlichen Stellen.

  Aufgrund ihrer Vorbildfunktion stehen öffentliche Stellen zuvörderst im Fokus. Deshalb werden die Mitglieder der DSK im Rahmen ihrer Zuständigkeit

  - die obersten Landes- bzw. Bundesbehörden über den Inhalt des Kurzgutachtens zeitnah informieren,
  - überprüfen, ob Landes- bzw. Bundesbehörden Facebook-Fanpages betreiben,
  - darauf hinwirken, dass von Landes- bzw. Bundesbehörden betriebene Facebook-Fanpages deaktiviert werden, sofern die Verantwortlichen die datenschutzrechtliche Konformität nicht nachweisen können.

    Dieser Nachweis betrifft vor allem

  - den Abschluss einer Vereinbarung nach Art. 26 DSGVO über die gemeinsame Verantwortlichkeit mit Facebook,
  - ausreichende Informationen über die gemeinsamen Datenverarbeitungen gegenüber den die Fanpages Nutzenden gemäß Art. 13 DSGVO,

- die Zulässigkeit zur Speicherung von Informationen in der Endeinrichtung des Endnutzers und der Zugriff auf diese Informationen gemäß § 25 TTDSG sowie
- die Zulässigkeit der Übertragung personenbezogener Daten in den Zugriffsbereich von Behörden in Drittstaaten.

Hinweis: Der Beschluss wurde mehrheitlich mit einer Gegenstimme gefasst. Die Gegenstimme richtet sich gegen die Ausführungen des dritten Absatzes.

- **15.04.2020 – Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu den Einwilligungsdokumenten der Medizininformatik-Initiative des Bundesministeriums für Bildung und Forschung**

  Aus Sicht der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder bestehen gegen den bundesweiten Einsatz der Einwilligungsdokumente der Medizininformatik-Initiative in der Version 1.6b, bestehend aus einer Patienteninformation und einer Einwilligungserklärung, sowie der zugehörigen Handreichung in der Version 0.9b keine Bedenken, unter der Voraussetzung, dass in den Einwilligungsdokumenten auf die Verarbeitung genetischer Daten aus Biomaterialien und insbesondere das damit verbundene Risiko der Rückverfolgbarkeit explizit hingewiesen wird, die Wahrung des jederzeitigen Widerrufs-rechts trotz der Übertragung des Eigentums an Biomaterialien klarer zum Ausdruck kommt und Patienten auf die Möglichkeit hingewiesen werden, sich bei einem E-Mail-Verteiler zu registrieren, der rechtzeitig vor Beginn über neue Forschungsprojekte auf Basis der Daten der Medizininformatik-Initiative informiert. In der Handreichung ist außerdem die Passage zu streichen, in der darauf hingewiesen wird, dass zukünftig die Datenübermittlung in Drittstaaten zulässig sein soll.

Anhang zum Informationsfreiheitsbericht

Veröffentlichungen der Konferenz der Informationsfreiheitsbeauftragten (IFK) in Deutschland 2022 und 2021

- **Entschließung zwischen der 42. und der 43. Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 26. Oktober 2022**

  Niedersachsen: Die Zeit für ein Transparenzgesetz ist gekommen!

  Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fordert die an den Koalitionsverhandlungen Beteiligten in Niedersachsen auf, den Erlass eines Transparenzgesetzes in den Koalitionsvertrag aufzunehmen.

  Der Bund und die Länder Baden-Württemberg, Berlin, Brandenburg, Bremen, Hamburg, Hessen, Nordrhein-Westfalen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen verfügen jeweils über ein Transparenz- oder Informationsfreiheitsgesetz. Diese Gesetze gewähren einen grundsätzlichen Anspruch auf Zugang zu Informationen öffentlicher Stellen, ohne dass ein berechtigtes Interesse dargelegt werden muss. Moderne Gesetze sehen zudem die Verpflichtung öffentlicher Stellen vor, Informationen proaktiv und antragsunabhängig bereitzustellen. Unabhängige Informationsfreiheitsbeauftragte kontrollieren die Einhaltung der Vorschriften. Niedersachsen bleibt bisher hinter dem bundesweiten Standard zurück, da es dort an einem solchen Gesetz fehlt.

