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

Bettina Gayk

zum Datenschutz

für die Zeit vom 1. Januar 2020 bis zum 31. Dezember 2020

und zur Informationsfreiheit

für die Zeit vom 1. Januar 2019 bis zum 31. Dezember 2020

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: 26. Bericht LDI NRW

ISSN: 0179–2431

Düsseldorf 2021

Gedruckt auf chlorfreiem Recyclingpapier

Inhaltsverzeichnis

Vorwort

Dieser Bericht umfasst eine Zeit, die aus mehreren Gründen ungewöhnlich ist. Meine Vorgängerin im Amt, Helga Block, ist in der Mitte des Berichtszeitraums in den verdienten Ruhestand eingetreten. Sie hat eine gut organisierte Behörde mit hoch motivierten Mitarbeiter*innen hinterlassen, die unter Leitung meines Vertreters, Roul Tiaden, die Arbeit ambitioniert weitergeführt haben. Das belegt dieser Bericht eindrücklich. Dafür danke ich Helga Block, Roul Tiaden und allen Beteiligten ganz herzlich. Ich selbst habe das Amt der Landesbeauftragten für Datenschutz und Informationsfreiheit des Landes Nordrhein-Westfalen am 1. Juni 2021 angetreten und lege hier also einen Bericht vor, der das Jahr vor meinem Amtsantritt betrachtet.

In den Berichtszeitraum fällt der Beginn der Corona-Pandemie. Auf den ersten Blick hat das nicht viel mit Datenschutz oder Informationsfreiheit zu tun. Aber ich erinnere nur an die Diskussion über eine datenschutzgerechte Corona-App zur Kontaktnachverfolgung. Der Umgang mit Kontaktangaben in Restaurants und mit Daten in Testzentren kam durch Corona auf die Datenschutzagenda. Homeoffice in Wirtschaft und Verwaltung und die Digitalisierung der Schulen wurden in dieser Zeit im Eiltempo vorangetrieben. Die Beratung meiner Behörde war dazu gefragt.

Einige haben ihr Recht auf Informationszugang genutzt, um der Verwaltung bei den Maßnahmen zur Bewältigung der Pandemie kritisch auf den Zahn zu fühlen. Wie sinnvoll es ist, Bürger*innen aktiv zu informieren, hat das wachsende Informationsangebot der Landesregierung zur Corona-Lage gezeigt. Mit modernen Dash-Boards sind hier transparente und informative

Angebote möglich. Ich hoffe, dass dies einen Impuls zur Weiterentwicklung des Informationsfreiheitsgesetzes hin zu einem Transparenzgesetz geben kann. An dieser Stelle sei erwähnt, dass in diesem Jahr zugleich mit dem jährlichen Datenschutzbericht auch der alle zwei Jahre zu erstellende Informationsfreiheitsbericht vorgelegt wird.

Corona hat auf verschiedene Lebensbereiche ein Brennglas gelegt, auch auf den Datenschutz. Die durch Corona beförderte Digitalisierungswelle zeigte, dass der Gedanke „data protection by design“ in den Datenverarbeitungsanwendungen auf dem Markt leider noch viel zu wenig beachtet wird. Anwendungen etwa, die per se zu einer Übermittlung von Daten in Drittstaaten führen, sind in manchen Bereichen kaum oder gar nicht datenschutzkonform einsetzbar. Dies war unter anderem im Bereich der Videokonferenztechnik festzustellen. Hier wünsche ich mir gerade von großen Unternehmen, dass sie die rechtlichen Regelungen in der Europäischen Union bei ihren Produkten von vornherein berücksichtigen.

Die Corona-App ist ein Beispiel dafür, wie schief manche Diskussionen über Datenschutz geführt werden: Die App wurde zurecht gelobt für ihre Datenschutzkonformität. Solche Apps können aber die Kontaktnachverfolgung mit viel menschlicher Recherchearbeit allenfalls unterstützen, jedoch nicht ersetzen. Statt dies zu erkennen, wurde der Datenschutz zum Sündenbock erklärt. Einzelne verstiegen sich sogar zu der Auffassung, der Datenschutz koste Menschenleben.

„Der Datenschutz“ erscheint in einer solchen Aussage als technischer, sehr abstrakter Begriff. Leicht lässt sich deshalb ein Interesse anführen, das auf den ersten Blick konkreter und wichtiger zu sein scheint: Leben

und Gesundheit, aber auch schon ein wirtschaftliches oder sonstiges Interesse. Viele Menschen gehen außerdem sehr freigiebig mit ihren Daten um und erlauben deren Nutzung für kleine Vorteile, wie einen Rabatt oder kostenlose Informationen. Warum also sollte der Datenschutz, der den Betroffenen selbst manchmal nicht viel bedeutet, so wichtig sein, wenn Daten zur Bekämpfung der Pandemie gesammelt werden? Der Begriff Datenschutz führt immer etwas in die Irre, weil er gerade nicht Selbstzweck ist. Datenschutz ist ein Mittel, um die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen. Das ist dann doch ein sehr gewichtiges Argument, das es mit anderen rechtlichen Interessen abzuwägen gilt. Nur darum geht es beim Datenschutz.

Die Technik ermöglicht heute über mobile Endgeräte, fast jede Regung der Nutzer*innen zu erfassen, bis hin zum Herzschlag. Tracking der Internetnutzung ist die Basis für umfassende Nutzer*innenprofile. Und die Entwicklung von künstlicher Intelligenz verspricht, potentielle Verhaltensweisen von Menschen demnächst vorwegzunehmen. Es stehen reichlich Daten und ausgefeilte Techniken zur Verfügung, die Erkenntnisse oder Vermutungen über Menschen generieren können. Nicht immer sind die Daten aktuell und auch nicht immer zum Vorteil der Betroffenen. Am Ende entscheidet ein Profil, ein Scorewert oder eine nicht aktuelle Datenlage, ob eine Person eine Wohnung, einen Kredit oder Vertrag erhält. Oder ob sie in den Fokus behördlicher Überprüfungen oder in den Genuss staatlicher Leistungen gerät. Oft bleiben die datenbasierten Hintergründe für die Betroffenen intransparent. Der Datenschutz will die Menschen vor dem Hintergrund dieser Möglichkeiten vor ungerechtfertigten Datenverarbeitungen zu ihrem Nachteil schützen.

Der Grundsatz der Datensparsamkeit ist hier ein zentrales Element, das sicherstellt, dass Daten gar nicht erst entstehen oder so zeitnah wie möglich gelöscht werden, damit Zugriffe auf solche Daten unterbleiben. Deswegen ist dies ein wesentlicher Grundsatz, auf den meine Behörde bei ihren Arbeiten achtet – sowohl bei der Beratung des Gesetzgebers und der Verantwortlichen, als auch bei der Durchsetzung von Datenschutzrecht. Mein Rat an die Bürger*innen ist in diesem Zusammenhang, dass sie selbst auch nicht zu freigiebig mit ihren Daten sein sollten.

Bettina Gayk

Sommer 2021

1. Teil: Datenschutzbericht

1. Überblick

- **Eingaben**

  Im Jahr 2020 haben uns insgesamt rund **12.150** schriftliche Eingaben erreicht, einschließlich Meldungen nach Art. 33 DS-GVO (sog. Datenpannen).

  Sie bleiben damit seit der Datenschutzreform auf einem hohen Niveau. Deutlich gestiegen ist die Zahl der förmlichen Begleitung bei Rechtsetzungsvorhaben von 21 (2019) auf 44 (2020).

  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“.

  Unser Bestreben ist es nach wie vor, alle Eingaben im Rahmen unserer Kapazität zeitnah zu bearbeiten. Das ist leider nicht immer möglich, sodass wir bei der Bearbeitung neben der Einhaltung gesetzlicher Fristen vorrangig die Schwere der geltend gemachten Verstöße und das Risiko der Datenverarbeitung berücksichtigen müssen.

- **Corona-Pandemie und Datenschutz**

  Die Corona-Pandemie sowie die Maßnahmen zu ihrer Eindämmung haben sich – wie bei vielen anderen öffentlichen Stellen in NRW – auch auf unsere Arbeit ausgewirkt, und zwar sowohl in organisatorischer als auch in inhaltlicher Hinsicht.

Auswirkungen auf die Organisation

Wir haben im gesamten Jahr 2020 den Dienstbetrieb aufrechterhalten können und waren so für die Bürger*innen und Verantwortliche da. Jedoch mussten auch wir verschiedene Maßnahmen treffen, um das Infektionsrisiko zu reduzieren. Dadurch kam es im Einzelfall zu Einschränkungen bei der Erreichbarkeit und zu Verzögerungen unserer Reaktionen. Planungen zu Fortbildungs-, Vortrags- und Erfahrungsaustauschveranstaltungen mussten wir zum Teil einstweilen einstellen, weil Präsenztermine aus Gründen der Gesundheitsvor- und -fürsorge bis auf Weiteres nicht mehr in Betracht kamen.

Inzwischen und für die Zukunft stehen uns so wie auch vielen anderen Behörden in NRW Videotools und die entsprechenden Endgeräte zur Verfügung, um an derartigen Veranstaltungen via Internet und somit quasi aus „sicherer Distanz“ teilzunehmen, und zwar wahlweise aus den Dienststellen oder dem Homeoffice.

Auswirkungen im Öffentlichen Bereich

Insgesamt waren die datenschutzrelevanten Fragen rund um die Pandemie und die getroffenen Schutzmaßnahmen bezogen auf die öffentlichen Stellen vielfältig und vielseitig.

Als eine der wenigen (auch) positiven Auswirkungen der Pandemie ist der Quantensprung bei der Digitalisierung vieler öffentlicher Stellen in NRW zu bilanzieren, der allerdings – und das ist die Kehrseite der Medaille – inhaltlich von vielfältigen Fragen und Problemen des Datenschutzes und der Datensicherheit begleitet wurde und wird.

Besonders viele Eingaben und Anfragen betreffen dabei den Schulbereich – siehe hierzu unter 5.2 „Digitalunterricht und die Schubkraft von Corona“; hier waren zur Aufrechterhaltung des Unterrichtsbetriebs durch den Einsatz digitaler Lehr- und Lernmittel zeitnahe und angemessene Entscheidungen und Maßnahmen erforderlich (siehe hierzu „Pandemie und Schule – Datenschutz mit Augenmaß“, abrufbar über www.ldi.nrw.de). Die Schulleitungen hatten sich pandemiebedingt darüber hinaus auch mit anderen neuen Datenschutzthemen zu befassen, wie zum Beispiel der Frage nach dem zulässigen Inhalt von und dem gebotenen Umgang mit ärztlichen Attesten im Zusammenhang mit der Entbindung von der Maskenpflicht – siehe hierzu unter 5.1 sowie „Maskenpflicht und Masernschutz – Verarbeitung von Gesundheitsdaten an Schulen“, abrufbar über www.ldi.nrw.de.

Die Arbeit von Strafverfolgungsbehörden und Ordnungsämtern wurde ebenfalls unvorhergesehen durch Corona-Themen mitgeprägt und die Antworten auf die neuen Fragen mussten rasch und sicher gefunden werden. So trat zu Beginn der Pandemie zum Beispiel kurzzeitig die Frage auf, ob und inwieweit die Polizei Erkenntnisse aus „Corona-Datenbanken“ anderer Stellen zu ihrer Aufgabenerfüllung nutzen und speichern dürfe. Ein Erlass des Innenministeriums NRW vom 27. März 2020 stellte hierzu zeitnah und klar fest, dass sowohl die Speicherung von personengebundenen Hinweisen auf eine Corona-Infizierung in polizeilichen Auskunftssystemen als auch die Nutzung von „Corona-Datenbanken“ anderer Behörden untersagt bleibe. Als Gründe wurden insbesondere die fragliche Validität dieser Erkenntnisse für den Einsatzfall sowie

ein möglicher unzureichender Schutz der Polizeibeamt*innen aufgrund des (nicht berechtigten) Vertrauens in die nicht valide Datenlage benannt.

Zur weiteren Übermittlung von Daten von Gesundheitsämtern über Corona-Infizierte und deren Kontaktpersonen siehe auch unter 6.4 „Gesundheitsdaten an Leitstellen von Polizei, Feuerwehr und Rettungsdiensten“.

In Medien und der Öffentlichkeit wurde auch thematisiert, ob und in welchen Fällen Strafverfolgungsbehörden auf Corona-Kontaktlisten zugreifen dürfen. Dazu haben wir uns wiederholt positioniert – siehe hierzu „Corona-Kontaktlisten – Zugriff von Strafverfolgungsbehörden nun gesetzlich ausgeschlossen“, abrufbar unter www.ldi.nrw.de. Der Bundesgesetzgeber hat auf die Diskussion reagiert und in § 28a Abs. 4 Infektionsschutzgesetz eine enge Verwendungsbeschränkung der Corona-Kontaktlisten festgeschrieben. In der Anwendungspraxis – zumindest in NRW – schien dieses Thema nach unserer Wahrnehmung kaum eine Rolle zu spielen.

Anders stellt sich die Rechtslage dar, wenn Beschäftigte der Ordnungsämter die Kontaktlisten einsehen wollen. Da Gesundheitsämter vermehrt darüber geklagt hatten, dass Kontakte mangels ordnungsgemäß ausgefüllter Kontaktlisten nicht nachverfolgt werden konnten, hat in diesem Fall der Landesgesetzgeber reagiert. Die Coronaschutzverordnung sieht seit Oktober 2020 einen Bußgeldtatbestand für den Fall vor, dass sich Personen mit unrichtigen Daten in die Listen eintragen. Um diese Ordnungswidrigkeit zu verfolgen, muss es den Ordnungsämtern möglich sein, die Listen

auch prüfen zu können. Die üblichen Grenzen der Erforderlichkeit und Datensparsamkeit sind dabei einzuhalten.