  Eigentlich hätte dieser Zustand schon längst beseitigt sein sollen. Im Jahr 2017 hatte die damalige Landesregierung die Einführung eines Transparenzgesetzes geplant. Nach dem Regierungswechsel geriet das Projekt jedoch ins Stocken. Die Regelungen der anderen Länder sollten zunächst evaluiert werden. Aus Bund und

Ländern liegen inzwischen Evaluierungen vor, die zu dem einhelligen Ergebnis kommen, dass sich die Transparenz- bzw. Informationsfreiheitsgesetze bewährt haben. Es besteht daher kein Grund, länger zu warten.

Öffentliche Stellen in Niedersachsen müssen vergleichbaren Transparenzpflichten unterliegen wie die öffentlichen Stellen anderer Länder und des Bundes. Nur wer gut informiert ist, kann fundiert mitreden und sich beteiligen. Die IFK fordert daher alle in Niedersachsen politisch Verantwortlichen auf, diesen Schritt hin zu einer offeneren Verwaltung mit mehr Partizipationsrechten der Bürgerinnen und Bürger zu vollziehen.

- **Entschließungen der 42. Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 30. Juni 2022 in Kiel**

  SMS in die Akte: Behördliche Kommunikation unterliegt umfassend den Regeln der Informationsfreiheit!
  Behördliche Kommunikation erfolgt nicht mehr nur in Papierform oder per E-Mail. Viele Behörden nutzen vermehrt Kommunikationsformen wie Kurznachrichtendienste, Messenger-Dienste, soziale Medien, aber auch SMS. Auch diese Behördenkommunikation kann eine amtliche Information sein.

  In seinem Urteil vom 28. Oktober 2021, Az. 10 C 3.20, ist das Bundesverwaltungsgericht davon ausgegangen, dass eine nichtöffentliche Twitter-Direktnachricht durchaus eine amtliche Information im Sinne des Informationsfreiheitsgesetzes sein kann. Jedoch müsse die Aufzeichnung der Information amtlichen Zwecken dienen, also „Aktenrelevanz“ haben. Diese Voraussetzung hat das Gericht im konkreten Einzelfall aufgrund des „bagatellartigen Charakters“ als nicht erfüllt angesehen.

  Grundsätzlich gilt, dass alle wesentlichen Vorgänge, die ersichtlich für eine Entscheidung von Bedeutung sein können, zu den Akten zu nehmen sind. Das gilt insbesondere für jegliche verkörperte Kommunikation zwischen Regierungsmitgliedern, kann

aber auch weitere Behördenvertreterinnen und -vertreter betreffen, die die oben genannten Kommunikationsformen nutzen. Vor diesem Hintergrund kritisiert die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK), dass gerade in diesem Bereich eine ordnungsgemäße Dokumentation oftmals nicht erfolgt und so im Ergebnis relevante Informationen über das Regierungs- und Verwaltungshandeln dem Informationszugang entzogen werden.

Der Staat muss bei der Nutzung von Kommunikationsmedien stets seine Dokumentations- und Informationspflichten erfüllen. Die IFK fordert daher die Verwaltungen in Bund und Ländern auf, jegliche relevante behördliche Kommunikation[1] über Kurznachrichtendienste, Messenger-Dienste, soziale Medien und SMS, insbesondere von Mitgliedern der Regierung, zu dokumentieren, um den Informationszugang zu garantieren.

[1] Hinweise zur datenschutzgerechten Gestaltung der Kommunikation von öffentlichen und nichtöffentlichen Stellen über soziale Medien lassen sich den Veröffentlichungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) entnehmen, u. a.:
Beschluss „Technische Datenschutzanforderungen an Messenger-Dienste im Krankenhausbereich“ vom 29. April 2021, https://www.datenschutzkonferenz-online.de/media/st/20210429_DSK_Stellungnahme_Messengerdienste_Krankenhausbereich.pdf;
Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages, 18. März 2022, https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK_Kurzgutachten_Facebook-Fanpages_V1_18.03.2022.pdf;
Beschluss „Zur Task Force Facebook-Fanpages“ vom 23. März 2022, https://datenschutzkonferenz-online.de/media/dskb/DSK_Beschluss_Facebook_Fanpages.pdf;
FAQ zu Facebook-Fanpages, 22. Juni 2022, https://www.datenschutzkonferenz-online.de/media/oh/20220622_oh_10_FAQ_Facebook_Fanpages.pdf.