Dass Gesundheitsdaten im Rahmen der Corona-Pandemie nur erhoben werden dürfen, wenn ihre Verarbeitung dem Grundsatz der Verhältnismäßigkeit entspricht, war auch bei Einlasskontrollen bei Gerichten zu berücksichtigen. Um Personen mit Covid-19-typischen Krankheitssymptomen den Zutritt zum Gericht zu verweigern, bedarf es keiner schriftlichen Abfrage zum Vorliegen entsprechender Symptome. Vielmehr ist es ausreichend, Besucher*innen mit entsprechenden Symptomen den Zutritt ins Gerichtsgebäude durch ein entsprechendes Hinweisschild vor dem Eingang zu untersagen. Siehe hierzu unter 6.3 „Einlasskontrolle bei Gerichten“.

Nicht-öffentlicher Bereich

Durch Corona bedingt sehen sich viele Unternehmen gezwungen, ihre Arbeitsabläufe und Arbeitsprozesse umzustellen. Hinzu kommen die Zunahme der elektronischen Datenverarbeitung, das Arbeiten im Homeoffice, in Telearbeit und mittels Videokonferenzsystemen sowie nicht zuletzt Fragen des Gesundheitsdatenschutzes bei Beschäftigten sowie Kund*innen.

Gerade die betrieblichen Datenschutzbeauftragten werden hier gebraucht und müssen ihre Kontroll- und Beratungsaufgaben erfüllen können. Dies gilt auch dann, wenn in einem Unternehmen Kurzarbeit eingeführt wurde. Siehe hierzu unter 10.4 „Kurzarbeit – ohne Datenschutzbeauftragte geht es nicht“.

Zur Rückverfolgbarkeit möglicher Infektionsketten sind verschiedene Wirtschaftsbereiche verpflichtet, Kontaktdaten ihrer Kund*innen zu erfassen, analog oder digital.

Dazu haben wir auf unserer Homepage fortlaufend die Hinweise zur Erfassung von Kundenkontaktdaten zwecks Rückverfolgbarkeit von Infektionsketten unter Berücksichtigung der geltenden Coronaschutzverordnung aktualisiert.

Ob dies immer datenschutzkonform erfolgt, haben wir stichprobenhaft geprüft. Siehe hierzu unter 10.3 „Corona: Stichprobenprüfung in Unternehmen“.

Bei Speditionslieferungen erfordert die Corona-Pandemie ein Umdenken bei der Annahme und Bestätigung von Speditionslieferungen. Wir haben geprüft, ob es Alternativen zur eigenhändigen Unterschrift gibt. Siehe hierzu unter 10.6 „Corona: Erfassung des Geburtsdatums bei Speditionslieferungen“.

Insbesondere in der Anfangszeit der Pandemie haben uns Anfragen von Besucher*innen stationärer Pflegeeinrichtungen erreicht, ob sie verpflichtet seien, vor Einlass Angaben zu ihrem Gesundheitszustand mitzuteilen. Siehe hierzu unter 7.2 „Erhebung von Gesundheitsdaten zur Kontaktnachverfolgung in Altenheimen“.

Maßnahmen im Zusammenhang mit der Pandemie wurden auch im Flugverkehr getroffen. Hier haben wir sog. Fluggast-Aussteigekarten datenschutzrechtlich bewertet. Siehe hierzu unter 10.5 „Datenerhebung mittels sog. Fluggast-Aussteigekarten“.

- **Übermittlung personenbezogener Daten in die USA und andere Drittländer**

  Der Europäische Gerichtshof hat den Angemessenheitsbeschluss für die USA zum EU-US Privacy Shield gekippt („Schrems II“-Urteil). Der Gerichtshof hat auch klargestellt, welche hohen Anforderungen an die Übermittlung personenbezogener Daten in Drittländer bestehen. Für Verantwortliche und andere Datenexporteure bedeutet das: Datenschutzniveau im Drittland prüfen, bei Bedarf ergänzende Maßnahmen treffen und – wenn dies nicht möglich ist – Alternativen zum Datenexport suchen. Siehe hierzu unter 3.

- **Internet und Medien**

  Beratung von Kinder-Website-Betreiber*innen

  Viele Anbieter*innen richten sich mit ihren Websites gezielt an Kinder, zum Beispiel um Medienkompetenz oder andere Lerninhalte zu vermitteln oder den digitalen Austausch zwischen Kindern zu ermöglichen. Ein besonders wichtiges Kriterium für „gute“ Kinder-Websites ist, dass die Datenschutzbestimmungen eingehalten werden.

  Vor diesem Hintergrund hielten wir im November 2020 einen Vortrag mit anschließender Diskussion beim Online-Mediencamp des Netzwerks „Seitenstark“ zum Thema „Gestaltung von Kinder-Websites nach der DS-GVO“. In dem Netzwerk haben sich rund 60 Kinderseiten-Betreiber*innen zusammengeschlossen, um insbesondere Qualitätsstandards für gute Kinderseiten zu entwickeln.

- **Datenschutz und Wirtschaft**

  Der Beratungsbedarf zum Datenschutz in der Wirtschaft ist nach wie vor sehr hoch. Neben unserer täglichen Beratung zu Einzelfragen aus der Praxis haben wir auf zahlreichen Veranstaltungen über die DS-GVO informiert. Zudem haben wir zu häufig angefragten Themen unsere Homepage um weitere Informationen ergänzt. Siehe hierzu unter 10.1.

- **Anlasslose Prüfungen**

  Im Jahr 2020 haben wir weitere Kontrollen und Prüfungen durchgeführt.

  Folgende Prüfverfahren befinden sich in verschiedenen Verfahrensstadien:

  - Datenschutzüberprüfung von Versicherungsunternehmen und Kreditinstituten. Siehe hierzu unter 10.2.
  - Corona: Stichprobenprüfung in Unternehmen. Siehe hierzu unter 10.3.
  - Datenschutzüberprüfung von Personaldienstleistern und Leiharbeitsunternehmen. Siehe hierzu unter 9.1.

- **Informationen und Öffentlichkeitsarbeit**

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

  Alle Veröffentlichungen der Datenschutzkonferenz 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**

  - Fachtagung Datenschutz der Sparkassenakademie NRW: „Datenschutzaufsicht – Aktuelle Themen und Best Practices“
  - Erfahrungsaustausch mit dem Rheinischen Sparkassen- und Giroverband (RSGV) und dem Sparkassenverband Westfalen-Lippe (SVWL)
  - Erfahrungsaustausch mit Versicherungsunternehmen
  - Erfahrungsaustausch mit betrieblichen Datenschutzbeauftragten von Banken und Versicherungen, die im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) organisiert sind
  - Erfahrungsaustausch mit dem Bundesverband sowie betrieblichen Datenschutzbeauftragten von Inkassounternehmen, die im BDIU organisiert sind
  - Vortrag zum richtigen Umgang mit Datenpannen im Unternehmen
  - Vortrag zur Datennutzung und Datenanalyse in Kreditinstituten im Bankenbereich
  - Vortrag vor Unternehmen des ÖPNV zum Thema Bodycams
  - Vortrag zur Videoüberwachung im Rahmen der Polizeifortbildung
  - Erfahrungsaustausch mit den Hochschuldatenschutzbeauftragten NRW

- **Datenschutzkonferenz und Expertengruppen des Europäischen Datenschutzausschusses**

  Die Beauftragten des Bundes und der Länder besprechen wichtige Datenschutzfragen in der **Datenschutzkonferenz** und streben einheitliche Bewertungen an, die in Arbeitskreisen vorbereitet werden. Im Rahmen der Datenschutzkonferenz leitet die LDI NRW die Arbeitskreise Wirtschaft (vormals Düsseldorfer Kreis), Statistik, Kreditwirtschaft und – gemeinsam mit Hessen – den Arbeitskreis Auskunfteien.

  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 der Key Provisions Expert Subgroup und in der Financial Matters Expert Subgroup des Europäischen Datenschutzausschusses aktiv.

2. Zahlen und Fakten

- **Eingabesituation im Überblick**

  Im Jahr **2020** haben uns insgesamt rund **12.150** schriftliche Eingaben erreicht, einschließlich Meldungen nach Art. 33 DS-GVO – sog. Datenpannen. Grundsätzlich nicht erfasst haben wir dabei die zahlreichen telefonischen Anfragen.

  Die Zahl der Eingaben bleibt damit hoch. Im Jahr 2019 waren es insgesamt etwa 12.500, im Jahr 2018 etwa 12.000.

  Von den Eingaben waren

  - **7.138 Beschwerden** nach Art. 77 DS-GVO,
  - **439** von **Dritten gemeldete Beschwerden**,
  - **1.595 schriftliche Beratungsanfragen**,
  - **44 Begleitungen bei Rechtsetzungsvorhaben**
  - **3 Genehmigungsverfahren** und
  - **1.775 Meldungen nach Art. 33 DS-GVO** zu sog. Datenpannen.

- **Beschwerden und Beratungsanfragen**

  Im Jahr 2020 haben uns **7.138 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. Wir können von Amts wegen aber auch Eingaben nachgehen, die auf mutmaßliche Datenschutzverstöße hinweisen, von denen die Einsendenden jedoch nicht selbst betroffen sind. Solche **Eingaben von Dritten** haben wir **439** erhalten.

Viele Beschwerden richten sich gegen Datenverarbeitungen im nicht-öffentlichen Bereich, das heißt die Verantwortlichen sind kleine, mittlere und große Unternehmen vieler Wirtschaftszweige, Selbständige aus dem Dienstleistungsbereich und aus den freien Berufen, Vereine und Privatpersonen.

Schriftliche **Beratungsanfragen** haben wir **1.595** 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 **1.775** erreicht. Im Jahr 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).

  Der mit den in Art. 33 und 34 DS-GVO eingeführten Melde- und Benachrichtigungspflichten verbundene Aufwand ist erheblich – sowohl für die Verantwortlichen, als auch für die LDI NRW. Seit März 2020 stellt die LDI NRW ein Webformular für Meldungen von Datenpannen zur Verfügung. Das Webformular wird von den Verantwortlichen – auch wegen der unmittelbaren Eingangsbestätigung mit Angabe des Aktenzeichens – positiv angenommen. Durch die direkte Weiterleitung der Meldungen an die Sachbearbeitung konnten wir unsere Reaktionszeiten auf Meldungen signifikant verkürzen und somit im Sinne des Schutzgedankens der Art. 33 und 34 DS-GVO bei Bedarf schneller tätig werden. Siehe hierzu unter 11.1.

- **Abhilfemaßnahmen**

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

  Von den dort genannten Abhilfemaßnahmen hat die LDI NRW insgesamt **631** Maßnahmen ergriffen. Im Einzelnen:

  - **348 Hinweise** nach Art. 58 Abs. 1 d)
  - **23 Warnungen** nach Art. 58 Abs. 2 a)
  - **70 Verwarnungen** nach Art. 58 Abs. 2 b)
  - **2 Anweisungen** nach Art. 58 Abs. 2 c)
  - **52 Anweisungen** nach Art. 58 Abs. 2 d)
  - **1 Beschränkung** nach Art. 58 Abs. 2 f)

  Zudem wurden im Jahr 2020 bei der Zentralen Bußgeldstelle der LDI NRW als Maßnahme nach Art. 58 Abs. 2 Buchstabe i DS-GVO

  - **123 Bußgeldverfahren** eingeleitet und
  - **93 Bußgeldbescheide** erlassen.

  Viele im Jahr 2020 begonnene Verfahren sind noch nicht beendet und werden statistisch nicht erfasst. 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 Europäischen Datenschutzausschuss 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 2020 war die LDI NRW in **1.558** Fällen mit gestarteten IMI-Modulen befasst. Im Jahr 2019 waren es 1.390 Fälle.

- **Förmliche Begleitung bei Rechtsetzungsvorhaben**

  Im Jahr 2020 wurde die LDI NRW bei **44 Rechtsetzungsvorhaben** beteiligt. Im Jahr 2019 waren es 21 Vorhaben.

  Unsere Hinweise 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.

  Inzwischen werden im Rahmen der Digitalisierung der Verwaltung vermehrt Gesetzgebungsvorhaben bei uns vorgelegt, die die Einrichtung automatisierter Abrufverfahren zum Gegenstand haben. Bei diesen Gesetzen und Verordnungen achten wir insbesondere darauf, dass die Verantwortlichkeiten für die technischen und organisatorischen Maßnahmen und die Betroffenenrechte zwischen den beteiligten öffentlichen Stellen eindeutig abgegrenzt sind.

  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 Datenschutzgesetz NRW). Dies soll sicherstellen,

dass wir die vorgesehenen Neuregelungen hinreichend gründlich prüfen und ggf. eingehend beratend tätig werden können. Versäumen es die zuständigen Ministerien, diese frühzeitige Beratung zu nutzen, entsteht nicht selten großer Unmut, wenn die LDI NRW nachträglich auf nicht ausreichenden Datenschutz hinweisen muss und sich das Verfahren dadurch verzögert. Es liegt in der Hand der zuständigen Stellen, dies durch ein rechtzeitiges Beratungsersuchen zu vermeiden.