Keine Umgehung der Informationsfreiheit durch Errichtung von Stiftungen bürgerlichen Rechts!

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) stellt fest, dass sich das Informationsfreiheitsrecht gegenüber Stiftungen, die öffentliche Aufgaben wahrnehmen, nicht nach deren Organisationsform richten darf. Entscheidend ist die Natur der wahrgenommenen Aufgabe. Nehmen Stiftungen öffentliche Aufgaben wahr, hat die Öffentlichkeit einen Anspruch auf entsprechende Informationen – und zwar unabhängig davon, ob es sich um eine Stiftung öffentlichen oder bürgerlichen Rechts handelt.

Anlass dieser Feststellung ist der Umgang mit dem Zugang zu Informationen über die „Stiftung Klima- und Umweltschutz MV“. Die Landesregierung Mecklenburg-Vorpommern hatte diese vor Beginn des russischen Angriffskriegs auf die Ukraine mit dem erklärten Ziel gegründet, Maßnahmen des Umwelt- und Klimaschutzes durchzuführen und zu fördern. Im Rahmen der Stiftungsgründung machte die Landesregierung deutlich, dass ein weiteres Ziel der Stiftung sei, die Erdgaspipeline Nord Stream 2 fertigzustellen. Abgesehen von der teilweisen öffentlichen Finanzierung hatte das Land auch Einfluss auf die personelle Besetzung der Stiftungsgremien. Dass es sich hier um die Wahrnehmung öffentlicher Aufgaben handelt, ist offenkundig.

Die Landesregierung und die Stiftung verweigern der Öffentlichkeit den vollständigen Zugang zu angefragten Informationen. Im Wesentlichen argumentieren sie damit, dass Stiftungen bürgerlichen Rechts der Informationsfreiheit entzogen seien. Demgegenüber hat das Landgericht Schwerin in einem presserechtlichen Verfahren (Urteil vom 8. April 2022, Az. 3 O 65/22) entschieden, dass die mit öffentlichen Mitteln finanzierte Landesstiftung öffentliche Zwecke verfolgt und ein beherrschender Einfluss der Landesregierung besteht. Somit sei diese private Stiftung genauso wie eine Behörde verpflichtet, den Medien gegenüber Auskünfte zu erteilen.

Die IFK bekräftigt, dass auch nach allgemeinem Informationszugangsrecht die Transparenz im Falle der Wahrnehmung öffentlicher Aufgaben durch Stiftungen des bürgerlichen Rechts gewährleistet sein muss und nicht durch gesetzliche Bereichsausnahmen ausgeschlossen werden darf.

- **Entschließungen der 41. Konferenz der Informationsfreiheitsbeauftragten in Deutschland vom 3. November 2021**

  EU-Richtlinie zum Whistleblowerschutz zeitnah umsetzen! Hinweisgeberinnen und Hinweisgeber umfassend und effektiv schützen!
  Whistleblowerinnen und Whistleblower sind Menschen, die Hinweise auf erhebliche Missstände in Unternehmen oder Behörden geben. Sie helfen, dadurch gravierende Rechtsverstöße aufzudecken, deren Beseitigung im öffentlichen Interesse liegt. Zumeist geschieht dies dadurch, dass sie Informationen „befreien“, Rechtsverstöße den Behörden melden oder bei deren Untätigkeit die Medien informieren. Whistleblowerinnen und Whistleblower sorgen so für Transparenz und Aufklärung. Die Information der Öffentlichkeit steht jedoch regelmäßig in einem Spannungsverhältnis zu ihren arbeitsrechtlichen Loyalitäts- und Verschwiegenheitspflichten. Wenn Beschäftigte Rechtsverstöße transparent machen, laufen sie nicht selten Gefahr, insbesondere gegen arbeitsvertragliche Pflichten zu verstoßen. Hinweisgebende riskieren durch die Offenlegung von Informationen oftmals nicht nur ihren Arbeitsplatz, sondern auch ihre Karriere und ihr Ansehen.