Wir wurden in unterschiedlicher Intensität und in verschiedenen Phasen der Verfahren vor der Einbringung in den Landtag oder als Sachverständige im Rahmen von Anhörungen im Landtag insbesondere bei den folgenden Gesetzesvorhaben tätig:

- Entwurf eines Gesetzes zur Durchführung strafrechtsbezogener Unterbringungen in einem psychiatrischen Krankenhaus und einer Entziehungsanstalt in Nordrhein-Westfalen (Strafrechtsbezogenes Unterbringungsgesetz NRW – StrUG NRW)
- Entwurf eines zweiten Gesetzes zur Änderung des Gesetzes über die juristischen Prüfungen und den juristischen Vorbereitungsdienst (Juristenausbildungsgesetz Nordrhein-Westfalen)
- Entwurf einer Rechtsverordnung des MWIDE NRW zu lebens- oder verteidigungswichtigen Einrichtungen nach dem Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Landes Nordrhein-Westfalen (Sicherheitsüberprüfungsgesetz Nordrhein-Westfalen – SÜG NW)
- Entwurf einer Verordnung über den Vollzug der Freiheitsentziehung im Polizeigewahrsam des Landes NRW

- Entwurf eines Gesetzes zur Änderung des VwVG NRW und weiterer Gesetze
- Entwurf einer Verordnung für ein elektronisches Antragsverfahren auf dem Bauportal.NRW
- Entwurf eines Gesetzes zur Digitalisierung wirtschaftsbezogener Verwaltungsleistungen
- Verordnungsentwurf zur Einführung der Serviceportal.NRW-Verordnung und zur Änderung der Servicekonto.NRW-Verordnung
- Referentenentwurf eines Gesetzes zur Änderung des Kunsthochschulgesetzes
- Entwurf eines Gesetzes zur Änderung des Gesetzes über den Brandschutz, die Hilfeleistung und den Katastrophenschutz sowie anderer Gesetze
- Entwurf eines Gesetzes zum Erlass eines Kulturgesetzbuches sowie zur Änderung und Aufhebung weiterer Vorschriften (Kulturrechtsneuordnungsgesetz)
- Datenübermittlungsverordnung zum Gefahrtiergesetz
- Entwurf eines Dritten Gesetzes zur Änderung des Krankenhausgestaltungsgesetzes Nordrhein-Westfalen (KHGG)
- Entwurf eines Gesetzes zur Änderung des Landesbeamtengesetztes (LBG NRW)

3. Übermittlung personenbezogener Daten in Drittländer

Der Europäische Gerichtshof hat den Angemessenheitsbeschluss der EU-Kommission für die USA zum EU-US Privacy Shield für ungültig erklärt. Er hat zudem hohe Anforderungen an die Übermittlung personenbezogener Daten in alle Drittländer deutlich gemacht. Die Datenschutzaufsichtsbehörden haben dazu Hilfestellungen erarbeitet und arbeiten weiterhin an einer sachgerechten Umsetzung und Durchsetzung.

Der Europäische Gerichtshof hat in seinem Urteil im Juli 2020 – C-311/18, genannt "Schrems II" – den Angemessenheitsbeschluss der EU-Kommission mit Bezug auf das EU-US Privacy Shield für ungültig erklärt. Die Angemessenheitsentscheidung kann daher nicht als Instrument für die Übermittlung personenbezogener Daten in die USA verwendet werden.

Gegenstand des Gerichtsverfahrens waren Übermittlungen in die USA. Die Anforderungen, die der Europäische Gerichtshof deutlich gemacht hat, sind aber nicht auf die USA beschränkt. Sie gelten für alle Drittländer, also für Länder außerhalb des Europäischen Wirtschaftsraums.

Der Europäische Gerichtshof zeigt auf, dass bei Übermittlung personenbezogener Daten in Drittländer in vielen Fällen besonders berücksichtigt werden muss, wie sich staatliche Überwachungsmaßnahmen in Drittländern auf Grundrechte und Grundfreiheiten von Betroffenen auswirken.

Grundsätze der Drittlandübermittlung nach „Schrems II“

Vor einer Übermittlung personenbezogener Daten müssen Verantwortliche prüfen, auf welcher Grundlage nach Kapitel V der Datenschutz-Grundverordnung (DS-GVO) die Daten übermittelt werden dürfen. Dafür müssen alle Übermittlungen von personenbezogenen Daten an Drittländer bekannt sein. Dazu müssen zuerst die konkreten Datenflüsse der eingesetzten Dienste und Software erkannt werden.

Dann muss das Übermittlungswerkzeug geprüft werden, auf das sich die Übertragung stützt. Dafür stehen drei Kategorien zur Verfügung:

- Angemessenheitsbeschluss der EU-Kommission für das Zielland (Art. 45 DS-GVO)
- Geeignete Garantien, zum Beispiel durch vertragliche Vereinbarungen (Art. 46 DS-GVO)
- Ausnahmen für bestimmte Fälle, zum Beispiel Einwilligungen (Art. 49 DS-GVO)

Wenn es einen Angemessenheitsbeschluss gibt, kann die Übertragung darauf gestützt werden, solange die Entscheidung noch in Kraft ist. Die Angemessenheitsentscheidungen sind auf der Internetseite der Europäischen Kommission abrufbar.

Ohne Angemessenheitsbeschluss müssen regelmäßige und sich wiederholende Übertragungen auf geeignete Garantien gestützt werden, also auf eines der unter Art. 46 DS-GVO aufgeführten Übertragungsinstrumente. Dann ist zu prüfen, ob ergänzende Maßnahmen erforderlich sind und wie sie umzusetzen sind.

Ausnahmen für bestimmte Fälle nach Art. 49 DS-GVO benötigen zwar keine ergänzenden Maßnahmen, sind aber nicht für regelmäßige und sich wiederholende Übertragungen anwendbar.

Die Anforderungen gelten auch für Auftragsverarbeiter, die Daten in Drittländer übermitteln, auch wenn Verantwortliche bzw. die/der Auftraggeber*in, nicht der DS-GVO unterliegt.

Prüfung ergänzender Maßnahmen

Bei Auswahl eines Übertragungsinstruments nach Art. 46 DS-GVO muss beurteilt werden, ob Gesetze oder die Praxis des Drittlandes die Wirksamkeit von angemessenen Schutzmaßnahmen der eingesetzten Übertragungsinstrumente im Kontext der konkreten Übertragung beeinträchtigen.

Das Erfordernis ergänzender Maßnahmen betrifft vor allem auch das Instrument der Standardvertragsklauseln, das nach dem Wegfall der Angemessenheitsentscheidung für die USA in der Praxis noch wichtiger geworden ist.

Die EU-Kommission hat bereits neue Standardvertragsklauseln entworfen. Der Europäische Datenschutzausschuss (EDSA) hat dazu Stellung genommen. Wir haben daran mitgearbeitet.

Auch wenn die EU-Kommission die neuen Standardvertragsklauseln verabschiedet, bleiben Verantwortliche und Auftragsverarbeiter in der Pflicht, das Erfordernis ergänzender Maßnahmen zu prüfen und umzusetzen.

Handlungsempfehlung zur Prüfung ergänzender Maßnahmen

Die europäischen Datenschutzaufsichtsbehörden haben Empfehlungen erarbeitet: Die Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus des EDSA 01/2020 werden durch Hinweise zur Bewertung des Drittlandes in den Empfehlungen des EDSA 02/2020 zu grundlegenden europäischen Garantien für Überwachungsmaßnahmen ergänzt.

Wenn eine Beeinträchtigung der Wirksamkeit von angemessenen Schutzmaßnahmen der Übertragungsinstrumente festgestellt wird, müssen diejenigen zusätzlichen Maßnahmen ergriffen werden, die erforderlich sind, um das wesentlich gleiche Schutzniveau gemäß der DS-GVO zu erreichen.

Die Empfehlungen des EDSA 01/2020 enthalten eine nicht abschließende Liste von Beispielen für ergänzende Maßnahmen mit Wirksamkeitsbedingungen. Die Wirksamkeit der ergänzenden Maßnahme ist vom jeweiligen Drittland abhängig.

Es kann auch notwendig sein, mehrere ergänzende Maßnahmen zu kombinieren. Wenn keine wirksame ergänzende Maßnahme geeignet ist, dürfen die Übermittlungen der personenbezogenen Daten in Drittländer nicht erfolgen.

Insbesondere ist zu prüfen, inwiefern mit den Maßnahmen Pseudonymisierung und Verschlüsselung wirksam gearbeitet werden kann. Bei manchen Diensten oder Softwarelösungen können solche Maßnahmen nur eingeschränkt umgesetzt werden, weil Zugriffsmöglichkeiten im Drittland für die Funktion erforderlich

oder sonst fest eingebaut sind. Manchmal würden die erforderlichen Maßnahmen zu einem Verlust an Funktionalität führen. Dies bedeutet aber nicht, dass solche Übermittlungen ohne Weiteres fortgesetzt werden dürfen – vielmehr müssen Anwender*innen in der Regel andere Lösungen finden.

Bei den USA als Empfängerland ist – gemessen an den dort bekannten staatlichen Überwachungsmaßnahmen – anzunehmen, dass auch eine Pseudonymisierung oder Transportverschlüsselung nicht immer ausreichend ist.

Außerdem müssen die Verantwortlichen und Auftragsverarbeiter alle formalen Verfahrensschritte vornehmen, beispielsweise in einigen Fällen ihre zuständigen Aufsichtsbehörden konsultieren.

Der Grundsatz der Rechenschaftspflicht erfordert es letztlich, das Schutzniveau in angemessenen Abständen neu zu bewerten und dazu die Entwicklung im Drittland zu beobachten.

Praktische Folgen für Verantwortliche und Auftragsverarbeiter

Grundsätzlich raten wir allen Verantwortlichen, den Einsatz von Software und Diensten zu überprüfen, die Daten in ein Drittland übermitteln oder übermitteln könnten. Das gilt auch für Auftragsverarbeiter, die Daten aus der EU in Drittländer übermitteln, auch wenn die verantwortliche, den Auftrag erteilende Stelle nicht der DS-GVO unterliegt.

Werden personenbezogene Daten in ein Drittland übermittelt, ist es in einigen Fällen praktisch empfehlenswert, diese Übermittlung abzustellen oder auf das

Produkt zu verzichten und ein anderes Produkt einzusetzen. Allgemein können die Anforderungen dazu führen, dass es in einigen Fällen keine datenschutzkonforme Übermittlung in ein Drittland geben kann und deswegen – als Praxisempfehlung – nach einer Alternative ohne Drittlandtransfer gesucht werden sollte.

Durch das Urteil „Schrems II“ des Europäischen Gerichtshofs ist klargeworden, dass hohe Anforderungen an die Übermittlung personenbezogener Daten in Drittländer bestehen. Verantwortliche müssen das Datenschutzniveau im Empfängerland vor der Übermittlung prüfen. Möglicherweise müssen sie zusätzliche ergänzende Maßnahmen treffen, die im Wesentlichen ein im Europäischen Wirtschaftsraum garantiertes Schutzniveau gewährleisten. In manchen Fällen sind keine geeigneten ergänzenden Maßnahmen aufzufinden. Eine rechtmäßige Übermittlung personenbezogener Daten in das Drittland ist dann nicht möglich.

Die europäischen Aufsichtsbehörden stimmen ihre Empfehlungen und ihre Durchsetzung im Europäischen Datenschutzausschuss ab. Wir beteiligen uns daran.

4. Internet und Medien

4.1 „Planet49“-Urteil des Bundesgerichtshofes zur datenschutzkonformen Verwendung von Cookies auf Websites

Der Bundesgerichtshof (BGH) hat in seiner Entscheidung vom 28. Mai 2020 zu Planet49 wichtige Grundsätze für die datenschutzkonforme Verwendung von Cookies auf Websites bestätigt.

Der BGH hat in seinem Urteil vom 28. Mai 2020 (Az. I ZR 7/16, Verbraucherzentrale Bundesverband e. V. gegen Planet49 GmbH) über Fragen im Zusammenhang mit der Einwilligung in Cookies auf Websites entschieden.

Im Vorfeld hatte der BGH dem Europäischen Gerichtshof (EuGH) in diesem Zusammenhang einige Rechtsfragen vorgelegt. Der EuGH hatte in seinem Urteil vom 1. Oktober 2019 (Az. C-673/17) entschieden, dass nach geltendem Recht keine wirksame Einwilligung vorliegt, wenn die Nutzer*innen zur Verweigerung ihrer Einwilligung ein bereits angekreuztes Kästchen abwählen müssen. Eine wirksame datenschutzrechtliche Einwilligung – auch online – erfordert vielmehr ein aktives Verhalten der Betroffenen. Zudem hatte der EuGH klargestellt, dass das Setzen und Abrufen von Cookies oder anderen Informationen, die im Endgerät der Nutzer*innen gespeichert sind, einer Einwilligung bedürfen. Siehe 25. Bericht unter 4.5.

Der BGH hat in seinem Urteil die Kernaussagen des EuGH-Urteils bestätigt. Hierbei hat er das Einwilligungserfordernis bei Cookies auf § 15 Abs. 3 Telemediengesetz (TMG) gestützt. Nach dem Wortlaut

dieser Regelung darf der Diensteanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern die/der Nutzer*in dem nicht widersprechen. Diese Vorschrift legt der BGH jedoch richtlinienkonform im Lichte der ePrivacy-Richtlinie 2002/58/EG (ePrivacy-RL) dahingehend aus, dass für das Setzen von Cookies eine aktive Einwilligung der Nutzer*innen erforderlich ist. Die sich aus dem Wortlaut des § 15 Abs. 3 TMG ergebende bloße Möglichkeit des Widerspruchs der Nutzer*innen (Opt-Out), nachdem das Cookie bereits gesetzt wurde, ist also nach der Auffassung des BGH nicht ausreichend.

Das Urteil des BGH zu Planet49 verstärkt nach Auffassung der Datenschutzkonferenz (DSK) den seit langem bestehenden, dringenden Handlungsbedarf. Das bekräftigt sie mit ihrer Entschließung „Betreiber von Webseiten benötigen Rechtssicherheit – Bundesgesetzgeber muss europarechtliche Verpflichtungen der „ePrivacy-Richtlinie“ endlich erfüllen“ vom 25. November 2020 (Abdruck im Anhang). Im Unterschied zum BGH kommt die DSK in ihrer „Orientierungshilfe für Anbieter von Telemedien“ vom 29. März 2019 zu dem Schluss, dass die Datenschutzregeln im TMG (unter anderem § 15 Abs. 3 TMG) neben der Datenschutz-Grundverordnung (DS-GVO) nicht mehr anwendbar sind. Nach Auffassung der DSK gelten die Regelungen des TMG nach Art. 95 DS-GVO nur dann fort, wenn es sich bei ihnen um eine Umsetzung der ePrivacy-RL handelt. Dies aber verneint die DSK, da kein formeller Umsetzungsakt der ePrivacy-RL im 4. Abschnitt des TMG erfolgt ist und insbesondere Art. 5 Abs. 3 ePrivacy-RL im deutschen Recht insgesamt nicht umgesetzt wurde. Die Frage nach dem

Einwilligungserfordernis wird daher – so die DSK – unmittelbar nach der DS-GVO beurteilt.

Richtet sich die Rechtmäßigkeit von Cookies unmittelbar nach der DS-GVO, kommt als Rechtsgrundlage neben einer Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO auch noch ein berechtigtes Interesse der Websitebetreibenden an der Verwendung eines Cookies oder eines anderen Tools nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO in Betracht. Hierbei gilt es insbesondere, im konkreten Einzelfall die Interessen der Websitebetreibenden mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Personen abzuwägen. Die Interessenabwägung fällt vor allem dann zugunsten der Nutzenden aus, wenn die Verarbeitung ihrer personenbezogenen Daten aufgrund der Verwendung von Cookies oder anderen Tracking-Techniken für sie nicht vorhersehbar ist, sie für die Bereitstellung der Webseite technisch nicht erforderlich ist, die Daten an eine Vielzahl von Beteiligten weitergegeben werden oder die Daten mit anderen Datensätzen verknüpft bzw. angereichert werden können. In diesen Fällen ist eine Datenverarbeitung nur mit Einwilligung der betroffenen Person möglich.

In den meisten Fällen führen die BGH-Entscheidung und die Orientierungshilfe der DSK zu dem gleichen Ergebnis: Es bedarf einer vorherigen aktiven Einwilligung der Nutzer*innen, bevor Cookies gesetzt werden dürfen. Für deren Ausgestaltung ist dann ohnehin wieder die DS-GVO einschlägig.

Es bleibt zu hoffen, dass in naher Zukunft neue gesetzliche Regelungen über die Verwendung von Cookies und anderen Tools auf Websites für mehr Klarheit sorgen werden. Auf Ebene der Europäischen

Union hätte die ePrivacy-Verordnung nach ursprünglichen Planungen bereits zeitgleich mit der DS-GVO wirksam werden sollen. Nicht zuletzt aufgrund der fehlenden Einigkeit zwischen den Mitgliedsstaaten ist es derzeit unklar, wann mit einem Inkrafttreten gerechnet werden kann. Auf nationaler Ebene befindet sich derzeit das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) in Planung, welches unter anderem die Datenschutzbestimmungen für Telemedien neu regeln und die Vorgaben der ePrivacy-Richtlinie umsetzen soll.

Der BGH hat in seiner Entscheidung vom 28. Mai 2020 zu Planet49 die Aussagen des EuGH-Urteils vom 1. Oktober 2019 grundsätzlich bestätigt. Er hat klargestellt, dass keine wirksame Einwilligung vorliegt, wenn die Nutzer*innen zur Verweigerung ihrer Einwilligung ein bereits angekreuztes Kästchen abwählen müssen. Zudem müssen Websitebetreiber*innen den Nutzer*innen klare und umfassende Informationen bereitstellen. Während der BGH das Einwilligungserfordernis bei Cookies jedoch auf § 15 Abs. 3 TMG stützt, wird in der Orientierungshilfe der DSK für Anbieter*innen von Telemedien vom 29 März 2019 die DS-GVO unmittelbar angewendet. Festzuhalten ist: Cookies bedürfen einer vorherigen aktiven Einwilligung der Nutzer*innen.

4.2 Rechtskonforme Gestaltung von Online-Gewinnspielen

Häufig bieten Unternehmen auf ihren Websites Gewinnspiele an, an denen Nutzer*innen nur unter der Bedingung teilnehmen dürfen, dass sie (jederzeit widerruflich) dem Abonnement eines E-Mail-Newsletters zustimmen. Die Verarbeitung der E-Mail-Adresse soll dann auf Art. 6 Abs. 1 Satz 1 Buchstabe a Datenschutz-Grundverordnung (DS-GVO) gestützt werden. Dies aber verstößt gegen das Gebot der Freiwilligkeit der Einwilligung und insbesondere gegen das Kopplungsverbot. Daher gilt es, eine andere Rechtsgrundlage heranzuziehen.

Um Kund*innen an sich zu binden, bieten viele Unternehmen regelmäßig Online-Gewinnspiele an, an denen Nutzer*innen nur dann teilnehmen können, wenn sie damit einverstanden sind, dass ihre E-Mail-Adressen für den regelmäßigen Newsetter-Versand des Unternehmens genutzt werden. Häufig stützen die Unternehmen den Newsletter-Versand auf eine Zustimmung nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO. Dies aber stellt in der Regel einen Verstoß gegen das Gebot der Freiwilligkeit der Einwilligung nach Art. 4 Nr. 11, 7 Abs. 4 DS-GVO und insbesondere gegen das Kopplungsverbot nach Art. 7 Abs. 4 in Verbindung mit Erwägungsgrund 43 (am Ende) DS-GVO dar.

Die fehlende Freiwilligkeit der Nutzer*innen, ihre Einwilligung zu erteilen, ergibt sich in solchen Fällen einerseits daraus, dass es als Nachteil im Sinne von Erwägungsgrund 42 (am Ende) DS-GVO zu bewerten ist, dass Nutzer*innen im Falle der Ablehnung des Newsletter-Abos nicht am Gewinnspiel teilnehmen

können. Da die Einwilligung der Nutzer*innen in die E-Mail-Werbung in der Regel nicht erforderlich für die Durchführung des Gewinnspiels ist (ein Online-Gewinnspiel kann regelmäßig auch ohne die Versendung von E-Mail-Werbung durchgeführt werden), wird zudem ein Verstoß gegen das Kopplungsverbot angenommen.

Aus unserer Sicht ist es jedoch unter bestimmten Voraussetzungen möglich, die Verknüpfung des Online-Gewinnspiels mit dem Newsletter-Versand auf die Rechtsgrundlage Art. 6 Abs. 1 Satz 1 Buchstabe b DS-GVO zu stützen. Hiernach ist die Verarbeitung rechtmäßig, wenn sie für die Erfüllung eines Vertrags erforderlich ist, dessen Vertragspartei die betroffene Person ist.

Zwischen Nutzer*innen und Websitebetreiber*innen wird vertraglich vereinbart, dass Nutzer*innen an dem Gewinnspiel teilnehmen können und sich als Gegenleistung mit dem Abonnement des E-Mail-Newsletters einverstanden erklären. Hierbei ist zu berücksichtigen, dass die Pflicht der Nutzer*innen zur Gestattung der Verwendung ihrer E-Mail-Adresse für Newsletter in einem Gegenseitigkeitsverhältnis mit der Pflicht der Anbieter*innen steht, die Nutzer*innen an dem Gewinnspiel teilnehmen zu lassen. Die Leistung der Anbieter*innen ist also an die Datenpreisgabe der betroffenen Person gekoppelt. Voraussetzung ist, dass dieser Tausch den Nutzer*innen gegenüber transparent gemacht wird. So darf das Gewinnspiel beispielsweise nicht „kostenlos“ angeboten werden, sondern muss offen als zweiseitiger Vertrag „Gewinnchance gegen Daten für Zusendung des Newsletters“ angeboten werden, bei dem die wesentlichen Vertragsmodalitäten den Nutzer*innen offengelegt werden. Die

Transparenz dürfte etwa dann zweifelhaft sein, wenn für das Angebot eines Web-Dienstes im Austausch ein umfangreiches, den Nutzer*innen nicht offen gelegtes Tracking eingesetzt wird, das die Weitergabe an unzählige andere Unternehmen beinhaltet. In solchen Fällen ist es für die Nutzer*innen nur schwer nachvollziehbar, wer ihre Daten zu welchen Zwecken verarbeitet. Das Abonnement eines jederzeit abbestellbaren Newsletters ist hingegen anders zu bewerten, sofern die E-Mail-Adressen nicht an Dritte weitergegeben und ausschließlich für den Zweck des Newsletter-Versands verwendet werden. Dies lässt sich aus unserer Sicht in der Regel ohne Weiteres transparent darstellen.

Die Verknüpfung zwischen der Teilnahme an einem Online-Gewinnspiel und der Zustimmung zum regelmäßigen Erhalt von Newslettern verstößt zwar gegen das Gebot der Freiwilligkeit der Einwilligung und insbesondere gegen das Kopplungsverbot. Allerdings kann die Verknüpfung des Online-Gewinnspiels mit dem Newsletter-Versand unter bestimmten Voraussetzungen auf einen Vertrag mit den betreffenden Nutzer*innen und damit auf die Rechtsgrundlage des Art. 6 Abs. 1 Satz 1 Buchstabe b DS-GVO gestützt werden.

4.3 EDSA veröffentlicht Entwurf von Richtlinien zum Targeting in Social Media

Der im April dieses Jahres vom Europäischen Datenschutzausschuss (EDSA) verabschiedete Richtlinienentwurf zum Targeting in Social Media knüpft an die Rechtsprechung des Europäischen Gerichtshofs (EuGH) zu Facebook-Fanpages und Facebook-Like-Button an. Erläutert wird anhand verschiedener Konstellationen die Reichweite der gemeinsamen Verantwortung nach Art. 26 DS-GVO zwischen Targetern (Werbenden) und Social Media-Plattformen (SMP).

Im Bereich der Online-Werbung greifen Unternehmen vielfach auf die von SMP angebotenen Targeting-Prozesse zurück, um ihre Werbung adressatengerecht zu platzieren. Dabei geben üblicherweise die Werbenden – auf Basis des Angebots der SMP – die Parameter vor, anhand derer die Adressaten der Werbung ausgewählt werden sollen. Die konkrete Auswahl der anzusprechenden Personen und das Einspielen der Werbung erfolgt seitens der SMP. Diese Vorgänge sind Gegenstand der im April verabschiedeten Richtlinie des EDSA zum Targeting in Social Media. Die am 13 April 2021 angenommenen „Guidelines 8/2020 on the targeting of social media users – Version 2.0“ ist auf der Internetseite des EDSA abrufbar. Das Dokument liegt bislang nur in englischer Sprache vor.

Bei derartigen Kooperationen sind in aller Regel Werbende und SMP als gemeinsam Verantwortliche im Sinne des Art. 26 DS-GVO anzusehen. Eine solche gemeinsame Verantwortlichkeit setzt voraus, dass zwei oder mehr Verantwortliche gemeinsam die Zwe-

cke der und die Mittel zur Verarbeitung in einer Vereinbarung festlegen. Die gemeinsame Verantwortlichkeit ist für das Targeting insbesondere seit den EuGH-Entscheidungen „Wirtschaftsakademie“ (Urteil vom 5. Juni 2018, Az. C-210/16) und „Fashion ID“ (Urteil vom 29. Juli 2019, Az. C-40/17) in den Fokus gerückt. Im ersten Fall ging es um den Betrieb sog. Facebook-Fanpages, im anderen Fall um die Einbettung des Facebook Like-Buttons auf einer Website. Der EuGH hat in beiden Fällen eine gemeinsame Verantwortlichkeit für die aus dem Betrieb der Fanpage bzw. der Einbettung des Facebook Like-Buttons resultierenden Verarbeitungen angenommen, also Fanpage- bzw. Website-Betreiber*innen einerseits und Facebook andererseits als gemeinsame Verantwortliche gemäß Art. 26 DS-GVO qualifiziert. Dies hat zur Folge, dass eine betroffene Person ihre Rechte aus der DS-GVO nach Art. 26 Abs. 3 DS-GVO grundsätzlich gegenüber jeder/jedem einzelnen der Verantwortlichen geltend machen kann. Gleichzeitig hat der EuGH in diesen Entscheidungen, primär in der Fashion-ID-Entscheidung, auch eine Grundlage dafür gelegt, über die Berücksichtigung von getrennten Verantwortungsbereichen eine potentiell ausufernde Haftung für jeweils andere Verantwortliche zu beschränken.

Diesen Weg verfolgt der EDSA mit den nun verabschiedeten Richtlinien weiter. Sie sollen, praktische Hilfe bei der Bewertung der Rollen und Verantwortlichkeiten der SMP und der Werbenden bei der Nutzung entsprechender Targetingmechanismen geben. Sie analysieren die Risiken für Betroffene durch das Targeting, sowie die Rollen der am Targeting Beteiligten (Nutzer*innen, SMP, Werbende) und prüfen die sich hieraus ergebenden Verantwortlichkeiten und

Anforderungen an verschiedene Formen des Targetings anhand einer Reihe typischer Beispiele. So differenzieren die Richtlinien zwischen Targeting auf Basis von Informationen der Betroffenen selbst, Targeting auf Basis von Beobachtungsdaten und Targeting auf Basis von abgeleiteten Daten.

Für diese Fallgruppen wird erörtert, welche Rechtsgrundlagen jeweils zugrunde gelegt werden können und welche Anforderungen an entsprechende Datenverarbeitungen zu stellen sind. Im Regelfall kommt als Rechtsgrundlage entweder eine Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a DS-GVO oder ein berechtigtes Interesse der Verantwortlichen nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO in Betracht.