  Vor diesem Hintergrund hat die EU im Oktober 2019 eine Richtlinie erlassen, die nicht nur die Voraussetzungen für den Schutz von Whistleblowerinnen und Whistleblowern, sondern auch einen Mindestschutzstandard festlegt (Richtlinie (EU) 2019/1937). Die Richtlinie gilt für die Meldung von Verstößen gegen europäisches Recht. Sie erlaubt es den Mitgliedstaaten aber ausdrücklich, den Schutz auch auf Hinweisgebende zu erstrecken, die Verstöße gegen nationales Recht melden. Whistleblowerinnen und Whist-

leblower, die sich an das in ihr vorgegebene Meldeverfahren halten, sollen vor jeglichen Repressalien geschützt werden. Stichtag für eine fristgemäße Umsetzung ist der 17. Dezember 2021. Die Bundesrepublik Deutschland hat die Richtlinie bisher jedoch nicht umgesetzt, da sich die letzte Bundesregierung nicht über die Reichweite eines Whistleblower-Schutzgesetzes einigen konnte.

Eine Ungleichbehandlung der Whistleblowerinnen und Whistleblower ist nicht nachvollziehbar. Warum sollte jemand, der Verstöße gegen europäisches Recht meldet, besser geschützt werden als jemand, der Verstöße gegen deutsches Recht offenbart? Schließlich liegt es im öffentlichen Interesse, Kenntnis von jedem relevanten Rechtsverstoß zu erhalten und diesen abzustellen. Auch können Whistleblowerinnen und Whistleblower wegen der Verzahnung von europäischem und nationalem Recht vorab oftmals nur sehr schwer einschätzen, welche Rechts-materie konkret betroffen ist. Es ist deshalb wichtig, dass der Gesetzgeber alle Hinweisgebende gleichermaßen gut schützt und Rechtssicherheit schafft.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fordert den Bundes-gesetzgeber auf, die EU-Richtlinie zum Schutz von Whistleblowerinnen und Whistleblowern so schnell wie möglich umzusetzen und den Schutz auch auf Hinweisgebende zu erstrecken, die Verstöße gegen nationales Recht melden.

Tromsø-Konvention ratifizieren und einheitlichen Mindeststandard für den Zugang zu Informationen in ganz Deutschland schaffen!
Die IFK fordert die neue Bundesregierung auf, die Tromsø-Konvention in der neuen Legislaturperiode zu unterzeichnen und das Ratifizierungsverfahren einzuleiten.

Am 1. Dezember 2020 ist die Konvention Nr. 205 des Europarats über den Zugang zu amtlichen Dokumenten (Tromsø-Konvention) vom 18. Juni 2009 ohne deutsche Beteiligung in Kraft getreten.

Bei der Konvention handelt es sich um einen völkerrechtlichen Vertrag, der seine Mitgliedstaaten verpflichtet, im Wege der nationalen Gesetzgebung ein allgemeines Recht auf Zugang zu amtlichen Dokumenten der öffentlichen Verwaltung zu schaffen und dabei Mindeststandards bei der Bearbeitung von Informationszugangsanträgen festzulegen. Die Konvention gilt damit als weltweit erstes internationales Abkommen, das ein generelles Recht auf Informationszugang zu amtlichen Dokumenten konstituiert. Im Falle des Verstoßes eines Vertragsstaates kann der Europäische Gerichtshof für Menschenrechte angerufen werden.

Die Bundesrepublik Deutschland hat auf eine Unterzeichnung und Ratifikation des Vertrags bisher verzichtet. Die letzte Bundesregierung argumentierte, dass mit dem Informationsfreiheitsgesetz des Bundes (IFG) ein solcher Mindeststandard für ganz Deutschland bereits geschaffen und das Ziel der Konvention erreicht sei. Eine Ratifikation sei daher nicht notwendig.

Diese Auffassung ist unzutreffend, denn das IFG gilt nur für den Bund, nicht jedoch für die Länder. Nicht alle Länder haben ein Informationsfreiheitsgesetz mit Landesbeauftragten für die Informationsfreiheit geschaffen. Bayern, Niedersachsen und Sachsen haben derzeit weder Informationsfreiheitsgesetze noch entsprechende Landesbeauftragte. Ein einheitlicher Mindeststandard für den Zugang zu Informationen, den die Konvention vorsieht, existiert in Deutschland daher nicht.