Allerdings greifen diese Rechtsgrundlagen nicht bei allen Konstellationen. Angesichts der auch vom EuGH in seiner FashionID-Entscheidung zugrunde gelegten restriktiven Anforderungen an eine Verarbeitung personenbezogener Daten auf Basis eines legitimen Interesses ist für Targeting vielfach eine Einwilligung der Nutzer*innen erforderlich. Dies gilt vor allem für besonders eingriffsintensives Tracking oder Profiling. Da auch die ePrivacy-Richtlinie neben der DS-GVO anwendbar ist, sofern die Verarbeitung unter Einbeziehung von Plug-ins, Cookies oder Pixel erfolgt, ist auch für solches Targeting stets eine Einwilligung in die Verarbeitung erforderlich.

Zudem adressieren die Richtlinien die Frage, wie weit die jeweilige Verantwortlichkeit der Beteiligten am Targeting reicht. Dabei betonen die Richtlinien in Anlehnung an die Entscheidung des EuGH in der Rechtsache Wirtschaftsakademie, dass Verantwortliche in unterschiedlichen Stadien der Verarbeitung perso-

nenbezogener Daten in unterschiedlichem Maß involviert sein können und die Verantwortung mit Blick auf spezifische Verpflichtungen nicht notwendigerweise gleich verteilt sein muss. Darüber hinaus reicht die gemeinsame Verantwortung nach Art. 26 DS-GVO immer nur soweit, wie tatsächlich eine gemeinsame Entscheidung über Zweck und Mittel der Verarbeitung personenbezogener Daten vorliegt. Vor- oder nachgeschaltete Datenverarbeitungen fallen auch nicht über die Anwendung des Art. 26 DS-GVO in die Verantwortung der jeweils anderen Verantwortlichen. Die Richtlinien stellen Lösungen vor, wie die jeweiligen Verantwortungsbereiche datenschutzkonform ausgestaltet und abgegrenzt werden können. Besondere Bedeutung kommt hierbei der nach Art. 26 Abs. 1 DS-GVO erforderlichen Vereinbarung der Verantwortlichen zu.

Ergänzend werden auch Transparenz- und Informationspflichten, das Auskunftsrecht und eine mögliche Verpflichtung zur Datenschutz-Folgenabschätzung diskutiert, jeweils unter Berücksichtigung der unterschiedlichen Verantwortungsbereiche.

Der Richtlinienentwurf wurde im September 2020 veröffentlicht und stand bis zum 19. Oktober 2020 zur öffentlichen Konsultation. Im April 2021 wurde die endgültige Fassung veröffentlicht.

Die sehr detaillierten Richtlinien zum Targeting in Social Media sind hilfreich, wenn es darum geht, komplexes Targeting zu analysieren, mögliche Rechtsgrundlagen hierfür zu identifizieren und Verantwortlichkeiten abzugrenzen. Sie konkretisieren die Vorgaben des EuGH und ermöglichen eine europaweit einheitliche Anwendung dieser Grundsätze.

5. Schule

5.1 Gerichtsentscheidungen

Corona – Befreiung von der Maskenpflicht an Schulen aus medizinischen Gründen

Der Beschluss des OVG NRW vom 24. September 2020, Az. 13 B 1368/20, liefert wichtige Anhaltspunkte zu der Frage, welche Daten Schulleitungen verarbeiten dürfen, um über die Befreiung einzelner Schüler*innen von der sog. Maskenpflicht zu entscheiden. Die Coronaschutzverordnung NRW sieht die Möglichkeit einer solchen Befreiung aus medizinischen Gründen vor.

Das Gericht kommt unter Erläuterung der Rahmenbedingungen und Anforderungen, die die Schulleitungen bei ihrer Entscheidung zu berücksichtigen haben, zu dem Ergebnis, dass Schüler*innen zur Glaubhaftmachung eines Ausnahmetatbestandes in Bezug auf die Maskenpflicht eines aussagekräftigen ärztlichen Attestes bedürfen, das bestimmten Mindestanforderungen genügen muss. Wie unserem Homepagebeitrag „Maskenpflicht und Masernschutz – Verarbeitung von Gesundheitsdaten durch Schulen“ im Einzelnen zu entnehmen ist, teilt die LDI NRW die grundlegende Auffassung des OVG NRW. Gleichzeitig weisen wir darauf hin, dass die Angabe konkreter Diagnosen in den Attesten in aller Regel nicht erforderlich sein dürfte.

Corona – Befreiung von der Präsenzpflicht an Schulen wegen Vorerkrankung von Angehörigen

Das Verwaltungsgericht Düsseldorf nimmt in seinem Beschluss vom 1. Dezember 2020, Az. 18 L 2278/20,

in dem es um die Befreiung einer Schülerin vom Präsenzunterricht wegen der Vorerkrankung eines Angehörigen geht, auf die oben genannte Entscheidung des OVG NRW Bezug. Für die Anforderungen an die Glaubhaftmachung der Vorerkrankung seien die Grundsätze heranzuziehen, die für Anträge zur Befreiung von der Maskenpflicht gelten.

5.2 Digitalunterricht und die Schubkraft von Corona

Wer noch zu Jahresbeginn 2020 vorausgesagt hätte, dass Schüler*innen ihre Schulen monatelang nicht mehr betreten und stattdessen „auf Distanz“ unterrichtet werden, dass sich Schüler*innen und Lehrkräfte zeitweise nicht mehr persönlich treffen, sondern allenfalls via Videokonferenz begegnen können und dass die Ausstattung von Lehrkräften mit dienstlichen Endgeräten zügig voranschreiten wird, hätte dafür allenfalls ein müdes Lächeln erhalten. In Pandemiezeiten gehört all dies inzwischen zur schulischen Realität.

Nachdem sich der Einsatz digitaler Lehr- und Lernmittel jahr(zehnt)elang eher schleppend entwickelt hatte, zwang die Corona-Pandemie und der dadurch erforderlich gewordene Unterricht auf Distanz die Verantwortlichen dazu, in kürzester Zeit Versäumnisse aus der Vergangenheit nachzuholen, um praxisgerechte Lösungen zu finden. Wie wichtig dabei auch der Datenschutz ist, zeigt sich anhand der großen Anzahl von Anfragen und Beschwerden, die die LDI NRW erreichten.

Dabei ist es nicht möglich und liegt auch nicht in der Verantwortung der LDI NRW, den Schulen datenschutzgerechte Lösungen zur Verfügung zu stellen.

Er wäre auch nicht angemessen, in der andauernden Pandemiesituation notwendige digitale Unterrichtsgestaltung aus Datenschutzgründen um jeden Preis zu verhindern. Vielmehr sieht die LDI NRW in dieser Situation ihre Aufgabe vorrangig darin, durch Beratung auf datenschutzgerechte Lösungen hinzuwirken, die zugleich den praktischen Erfordernissen gerecht werden.

Insofern hat die Schubkraft von Corona einiges bewegt. So hat das Land NRW die von der LDI NRW seit Jahren empfohlene Ausstattung von Lehrkräften, aber auch von Schüler*innen mit digitalen Endgeräten, die die Sicherstellung eines angemessenen Datenschutzniveaus mit Hilfe technischer Maßnahmen ermöglicht, deutlich vorangetrieben.

Weiterhin gibt es erhebliche Fortschritte im Rahmen des Projekts LOGINEO NRW. So bietet das Land den Schulen inzwischen neben einer digitalen Lernplattform (LOGINEO NRW LMS) auch einen Messenger-Dienst (LOGINEO NRW Messenger) mit integrierter Videokonferenzoption an. Mit dieser Erweiterung des Angebots an digitalen Kommunikationsmitteln im Schulbereich kommt das Land ebenfalls einer Forderung der LDI NRW nach. Die im Rahmen seiner sog. Ressortverantwortung konzipierten Angebote des Schulministeriums NRW entlasten die Schulen bei ihrer Auswahl. Darüber hinaus verzichten sie nach Angaben des Ministeriums auf eine Datenübermittlung in Drittstaaten, an die nach dem „Schrems II“-Urteil des Europäischen Gerichtshofs (Rechtssache C-311/18) erhöhte Anforderungen bestehen.

Die LDI NRW hatte außerdem die Ergänzung der schulrechtlichen Vorschriften um eine gesetzliche

Rechtsgrundlage für die Datenverarbeitung im Zusammenhang mit dem Einsatz von digitalen Lehr- und Lernmitteln angeregt, um Rechtssicherheit zu schaffen und deren verbindlichen Einsatz zu ermöglichen. Dieser Anregung wurde durch Konkretisierung der § 120 Abs. 5 und § 121 Abs. 1 Satz 1 Schulgesetz NRW gefolgt.

Trotz der Verbesserung einiger Rahmenbedingungen besteht die Herausforderung in der Zukunft darin, Lösungen, die angesichts der Dringlichkeit der Pandemiebewältigung zum Einsatz gebracht wurden, im Hinblick auf die Einhaltung des Datenschutzes kritisch zu hinterfragen. Ziel ist der dauerhafte Einsatz von Tools, die den bestmöglichen Ausgleich zwischen Praxistauglichkeit und Gewährleistung eines angemessenen Datenschutzniveaus bieten.

Versäumnisse vieler Jahre lassen sich nicht innerhalb weniger Monate aufholen. Mit Unterstützung durch das Schulministerium NRW befinden sich die Schulen in NRW – sicherlich noch mit unterschiedlichem Tempo – inzwischen aber auf einem guten Weg in das digitale Zeitalter. Dabei dürfen die Anforderungen des Datenschutzes und der Datensicherheit keinesfalls aus den Augen verloren werden.

6. Verwaltung, Inneres und Justiz

6.1 Gerichtsentscheidungen

Das Verwaltungsgericht Gelsenkirchen bestätigt den Anspruch auf kostenlose Klausurkopien für Examenskandidat*innen

Mit Urteil vom 27. April 2020 (Az. 20 K 6392/18) hat das Verwaltungsgericht Gelsenkirchen entschieden: Jura-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. Das Gericht bestätigt damit die Auffassung der LDI NRW. Siehe hierzu unter 6.7. Das Urteil ist noch nicht rechtskräftig, da das Landesjustizprüfungsamt NRW Berufung eingelegt hat.

Gerichtsbeschlüsse zur Videoüberwachung durch Polizeibehörden

Anknüpfend an unseren 24. Bericht (siehe dort unter 9.3), in dem wir über die Ausweitung der Videoüberwachung durch die Polizei und unsere umfassende Prüfung informiert hatten, gibt es in diesem Kontext bemerkenswerte gerichtliche Beschlüsse. So konkretisieren das Verwaltungsgericht Köln und das Oberverwaltungsgericht des Landes NRW (OVG NRW) Detailaspekte zur Videoüberwachung bei Versammlungen. Dabei liegen die Schwerpunkte zwar nicht auf dem Grundrecht auf informationelle Selbstbestimmung, sondern auf dem Grundrecht auf Versammlungsfreiheit (Art. 8 Grundgesetz). Gleichwohl sind die Ausführungen im Rahmen der polizeilichen Videoüberwachung auf jeden Fall zu beachten.

Mit Beschluss vom 13. März 2020 (Az. 15 B 332/20) hat das OVG NRW einen Beschluss des Verwaltungsgerichts Köln bestätigt, wonach bereits die Existenz stationärer polizeilicher Kameras die Versammlungsfreiheit beeinträchtigt, wenn diese Kameras nicht während der Versammlung erkennbar abgedeckt sind.

Einen weiteren inhaltsähnlichen Beschluss des Verwaltungsgerichts Köln beurteilte das OVG NRW mit Beschluss vom 2. Juli 2020 (15 B 950/20) anders. Danach überschreitet grundsätzlich das bloße Vorhandensein vorübergehend deaktivierter Kameras nicht die Schwelle eines Eingriffs in das Grundrecht auf Versammlungsfreiheit. Ein Abschreckungseffekt auf potentielle Versammlungsteilnehmende begründen die nicht verdeckten Kameras demnach zumindest dann nicht, wenn zu Beginn der Versammlung in geeigneter mündlicher Weise darüber informiert wird, dass die Kameras während der Versammlung außer Betrieb sind.

Manuelle Bestandsdatenauskünfte von Sicherheitsbehörden

Die sog. Bestandsdatenauskunft II-Entscheidung vom 27. Mai 2020 (Az. 1 BvR 1873/13, 1 BvR 2618/13) bildet ein weiteres Kapitel der Prüfung von Eingriffsbefugnissen der Sicherheitsbehörden durch das Bundesverfassungsgericht (BVerfG).

Das BVerfG hält die in Folge seiner Bestandsdatenauskunft I-Entscheidung geänderte Vorschrift des § 113 Telekommunikationsgesetz sowie die für verschiedene Sicherheitsbehörden neu geschaffenen Regelungen zum manuellen Abruf von Bestandsdaten für in wesentlichen Teilen mit dem Grundgesetz

unvereinbar. Es betont dabei erneut, dass elementare Voraussetzung für die Verhältnismäßigkeit eines Grundrechtseingriffs von Sicherheitsbehörden ist, dass in Gesetzen – in Abhängigkeit des Eingriffsgewichts der Maßnahme – hinreichende Eingriffsschwellen und Anforderungen an den Rechtsgüterschutz festgeschrieben werden. Zusätzlich kann es erforderlich sein, ergänzende grundrechtssichernde Verfahrensregelungen vorzusehen.

Diese Entscheidungen in der Sache stellen bereits für sich einen weiteren bedeutenden Schritt zur verfassungskonformen Ausgestaltung der Befugnisse der Sicherheitsbehörden dar. Gleichzeitig setzt das Gericht mit der Entscheidung die insbesondere mit dem sog. BKAG-Urteil (also dem Urteil zum Bundeskriminalamtgesetz) vom 20. April 2016 (Az.1 BvR 966/09, 1 BvR 1140/09) begonnene Konsolidierung seiner bisherigen Rechtsprechung zu Eingriffsbefugnissen der Sicherheitsbehörden fort und formuliert unter anderem wichtige Klarstellungen zum Gebot der Zweckbindung sowie zum Prinzip der „Doppeltür“, wonach eine gesetzliche Legitimierung sowohl für die datenübermittelnde Stelle als auch für die datenerhebende Polizei erforderlich ist.