Hinzukommt, dass sich die Regelungen der Konvention nicht vollkommen mit den Vorschriften der bereits vorhandenen Informationsfreiheitsgesetze des Bundes und der Länder decken. Die Konvention ist insbesondere bei der Erhebung von Gebühren wesentlich bürgerfreundlicher als das deutsche Recht.

Wer Transparenz und Informationsfreiheit dauerhaft verwirklichen will, muss den Zugang zu amtlichen Informationen auch völkerrechtlich garantieren. Mehr als zwölf Jahre nach Entstehung des Abkommens wird es höchste Zeit, dass Deutschland sich zu einem europaweiten Mindeststandard für den Informationszugang bekennt.

Umweltinformationen: Beratungs- und Kontrollkompetenz auch auf Landesbeauftragte für Informationsfreiheit übertragen!

Das Gutachten zur Evaluierung des Umweltinformationsgesetzes des Bundes (UIG) hat im Oktober 2020 vorgeschlagen, eine Bundesbeauftragte oder einen Bundesbeauftragten für Umweltinformationsfreiheit zu schaffen, die oder der für die Einhaltung und Kontrolle der Vorschriften des Umweltinformationsrechts zuständig ist. In dem Gutachten wird empfohlen, diese Aufgabe der bzw. dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zu übertragen. Der Bundesgesetzgeber ist dieser Empfehlung im März 2021 gefolgt und hat der bzw. dem BfDI in § 7a UIG ausdrücklich die Befugnis gegeben, die Einhaltung des Umweltinformationsrechts zu kontrollieren.

Während im Bund nun explizit eine einheitliche Beratungs- und Kontrollkompetenz für beide Rechtsmaterien besteht, ist dies in den meisten Ländern bisher nicht der Fall. Die Landesbeauftragten für Informationsfreiheit kontrollieren oftmals nur die Einhaltung des allgemeinen In-formationsfreiheitsrechts, nicht jedoch des Umweltinformationsrechts. Da sich die Rechtsmaterien nicht wesentlich unterscheiden, bleibt ihre vorhandene Fachkompetenz ungenutzt. Bei den Menschen, die sich an sie wenden, stößt dies auf Unverständnis. Sie wollen dahingehend unterstützt werden, dass ihrem Anliegen umfassend Rechnung getragen wird. Gleiches gilt für die Behörden, die die Informationsfreiheitsbeauftragten schon jetzt im Umweltinformations-recht um Unterstützung bitten.

Eine antragstellende Person kann derzeit in Streitfällen mit Bundesbehörden zwar auf die Unterstützung des Bundesbeauftragten zählen. Die Schlichtung im Streit mit Landesbehörden oder Gemeinden bleibt ihr hingegen weitestgehend versagt, nur weil sich der Antrag auf Informationen über die Umwelt an eine Landesbehörde richtet. Diese Ungleichbehandlung lässt sich nicht nachvollziehbar begründen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher die Landesgesetzgeber auf, dem Vorbild des Bundes zu folgen und den Landesbeauftragten für Informationsfreiheit, soweit noch nicht geschehen, ausdrücklich auch die Beratungs- und Kontrollkompetenz für das Umweltinformationsrecht zu übertragen. Zur Erfüllung dieser neuen Aufgabe sind die Beauftragten mit ausreichenden personellen und sachlichen Mitteln auszustatten.

- **Entschließungen der 40. Konferenz der Informationsfreiheitsbeauftragten in Deutschland am 2. Juni 2021**

  Mehr Transparenz beim Verfassungsschutz – Vertrauen und Legitimation stärken!
  Die Verfassungsschutzbehörden in Bund und Ländern haben die Aufgabe, die freiheitlich- demokratische Grundordnung der Bundesrepublik Deutschland vor Bedrohungen zu schützen. Die im Vorfeld konkreter Gefahren zur Erfüllung ihrer Aufgaben vorgenommenen Maßnahmen der Informationsgewinnung unterliegen dabei zumeist der Geheimhaltung. Dies bedeutet aber nicht, dass ihre gesamte Tätigkeit zwangsläufig intransparent sein muss.