Die mit der Entscheidung für verfassungswidrig erklärten Vorschriften bleiben nach den Maßgaben des Gerichts noch längstens bis zum 31. Dezember 2021 in Kraft. Die Datenschutzkonferenz hat dazu jedoch angemahnt, diese Frist nicht auszureizen (Entschließung der Datenschutzkonferenz „Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten“ vom 25. November 2020 – Abdruck im Anhang). Entsprechend dieser

Mahnung hat der Bundesgesetzgeber noch im Dezember 2020 einen Gesetzentwurf zur Änderung der in Rede stehenden Vorschriften in den Bundestag eingebracht (BT-Drs. 19/25294).

„Data-Mining“ in der Antiterrordatei

Das Bundesverfassungsgericht hat sich im Berichtsjahr erstmals mit der Technik des sog. „Data-Mining“ in durch Sicherheitsbehörden gespeicherten Datenbeständen befasst (Urteil vom 10. November 2020, Az. 1 BvR 3214/15). Gegenstand war eine im Jahr 2015 in Kraft getretene Vorschrift, die die Antiterrordatei für das „Data-Mining“ geöffnet hat. Der Begriff „Data-Mining“ beschreibt die Gewinnung neuer Erkenntnisse aus den Querverbindungen gespeicherter Datensätze. Praktisch handelt es sich um eine umfassende Analyse und Auswertung bestehender Datenbanken.

Die Entscheidung erklärt die Vorschrift des § 6a Antiterrordateigesetz teilweise für verfassungswidrig. „Data-Mining“ stelle einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Dieser liege nicht allein in der zweckändernden weiteren Verwendung vormals getrennter Daten, sondern auch in dem darüberhinausgehenden Zugriff, den die erweiterte Nutzung ermögliche. Insgesamt habe die erweiterte gemeinsame Nutzung durch Polizei und Geheimdienste ein hohes Eingriffsgewicht. Die durch die Vorschrift ermöglichten Eingriffe seien jedoch nur teilweise verhältnismäßig.

Eingriffe in Grundrechte sind nur aufgrund eines verfassungsmäßigen Gesetzes zulässig, welches gemessen am Eingriffsgewicht präzise und normenklar

hinreichende Eingriffsschwellen festlegt und ausreichende Anforderungen an den Rechtsgüterschutz stellt. Derartige ausreichende Eingriffsschwellen waren nach Auffassung des Gerichts vorliegend jedoch nur teilweise gegeben.

Zu Zwecken der Strafverfolgung setze der Einsatz von „Data-Mining“ in der Antiterrordatei einen vom strafprozessualen „Anfangsverdacht“ verschiedenen sog. „verdichteten Tatverdacht“ voraus. Ein solcher war in der Regelung bisher nicht vorgesehen.

Zur Informationsauswertung durch Nachrichtendienste und zu Gefahrenabwehrzwecken hielt das Gericht die gesetzlich geregelte Eingriffsschwelle nach Maßgabe seiner verfassungskonformen Auslegung dagegen noch für mit dem Grundgesetz vereinbar. Danach sei für eine Nutzung zur Gefahrenabwehr mindestens eine hinreichend konkretisierte Gefahr erforderlich. Für den Einsatz von „Data-Mining“ zur Informationsauswertung durch Nachrichtendienste sei ein wenigstens der Art nach konkretisiertes und absehbares Geschehen erforderlich.

Die Entscheidung enthält über den Einzelfall hinaus wichtige grundsätzliche Hinweise für den datenschutzgerechten Einsatz von „Data-Mining“ im Bereich der Sicherheitsbehörden. Diese Hinweise sind hilfreich, da es im Polizeibereich vermehrt Bestrebungen gibt, Software zum „Data-Mining“ auch in polizeilichen Datenbanken einzusetzen.

EuGH-Urteil zur Anwendbarkeit der Datenschutz-Grundverordnung auf den Petitionsausschuss eines Landtags

Nach dem Urteil des Europäischen Gerichtshofs vom 9. Juli 2020 (Az. C-272/19) ist die DS-GVO für den Petitionsausschuss eines Landtags anwendbar. Die Datenschutzkonferenz hat in der Folge ihren Beschluss zur Anwendbarkeit der DS-GVO auf Parlamente angepasst. Siehe Entschließung der Datenschutzkonferenz „Anwendung der DSGVO auf Datenverarbeitungen von Parlamenten“ vom 22. September 2020 (Abdruck im Anhang).

6.2 Veröffentlichungen

- Homepage-Beitrag Abgrenzung justizielle Tätigkeit / Verwaltungsaufgaben von Gerichten
- Homepage-Beitrag Datenspeicherungen durch die Polizei

6.3 Einlasskontrolle bei Gerichten

Gesundheitsdaten dürfen auch im Rahmen der Corona-Pandemie nur erhoben werden, wenn ihre Verarbeitung dem Grundsatz der Verhältnismäßigkeit entspricht.

Ein Rechtsanwalt hat sich an uns gewandt, da an der Einlasskontrolle eines Gerichts von Besucher*innen eine schriftliche Selbstauskunft zum Vorliegen von Covid-19-typischen Krankheitssymptomen verlangt wurde.

Diese Frage betrifft Gesundheitsdaten, die dem grundsätzlichen Verarbeitungsverbot mit Erlaubnisvorbehalt des Art. 9 DS-GVO unterliegen. Ausnahmen zu dem grundsätzlichen Verbot der Verarbeitung von Gesundheitsdaten sind in Art. 9 Abs. 2 DS-GVO abschließend geregelt. Da keine wirksame Einwilligungserklärung nach Art. 9 Abs. 2 Buchtstabe a DS-GVO vorliegt, müsste die erforderliche Datenverarbeitung auf Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats erfolgen, das heißt zumindest auf Grundlage einer Rechtsverordnung.

Zwingende Voraussetzung für die Zulässigkeit der Verarbeitung von Gesundheitsdaten ist die Erforderlichkeit ihrer Verarbeitung. Um Personen mit Covid-19-typischen Krankheitssymptomen den Zutritt zum Gericht zu verweigern, bedarf es keiner schriftlichen Abfrage zum Vorliegen entsprechender Symptome. Vielmehr wäre es zum Beispiel ausreichend, Besucher*innen mit entsprechenden Symptomen den Zutritt ins Gerichtsgebäude durch ein entsprechendes Hinweisschild vor dem Eingang zu untersagen. Eine darüber hinaus gehende schriftliche Erklärung zum Vorliegen von Covid19-typischen Krankheitssymptomen ist aus der Sicht der LDI NRW weder durch die Verordnung zum Schutz vor Neuinfizierungen mit dem Coronavirus SARS-CoV-2 (CoronaSchVO NRW) noch durch entsprechende Erlasse gedeckt.

Durch unser Aufgreifen des Sachverhalts wurde seitens des Gerichts von der Pflicht zur Selbstauskunft nebst Erhebung von Gesundheitsdaten abgesehen. Stattdessen werden Besucher*innen bei der Einlasskontrolle nur noch anlassbezogen entsprechend den Richtlinien des Robert Koch-Instituts nach Krank-

heitssymptomen, die eine Covid-19 Erkrankung nahelegen, wie zum Beispiel starke Erkältungssymptome, Fieber und Husten, befragt. Eine schriftliche Erfassung etwaig mitgeteilter Daten findet nicht statt. Zur Nachverfolgung von Infektionsketten werden Vordrucke verwendet, in denen lediglich Kontaktdaten und das Datum des Gerichtsbesuches erfragt werden.

Die Verarbeitung von sensiblen Gesundheitsdaten ist bei Einlasskontrollen nicht erforderlich, wenn der gleiche Erfolg durch mildere Mittel, wie zum Beispiel durch Hinweisschilder oder mündliche Abfragen vor Betreten eines Gebäudes, erreicht werden können.

6.4 Weitergabe von Gesundheitsdaten an Leitstellen von Polizei, Feuerwehr und Rettungsdiensten

Die Weitergabe von Gesundheitsdaten durch Gesundheitsämter an Einsatzkräfte ist nicht dazu geeignet, einsatzspezifischen Gefahren im Rahmen der Corona-Pandemie zu begegnen.

Zu Beginn der Corona-Pandemie erreichten uns Anfragen, ob die Übermittlung der Daten von Gesundheitsämtern über Corona-Infizierte und deren Kontaktpersonen an Leitstellen von Polizei, Feuerwehr und Rettungsdiensten zulässig sei. Dies wurde von der LDI NRW verneint.

Gemäß § 23 Abs. 2 Gesundheitsdatenschutzgesetz (GDSG NRW) ist die Übermittlung von Daten an Dritte außer in den Fällen des § 5 Abs. 1 GDSG NRW nur zulässig, soweit dies zur Abwehr einer gegenwärtigen Gefahr für Leben, körperliche Unversehrtheit oder persönliche Freiheit des Betroffenen oder eines Dritten erforderlich ist. Eine pauschale Übermittlung

der Daten von Infizierten und deren Kontaktpersonen ist zur Abwehr einer gegenwärtigen Gefahr weder geeignet, erforderlich noch angemessen.

Zum einen würde die Übermittlung dieser Daten nur eine scheinbare Sicherheit für Einsatzkräfte bieten. Aufgrund der Meldewege können die Information über den aktuellen Gesundheitszustand der Personen im Zeitpunkt eines Einsatzes schon veraltet sein. Zum anderen bieten diese Daten keinen Schutz vor Personen, die keine Krankheitssymptome aufweisen. Vielmehr helfen hier nur Eigensicherungsmaßnahmen, die auf der Grundlage der Empfehlungen des Robert Koch-Instituts (RKI) zu treffen sind, um Einsatzkräfte vor möglichen Infektionsrisiken bei Einsätzen zu schützen.

Zu der Nutzung von Erkenntnissen aus „Corona-Datenbanken seitens der Polizei stellt ein Erlass des Innenministeriums NRW vom 27. März 2020 fest, dass sowohl die Speicherung von personengebundenen Hinweisen auf eine Corona-Infizierung in polizeilichen Auskunftssystemen als auch die Nutzung von „Corona-Datenbanken“ anderer Behörden untersagt bleibe.

Eigensicherungsmaßnahmen bieten Einsatzkräften Schutz vor möglichen Infektionsrisiken in der Corona-Pandemie; eine übermäßige Datenweitergabe hingegen nicht.

6.5 Datenübermittlungen durch Staatsanwaltschaften an Sachverständige

Staatsanwaltschaften haben infolge unserer Empfehlungen begonnen, ihre Praxis hinsichtlich der Beauftragung von Sachverständigen datenschutzgerecht zu gestalten.

Im Jahr 2017 wurden wir aufgrund einer Beschwerde darauf aufmerksam, dass eine Staatsanwaltschaft in einem Strafverfahren wegen möglicher Urheberrechtsverletzungen mehrere vollständige Datenträger einer verdächtigen Person an die Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU) und die proMedia Gesellschaft zum Schutz geistigen Eigentums mbH (proMedia) zwecks Auswertung übersandt hatte. Bei diesen Gesellschaften handelt es sich um privatrechtlich organisierte Einrichtungen, die im Auftrag der Film- und Musikindustrie Urheberrechtsverletzungen zivilrechtlich verfolgen. Da sie unmittelbar mit diesem Industriebereich zusammenarbeiten, sind oft nur diese Organisationen in der Lage festzustellen, ob es sich bei einer Datei um eine illegale Kopie eines urheberrechtlich geschützten Werkes handelt. Ihnen kommt somit eine wichtige Funktion bei der Feststellung von Urheberrechtsverstößen zu.

Problematisch ist dabei, dass die Gesellschaften die übersandten Dateien bislang nicht nur für Zwecke der Strafverfolgung auf Urheberrechtsverstöße untersucht haben. Sie haben die Ergebnisse vielmehr auch für ihre eigene Aufgabe der zivilrechtlichen Verfolgung von Urheberrechtsverstößen für die Film- und Musikindustrie genutzt. Damit haben die Gesellschaften Informationen, die ihnen zum Zweck ihrer Tätigkeit als Sachverständige im Strafverfahren übermittelt

worden waren, zugleich für eigene wirtschaftliche Zwecke genutzt. Dies ist nicht zulässig.

Sachverständige haben ihre Aufgabe unabhängig wahrzunehmen und sind verpflichtet, die ihnen im Rahmen ihrer Sachverständigentätigkeit anvertrauten Daten ausschließlich für diesen Zweck zu verwenden. Soweit mangels gleichgeeigneter anderer Fachleute bestimmte Sachverständige eingeschaltet werden müssen, obwohl diese möglicherweise nicht unabhängig sind, ist seitens der Strafverfolgungsbehörden durch geeignete Maßnahmen sicherzustellen, dass eine Verwendung der übermittelten Daten für eigene Zwecke unterbunden wird. Dies wird nunmehr mittels einer Verfügung zur Verwendungsbeschränkung erreicht, mit der Sachverständige verpflichtet werden, die gewonnenen Erkenntnisse nicht für eigene Zwecke zu nutzen.

In dem konkret geprüften Einzelfall fiel darüber hinaus ein weiteres Problem auf: Die Staatsanwaltschaft hatte an die Sachverständigen die jeweiligen Datenträger vollständig übermittelt. Letztere enthielten teils Urlaubsfotos und andere offensichtlich private Daten, bei denen ein Zusammenhang mit der verfolgten Straftat eindeutig ausgeschlossen werden konnte. Zudem wurden weitere Angaben wie Name und Adresse der verdächtigen Person an die Sachverständigen übersandt. Dieselbe Problematik gab es allerdings auch bei der Einschaltung unabhängiger Sachverständiger.

Auch diesbezüglich hat die Staatsanwaltschaft inzwischen ihre Verfahrenspraxis geändert: Nunmehr werden an alle Sachverständige ausschließlich solche Dateien weitergegeben, die zur Bewertung der in

Rede stehenden Straftat erforderlich sind. Auch weitere Angaben wie Namen und Adressen der Verdächtigen werden lediglich dann übermittelt, wenn dies im Einzelfall notwendig ist.

Wir haben uns an das Justizministerium NRW sowie die drei Generalstaatsanwaltschaften mit der Bitte gewandt, alle Staatsanwaltschaften in NRW auf die oben beschriebenen Verfahrensvorschläge hinzuweisen. Mittlerweile haben uns Rückmeldungen von mehreren Staatsanwaltschaften erreicht, dass unsere Hinweise künftig beachtet werden und die Beschäftigten entsprechend sensibilisiert wurden.

Die aufgrund der Empfehlungen der LDI NRW geänderte Praxis stellt eine deutliche Verbesserung gegenüber der bisherigen Vorgehensweise dar. Aufgrund der Verwendungsbeschränkung und der Beschränkung der Übermittlung auf notwendige Daten wird dem Recht auf informationelle Selbstbestimmung der betroffenen Personen in angemessenem Maße Rechnung getragen. Gleichzeitig ist aber weiterhin sichergestellt, dass die Sachverständigen alle Daten erhalten, die für diese Tätigkeit erforderlich sind.

6.6 Technisches System zur Erkennung von Suizidversuchen im Strafvollzug

Bei Gefangenen in Justizvollzugsanstalten ist die Suizidrate deutlich höher als in der übrigen Bevölkerung. Die Landesregierung hat es sich daher zur Aufgabe gemacht, zur Verbesserung der Suizidprävention auch die Möglichkeit eines Einsatzes von Künstlicher Intelligenz (KI) auszuloten. Dabei gilt es vor allem auch, den Anforderungen des Datenschutzes Rechnung zu tragen.

Als weiterer Baustein bei der Verbesserung der Suizidprävention in Justizvollzugsanstalten soll zukünftig eine ereignisgesteuerte Videoüberwachung von Gefangenen hinzutreten. Dieses Überwachungssystem soll potentielle Suizidvorhaben in den Hafträumen erkennen und an die Justizvollzugsbediensteten melden.

Die Bewertung als Suizidvorhaben soll dabei durch einen Abgleich der Videoaufnahme mit Bewegungsmustern erfolgen, die in dem System als typischerweise suizidale Handlung hinterlegt sind. Relevante Merkmale könnten beispielsweise bestimmte Bewegungsabläufe bei einem Strangulationsversuch oder der Einsatz gefährlicher Gegenständen (zum Beispiel Messer) sein. Das Einspeisen typischer Bewegungsmuster soll in der Entwicklungsphase des Systems stattfinden.

In diesem Stadium soll auch die technische Grundlage für sein selbständiges Lernen angelegt werden. Der eigentliche Lernprozess durch diese KI-Komponente soll sodann während des Einsatzes in der Praxis erfolgen. Die Justizvollzugsbediensteten führen

dem System nach der Meldung eines Suizidvorhabens die Information zu, ob es die Situation richtig bewertet hat. Das System speichert diese Information ab und verwertet sie zur Verbesserung des verwendeten Algorithmus.

Im Jahr 2019 hat das Ministerium der Justiz NRW ein Forschungsprojekt ins Leben gerufen, in dessen Rahmen ein solches System entwickelt und getestet werden soll. Erweist es sich dabei als hilfreich, soll es zunächst in einer Justizvollzugsanstalt im Pilotbetrieb zum Einsatz kommen.

In unserer Stellungnahme an den Landtag vom 6. Mai 2020 (Landtag-Stellungnahme 17/2617) haben wir unter anderem auf folgende Aspekte hingewiesen:

- Der Einsatz eines solchen technischen Systems kann sinnvoll sein und ist grundsätzlich datenschutzgerecht umsetzbar. Allerdings hängt das von der genauen Ausgestaltung des Systems ab, das heißt etwa dem Kreis der zugriffsberechtigten Personen, Speicherfristen, dem Ausschluss oder der Beschränkung von Zweckänderungen und der Nachvollziehbarkeit der Ergebnisse und Entscheidungen.
- Erforderlich ist eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Dabei ist zwischen der Entwicklung und dem Einsatz des Systems zu unterscheiden.
- Unzulässig ist vor dem Hintergrund der in Art. 1 Grundgesetz verbrieften Menschenwürde jedenfalls, die Daten von Gefangenen für die erstmalige Entwicklung des Systems zu verwenden. Sie hat folglich ausnahmslos mit Schauspieler*innen zu erfolgen. Als Grundlage für die Datenverarbeitung kommt diesbezüglich eine Einwilligung oder

ein Vertrag in Betracht (Art. 6 Abs. 1 Satz 1 Buchstaben a, b DS-GVO). Der nähere rechtliche Rahmen für die erstmalige Einrichtung bzw. Entwicklung des Systems ist nach § 24 Abs. 8 Justizvollzugsdatenschutzgesetz NRW (JVollzDSG NRW) durch eine Rechtsverordnung festzulegen. Das ist bislang noch nicht erfolgt.

- § 24 Abs. 7 Satz 2 JVollzDSG NRW stellt die Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Gefangenen beim Betrieb des Systems dar. Das umfasst grundsätzlich auch die Weiterentwicklung des Systems im Rahmen seiner Eigenschaft als KI-System. Für den späteren Lernprozess der Systeme dürfen Gefangenendaten somit grundsätzlich verwendet werden.
- Die gesetzgeberischen Wertungen sind auch bei der Fortentwicklung des Systems zu berücksichtigen. Hierzu gehören insbesondere die Auswahl der an der Fortentwicklung beteiligten Personenkreise, der nötige Umfang der Aufzeichnungen von Videosequenzen und die Sicherstellung der Zweckbindung der aufgezeichneten Videodaten ausschließlich zur Suizidprävention.

KI-Systeme zur Suizidprävention sind grundsätzlich datenschutzgerecht umsetzbar, soweit die aufgezeigten Leitplanken beachtet werden. Die LDI NRW stand und steht insoweit gerne beratend zur Verfügung.

Wenn Ihre Gedanken darum kreisen, sich das Leben zu nehmen, bieten verschiedenen Organisationen Hilfe und Auswege an. Die Telefonseelsorge etwa ist unter 0800 / 111 0 111 oder 0800 / 111 0 222 anonym und kostenlos zu erreichen. Dort können Sie rund um die Uhr mit anderen Menschen über Ihre Sorgen und Ängste sprechen. Die Telefonseelsorge bietet unter www.telefonseelsorge.de auch einen Hilfe-Chat und eine E-Mail-Beratung an.

6.7 Anspruch auf kostenfreie Klausurkopien im juristischen Staatsexamen

Das Verwaltungsgericht Gelsenkirchen bestätigt unsere Auffassung: Prüflinge im juristischen Staatsexamen haben einen Anspruch auf kostenlose Übermittlung ihrer Klausuren samt Gutachten in Kopie. Während die Vorteile des europäischen Datenschutzrechts für die Prüflinge unmittelbar spürbar werden, wird für Prüfungsämter möglicherweise zusätzlicher Arbeits- und ggf. auch Kostenaufwand anfallen. Das Urteil ist allerdings noch nicht rechtskräftig.

Wollten Prüflinge in den juristischen Staatsexamina ihre geschriebenen Klausuren und die Gutachten kostenfrei in Augenschein nehmen, so mussten sie bislang das für sie zuständige Prüfungsamt aufsuchen und dort Einsicht in die Akten nehmen. Geregelt ist dieses Einsichtsrecht in § 23 Abs. 2 Satz 1 des Juristenausbildungsgesetzes NRW (JAG NRW).

In der Datenschutz-Grundverordnung (DS-GVO) wurde ein Anspruch auf Übermittlung kostenfreier Ko-

pien (in Papierform oder elektronisch) von personenbezogenen Daten festgeschrieben, die Gegenstand der Verarbeitung sind (Art. 15 Abs. 3 in Verbindung mit Art. 12 Abs. 5 Satz 1 DS-GVO).

Wenn Prüflinge davon ausgingen, dass dieser Anspruch nun neben das Einsichtsrechts vor Ort treten würde, wurden sie jedoch tatsächlich enttäuscht. Soweit uns bekannt ist, stellte kein Prüfungsamt die Kopien unentgeltlich zur Verfügung. Einige Prüflinge haben sich daher an uns gewandt. Wir haben ihr Anliegen gegenüber dem jeweiligen Prüfungsamt aufgegriffen und dargelegt, dass der begehrte Anspruch besteht. Auch dem Justizministerium NRW haben wir unsere Rechtsansicht vorgetragen, konnten allerdings leider keine übereinstimmende Auffassung erzielen.

Zudem haben wir in unserer Stellungnahme zur neuen Fassung des JAG NRW darauf hingewiesen, dass wir eine Klarstellung zu dem Bestehen des Anspruchs aus Transparenzgründen für geboten halten.

In der Zwischenzeit hatte ein Prüfling Klage gegen das Landesjustizprüfungsamt NRW erhoben. Das Verwaltungsgericht Gelsenkirchen bestätigt in seinem Urteil unsere Auffassung (Urteil vom 27. April 2020, Az. 20 K 6392/18).

Die maßgeblichen Erwägungen des Gerichts und der LDI NRW sind insbesondere folgende:

- Es kann dahinstehen, ob die Vorschriften der DS-GVO aufgrund eines möglicherweise fehlenden Unionsrechtsbezugs der in Rede stehenden Verarbeitung schon gar keine Anwendung finden (vgl. Art. 2 Abs. 2 Buchstabe a DS-GVO), denn

§ 5 Abs. 8 Satz 1 Datenschutzgesetz NRW (DSG NRW) ordnet in diesen Fällen eine entsprechende Anwendung der Vorschriften der DS-GVO an.

- Das analoge Archivieren der Klausuren stellt eine Verarbeitung personenbezogener Daten dar, die in einem Dateisystem gespeichert sind (Art. 2 Abs. 1 DS-GVO, Art. 4 Nr. 6 DS-GVO). Die Aufsichtsarbeiten sind nach Kennziffern geordnet und abgelegt, die sich aus Jahrgang und laufender Nummer als Zuordnungskriterien zusammensetzen. Der sachliche Anwendungsbereich der DS-GVO ist damit eröffnet. Letztlich kann allerdings auch diese Frage aufgrund des § 5 Abs. 8 DSG NRW dahinstehen. Für manuelle Sammlungen von Akten, die nicht nach bestimmten Kriterien sortiert sind, wird im Ergebnis die entsprechende Anwendbarkeit der Vorschriften der DS-GVO angeordnet.
- Es gibt keine Vorschriften, die den Anspruch beschränken könnten. § 23 Abs. 2 Satz 1 JAG NRW lässt sich nicht entnehmen, dass mit dem Einsichtsrecht zugleich ein Ausschluss des Rechts auf Erhalt einer Kopie einhergeht. Die Ansprüche stehen vielmehr nebeneinander. Auch die gebührenrechtlichen Vorschriften des Landes NRW können die Unentgeltlichkeit des Anspruchs nicht beschränken. Die jeweiligen Vorschriften sind zu allgemein gefasst, sodass sie in gemeinschaftsrechtskonformer Auslegung keine beschränkende Wirkung hinsichtlich der Unentgeltlichkeit haben können.
- Die Argumente, bei einer Anerkennung des Anspruchs sei mit finanziellen Mehraufwendungen zu rechnen und der Betrieb des Prüfungsamts gefährdet, vermögen den Anspruch der Prüflinge

nicht auszuschließen. Zum einen wird dem Verantwortlichen die Kostenlast für Ansprüche aus der DS-GVO bewusst aufgebürdet. Der Haushaltsgesetzgeber hat sicherzustellen, dass die Ansprüche der Bürger*innen erfüllt werden. Zum anderen ist eine nicht zu bewerkstelligende Mehrbelastung nicht zwingend erkennbar. Prüflinge werden vermutlich mit einer elektronischen Kopie einverstanden sein, sodass der Aufwand für das Anfertigen analoger Kopien abnehmen wird.

Den Prüflingen vereinfacht der Anspruch aus Art. 15 Abs. 3 DS-GVO den Zugang zu ihren korrigierten Klausuren samt Gutachten - eine Fahrt zum jeweiligen Prüfungsamt ist für eine kostenlose Inaugenscheinnahme nicht länger erforderlich. Ob das Urteil des Verwaltungsgerichts Gelsenkirchen Bestand haben wird, wird sich im Berufungsverfahren zeigen.

6.8 „Blitzer“ auf der Umweltspur

Die Kontrolle von Verkehrsverstößen ist sinnvoll und grundsätzlich mit dem Datenschutzrecht vereinbar. Eine Stadt ist dabei jedoch über das Ziel hinausgeschossen, indem sie anlasslos jedes Fahrzeug fotografieren ließ, das sich auf einer bestimmten Fahrspur befand.

Um die Stickoxidbelastung in der Luft zu reduzieren, haben einige Städte Bussonderspuren eingerichtet, die grundsätzlich nicht von Autos mit Verbrennungsmotoren genutzt werden dürfen. Regelmäßig besteht eine Nutzungserlaubnis ausschließlich für Busse, Taxis, Fahrräder und Elektroautos (sog. Umweltspuren).