  Transparenzpflichten, wie die Pflicht zur Erstellung von Verfassungsschutzberichten, finden sich nicht nur in den Verfassungsschutzgesetzen des Bundes und der Länder (vgl. § 16 BVerfSchG). Auch die Presse hat grundsätzlich einen presserechtlichen Auskunftsanspruch, sofern nicht das operative Geschäft der Behörden betroffen ist. So sind z.B. Themen und

Teilnehmende von Hintergrundgesprächen auch gegen den Willen der Behörden transparent zu machen. Bürgerinnen und Bürger haben darüber hinaus nach den Umweltinformationsgesetzen des Bundes und der Länder prinzipiell einen Anspruch auf Zugang zu Umweltinformationen gegenüber den Verfassungsschutzbehörden.

Wenn die Behörden nach dem Presse- oder dem Umweltinformationsrecht Auskunft geben müssen, sofern nicht ihre geheime Tätigkeit betroffen ist, erschließt es sich nicht, warum sie auf entsprechende allgemeine Fragen nach dem Informationsfreiheitsrecht schweigen dürfen. Mehr Transparenz stärkt das Vertrauen in die Verfassungsschutzbehörden und erhöht ihre Legitimation.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert daher die Gesetzgeber in Bund und den betroffenen Ländern auf, die Bereichsausnahmen für den Verfassungsschutz abzuschaffen und die entsprechende Ausnahmeregelung auf den Schutz konkreter Sicherheitsbelange im Einzelfall zu beschränken.

Forderungen für die neue Legislaturperiode des Bundes: Ein Transparenzgesetz mit Vorbildfunktion schaffen!
Informationen sind die Basis einer Demokratie. Ein demokratischer Staat kann nicht ohne freie und möglichst gut informierte öffentliche Meinung bestehen. Das Recht auf Zugang zu Informationen ist ein zentrales Element zur Regelung des Informationsflusses von staatlichen Stellen zu Bürgerinnen und Bürgern in Deutschland. Moderne Transparenzgesetze stellen die Informationen über ein Register im Internet voraussetzungs- und kostenlos zur Verfügung.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fordert den Gesetzgeber daher auf, das Informationsfreiheitsrecht des Bundes in der nächsten Legislaturperiode zu modernisieren und das Informationsfreiheitsgesetz des Bundes

zu einem modernen Transparenzgesetz mit einem Transparenzregister weiterzuentwickeln. Die IFK fordert insbesondere:

A. Weiterentwicklung des Informationsfreiheitsgesetzes in ein Transparenzgesetz mit einem Transparenzregister

- Das Informationsfreiheitsgesetz (IFG) des Bundes muss zu einem echten Transparenzgesetz mit einem gesetzlich geregelten Transparenzregister weiterentwickelt werden.
- In dem Transparenzgesetz des Bundes müssen das IFG und das Umweltinformations-gesetz (UIG) zusammengelegt werden. Unterschiedliche Regelungen im IFG und UIG verkomplizieren den Zugang zu Informationen unnötig. Die Zusammenfassung der Informationsansprüche in einem Gesetz ist übersichtlicher und bürgerfreundlicher. „Ein einheitliches, übergreifendes Transparenzgesetz würde die Bekanntheit, die Anwenderfreundlichkeit und die Durchsetzungskraft aller Informationszugangsgesetze erhöhen.“ (vgl. Umweltbundesamt (Dez. 2020): Evaluation des UIG; S. 163)
- Das Transparenzregister sollte wie in mehreren Ländern einen Katalog veröffentlichungspflichtiger Informationen enthalten. Die Veröffentlichung weiterer geeigneter Informationen sollte ausdrücklich zugelassen werden.
- Zu den Informationen, die im Transparenzregister veröffentlicht werden, sollten insbesondere Kabinettbeschlüsse und deren dazugehörige Kabinettvorlagen, Verträge von öffentlichem Interesse, Gutachten, Studien und wesentliche Unternehmensdaten staatlicher Beteiligungen gehören.
- In das Gesetz sollte eine Regelung aufgenommen werden, nach der Informationen, die auf individuellen Antrag hin zugänglich gemacht wurden, auch im Informationsregister veröffentlicht werden können (Access for one = access for all), wenn ein öffentliches Interesse an der Veröffentlichung besteht.

B. Bereichsausnahmen und Ausschlussgründe

- Die Ausschlussgründe des IFG bedürfen einer grundlegenden Überarbeitung, da einige Ausschlussgründe überflüssig sind oder sich überschneiden. Sie sollten reduziert und harmonisiert werden.
- Eine allgemeine Güterabwägung zwischen Informations- und Geheimhaltungsinteresse (sog. public interest test) sollte als zusätzliches Korrektiv eingeführt werden.
- Die Bereichsausnahme für den Verfassungsschutz geht zu weit und sollte in einem neuen Transparenzgesetz nicht mehr enthalten sein.

C. Regelungen zur Förderung der Informationsfreiheit

- Die Anforderungen an die Informationsfreiheit sind i. S. v. „Informationsfreiheit by Design“ bereits von Anfang an in die Gestaltung der IT-Systeme und organisatorischen Prozesse einzubeziehen.
- In dem neuen Transparenzgesetz sollte die Benennung eines behördlichen Informationsfreiheitsbeauftragten verbindlich vorgesehen werden.

D. Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

- Der Bundesbeauftragte sollte eine Anordnungsbefugnis bekommen, um Rechtsverstöße gegen das Informationsfreiheitsrecht beseitigen zu können.

E. Rechtspolitik

- Die Bundesrepublik Deutschland sollte in der neuen Legislaturperiode die Tromsö-Konvention ratifizieren. Die Tromsö-Konvention ist ein im Jahr 2020 in Kraft getretener völkerrechtlicher Vertrag, der Mindeststandards setzt für das Recht auf Zugang zu amtlichen Dokumenten.

Mehr Transparenz durch behördliche Informationsfreiheitsbeauftragte!

Alle öffentlichen Stellen sollten Beauftragte für Informationsfreiheit benennen, so wie es bereits für den Datenschutz verpflichtend ist. In zwei Ländern ist dies schon im Gesetz vorgesehen: Sowohl in Rheinland-Pfalz als auch in Thüringen soll durch Bestellung von behördlichen Beauftragten das Recht auf Informationszugang gefördert werden.
Die Vorteile einer solchen Bestellung liegen auf der Hand:

- Informationsfreiheitsbeauftragte können die öffentlichen Stellen in ähnlicher Weise unterstützen und die Informationsfreiheit fördern, wie es im Bereich des Datenschutzes schon seit Langem vorgesehen ist.
- Informationsfreiheitsbeauftragte können ihren öffentlichen Stellen behilflich sein, wenn diese Fragen zur Auslegung des Informationsfreiheitsgesetzes haben, beispielsweise wenn es um die Berechtigung und den Umfang erhobener Informationszugangsansprüche geht. Dies garantiert zugleich die einheitliche Rechtsanwendung innerhalb der öffentlichen Stelle.
- Sie können zudem sicherstellen, dass eine auf einen Informationszugang gerichtete Anfrage als Antrag zur Verwirklichung eines subjektiven Rechts und nicht lediglich als „einfache Bitte“ qualifiziert, sondern fristgerecht bearbeitet wird.
- Zielführend wäre auch, dass sie die Bearbeitung der entsprechenden Anträge koordinieren. Hierbei können die Informationsfreiheitsbeauftragten unterstützend zur Verfügung stehen. Dies führt letztlich zu einer Arbeitserleichterung, da die Beschäftigten von deren Kenntnis im Informationsfreiheitsrecht profitieren.
- Die Informationsfreiheitsbeauftragten unterrichten und beraten die öffentlichen Stellen auch zu der proaktiven Veröffentlichung von Informationen.
- Gleichzeitig stehen sie Antragstellenden für Fragen im Zusammenhang mit dem Informationsfreiheitsgesetz als Ansprechstellen zur Verfügung.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) fordert daher den Bundes- und die Landesgesetzgeber auf, die Bestellung von behördlichen Informationsfreiheitsbeauftragten in allen deutschen Informationsfreiheitsgesetzen verbindlich vorzusehen. Die IFK empfiehlt informationspflichtigen Stellen, im Rahmen ihrer Organisationshoheit auch ohne Verpflichtung behördliche Informationsfreiheitsbeauftragte zu benennen.