Aufgrund der Beschwerde eines Elektroautofahrers wurden wir darauf aufmerksam, dass eine Stadt zur Kontrolle von Verstößen gegen die Nutzung einer Umweltspur eine Geschwindigkeitsmessanlage auf „0 km/h“ eingestellt hatte. Diese Anlage erfasste damit fotografisch sämtliche passierende Fahrzeuge und ihre Insass*innen. Folglich wurden auch jene erfasst, die die Spur rechtmäßig nutzten. Die Einstellung war darauf zurückzuführen, dass sich ein Verstoß gegen das Nutzungsverbot nicht separat durch die Anlage erfassen ließ.

Die Aufnahme von Fotos zur Ahndung von Verkehrsverstößen ist grundsätzlich zulässig. Als Rechtsgrundlage kommt § 100h Abs. 1 Satz 1 Nr. 1 Strafprozessordnung in Verbindung mit § 46 Abs. 1 Ordnungswidrigkeitengesetz in Betracht. Diese Vorschriften gestatten jedoch nicht eine verdachtsunabhängige Erhebung von Daten, wie dies bei einem Auslösen der Messanlage bei jedem passierenden Fahrzeug der Fall ist. Da die Anlage mehrere Monate in

dieser Weise betrieben wurde, sind wohl zahlreiche Datenschutzverstöße erfolgt.

Wir haben diesen Sachverhalt gegenüber der Stadt aufgegriffen und dadurch rasch bewirken können, dass der Betrieb der Anlage in der beschriebenen Form eingestellt wurde. Eine Überprüfung des Nutzungsverbots der Spur ist seither an eine Kontrolle der erlaubten Höchstgeschwindigkeit gekoppelt.

„Blitzer“, die personenbezogene Daten erheben, dürfen nicht so eingestellt werden, dass sie jedes Fahrzeug fotografieren und erst im Anschluss ermittelt wird, ob tatsächlich ein Verkehrsverstoß vorliegt. Durch unser Eingreifen haben wir Datenschutzverstöße abgestellt und konnten zugleich einen Beitrag dazu leisten, eine rechtswidrige Praxis zur Ermittlung von Verkehrsverstößen zu beenden.

6.9 Entwurf eines Betreuungsorganisationsgesetzes

Die Bundesregierung plant eine Reform des Vormundschafts- und Betreuungsrechts, die auch bereichsspezifische Regelungen zur Datenverarbeitung durch Betreuer*innen enthält. Dies geht aus dem Entwurf eines Gesetzes zur Reform des Vormundschafts-und Betreuungsrechts hervor (BT-Drucksache 19/24445).

Die Reform der materiell- und verfahrensrechtlichen Vorschriften des Betreuungsrechts ist auf das zentrale Ziel ausgerichtet, auf den verschiedenen Umsetzungsebenen im Vorfeld und innerhalb der rechtlichen Betreuung eine konsequent an der Verwirklichung des Selbstbestimmungsrechts der Betroffenen orientierte Anwendungspraxis zu gestalten, die die

Betroffenen bei der Ausübung ihrer rechtlichen Handlungsfähigkeit unterstützt.

Das Betreuungsbehördengesetz soll durch ein Betreuungsorganisationsgesetz (BtOG-E) ersetzt werden. In dieses Gesetz sollen künftig all diejenigen Regelungen Eingang finden, die die Rechtsstellung und Aufgaben der Betreuungsbehörden, der Betreuungsvereine und der rechtlichen Betreuer*innen näher ausgestalten. Für diese im Betreuungsrecht tätigen Akteur*innen werden im BtOG-E erstmals auch bereichsspezifische Datenschutzregelungen eingeführt. Soweit diese Rechtsgrundlagen keine Regelungen treffen, gilt für die Datenverarbeitung der genannten Akteur*innen die Datenschutz-Grundverordnung (DS-GVO).

Aus Sicht der LDI NRW ist es zu begrüßen, dass aus Gründen der Rechtsklarheit die Schaffung einer bereichsspezifischen Rechtsgrundlage für die Datenverarbeitung durch rechtliche Betreuer*innen erfolgen soll. Die zentralen datenschutzrechtlichen Regelungen des BtOG-E knüpfen dabei an das Kriterium der Erforderlichkeit der Datenverarbeitung zur Erfüllung der jeweiligen Aufgaben an. Dies entspricht der Systematik, die sich etwa auch in den allgemeinen Rechtsgrundlagen nach Art. 6 Abs. 1 Satz 1 Buchstabe b bis f DS-GVO sowie in § 26 Abs. 1 und Abs. 3 Bundesdatenschutzgesetz für den Bereich der Beschäftigungsverhältnisse findet.

6.10 Keine Preisgabe der Identität von Petent*innen, auch nicht bei Akteneinsicht durch den Verantwortlichen!

Das Recht, sich bei einer tatsächlichen oder angenommenen Verletzung des Rechts auf informationelle Selbstbestimmung mit einer Beschwerde an die LDI NRW wenden zu können, dient dem effektiven Schutz der Bürger*innen. Niemand soll aufgrund einer Beschwerde bei der LDI NRW gegen seinen Willen die Preisgabe seiner Identität und mögliche Nachteile befürchten müssen.

In einer nordrhein-westfälischen Stadt waren zu Marketingzwecken von einem Gebäude zwei Webcams auf Teile der Fußgängerzone gerichtet. Der dafür Verantwortliche stellte das Geschehen auf einer von ihm betriebenen Internetseite dar. Nachdem bei der LDI NRW eine Beschwerde über die Webcam eingegangen war, verlangte der Verantwortliche Akteneinsicht in die bei uns geführte Verwaltungsakte. Insbesondere ging es ihm darum zu erfahren, wer die LDI NRW auf die Videoüberwachungsanlage aufmerksam gemacht hatte. Der Petent hatte in seiner Beschwerde zum Ausdruck gebracht, mit der Mitteilung seiner Identität an Dritte nicht einverstanden zu sein. Der Verantwortliche erhielt zwar Akteneinsicht, allerdings wurden personenbezogene Daten des Petenten geschwärzt. Die LDI NRW begründete dies damit, dass nach Abwägung der gegenseitigen Interessen aufgrund der DS-GVO, des Datenschutzgesetzes NRW (DSG NRW) und des Verwaltungsverfahrensgesetzes NRW (VwVfG NRW) ein Auskunfts- und Einsichtsrecht insoweit nicht besteht.

Im Verwaltungsverfahren begründete der Verantwortliche sein Begehren damit, er benötige die ungeschwärzte Verwaltungsakte zur Vervollständigung seiner Akte sowie für ggf. zukünftige Verwaltungsstreitverfahren. Gegen die durch Schwärzung der Daten des Petenten nur teilweise gewährte Akteneinsicht klagte der Verantwortliche vor dem Verwaltungsgericht. In seiner Klagebegründung führte er zudem mögliche zivilrechtliche Schadensersatzansprüche wegen falscher Verdächtigung, Vortäuschen einer Straftat, Kreditgefährdung und sittenwidriger vorsätzliche Schädigung ins Feld. Darüber hinaus behauptete der Verantwortliche, der Petent sei kein Betroffener nach Art. 77 DS-GVO.

Den Argumenten des Verantwortlichen trat die LDI NRW sowohl im Verwaltungs- als auch im Klageverfahren entgegen.

Das Verwaltungsgericht hat sich mit den Argumenten des Verantwortlichen und der LDI NRW in seinem Urteil umfassend auseinandergesetzt und gab der LDI NRW recht, indem es einen Anspruch des Verantwortlichen auf Akteneinsicht mit dem Ziel, die Identität des Petenten zu erfahren, unter allen denkbaren rechtlichen Aspekten verneinte. Das Gericht begründete seine Auffassung – unter Hinweis auf § 29 Abs. 2 Var. 3 VwVfG NRW und der weiteren oben genannten Rechtsgrundlagen – im Wesentlichen sowohl mit der objektiven Geheimhaltungsbedürftigkeit der personenbezogenen Daten des Petenten als auch mit seinem überwiegenden berechtigten Geheimhaltungsinteresse. Dabei stellte es insbesondere auf mögliche Nachteile für den Petenten ab für den Fall, dass der Verantwortliche bei Preisgabe von dessen Identität gegen diesen vorgeht.

Die Webcams wurden nach Tätigwerden der LDI NRW durch den Verantwortlichen so eingestellt, dass eine Identifizierung von Passanten ausgeschlossen ist.

Auch im Falle einer Akteneinsicht durch den Verantwortlichen für die Datenverarbeitung besteht in der Regel kein Recht, die Identität der Beschwerdeführer*innen zu erfahren. Dies wurde durch das Verwaltungsgericht bestätigt.

7. Gesundheit und Soziales

7.1 Prüfaktion zu Datenschutzbeauftragten bei großen Krankenhäusern in NRW

Krankenhäuser verarbeiten mit Gesundheitsdaten überwiegend besondere Datenkategorien. Sie sind daher besonders auf die Unterstützung durch eigene Datenschutzbeauftragte bei der Einhaltung datenschutzrechtlicher Vorgaben angewiesen. Wir haben geprüft, ob große Krankenhäuser in NRW ihrer Verpflichtung zur Benennung von Datenschutzbeauftragten nachkommen.

Gegenstand der Prüfaktion war, ob die Krankenhäuser eigene Datenschutzbeauftragte benannt, deren Kontaktdaten an geeigneter Stelle veröffentlicht und diese der LDI NRW gemeldet haben. Für die Prüfung haben wir 32 große Krankenhäuser mit mindestens 500 Betten herangezogen. Nicht in die Prüfung einbezogen wurden Krankenhäuser in kirchlicher oder bundesunmittelbarer Trägerschaft (zum Beispiel Knappschaft, Berufsgenossenschaften).

Für Krankenhäuser, die als privatwirtschaftliches Unternehmen geführt werden, ergibt sich die Pflicht zur Benennung von Datenschutzbeauftragten aus Art. 37 Abs. 1 Buchstabe c Datenschutz-Grundverordnung (DS-GVO). Danach benennen Verantwortliche und Auftragsverarbeiter immer dann Datenschutzbeauftragte, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Verarbeitung besonderer Kategorien von Daten nach Art. 9 besteht. Für Krankenhäuser in öffentlicher Hand ergibt sich die Pflicht zudem aus Art. 37 Abs. 1 Buchstabe a DS-GVO, da öffentliche Stellen in jedem Fall Datenschutzbeauftragte zu benennen haben.

Als Datenschutzbeauftragte können geeignete Personen innerhalb oder außerhalb des Verantwortlichen bzw. Auftragsverarbeiters benannt werden.

Die Prüfaktion hatte folgendes Ergebnis:

Alle geprüften Krankenhäuser sind der Pflicht zur Benennung von Datenschutzbeauftragten nachgekommen und haben deren Kontaktdaten an geeigneter Stelle veröffentlicht. Sechs von 32 Krankenhäusern haben wir allerdings empfohlen, zusätzliche Angaben auf der jeweiligen Homepage zu ergänzen, um Patient*innen sowie anderen Betroffenen die Kontaktaufnahme zu den Datenschutzbeauftragten zu erleichtern. Zwei Krankenhäuser sind dieser Empfehlung gefolgt.

Drei von 32 Krankenhäusern hatten die Kontaktdaten ihrer Datenschutzbeauftragten der LDI NRW noch nicht gemäß Art. 37 Abs. 7 DS-GVO gemeldet; haben dies aber nachgeholt.

Krankenhäuser verarbeiten nahezu ausschließlich sensible Daten, deshalb kommt der internen Beratung und Kontrolle durch eigene Datenschutzbeauftragte ein besonderes Gewicht zu. Erfreulicherweise haben die Verantwortlichen dies erkannt und in allen Fällen Datenschutzbeauftragte benannt.

7.2 Erhebung von Gesundheitsdaten bei Besuchen von stationären Pflegeeinrichtungen

Vor Betreten einer stationären Pflegeeinrichtung ist die Erhebung von Gesundheitsdaten durch ein Kurzscreening zulässig.

Uns erreichen im Zuge der Corona-Pandemie zahlreiche Anfragen von Angehörigen dazu, ob sie verpflichtet seien, vor Einlass in stationäre Pflegeeinrichtungen Angaben zu ihrem Gesundheitszustand mitzuteilen.

Die Erhebung der Gesundheitsdaten ist gemäß Art. 6 Abs. 1 Buchtstabe c, Art. 9 Abs. 2 Buchstabe i DS-GVO in Verbindung mit §§ 17 Abs. 4, 16 Abs. 1 Infektionsschutzgesetzes (IfSG) in Verbindung mit § 10 Coronaschutzverordnung (CoronaSchVO, Stand 24.06.2021) und Nr. 2.4 der Allgemeinverfügung des Gesundheitsministeriums (CoronaAVPflegeundBesuche, Stand 05.02.2021) zulässig. Aufgrund der besonderen Vulnerabilität der Pflegeheimbewohner*innen ist vorgesehen, dass bei Besucher*innen anlässlich jedes Besuchs ein Kurzscreening (Erkältungssymptome, SARS-CoV-2-Infektion, Kontakt mit Infizierten oder Kontaktpersonen ersten Grades gemäß der Richtlinie des Robert Koch-Instituts) einschließlich Temperaturmessung durchzuführen ist. Dies dient dazu festzustellen, ob ein Zutritt zu der Einrichtung möglich ist. Auf diese Weise soll verhindert werden, dass Krankheitserreger in die Einrichtungen eingetragen werden. Eine Verweigerung der Mitwirkung am Kurzscreening berechtigt die Einrichtungsleitung dazu, den Zutritt zu versagen. Weitergehende Gesundheitsdaten, die keinen Zusammenhang zu der Infektionslage haben können, dürfen hingegen nicht erhoben werden.

Unabhängig vom Kurzscreening ist zur Rückverfolgbarkeit gemäß § 8 Abs. 1 CoronaSchVO in Verbindung mit Nr. 2.8 CoronaAVPflegeundBesuche ein Besuchsregister zu führen, in dem die Namen der Besucher*innen, eine Telefonnummer, unter der die Besucher*innen erreicht werden können, das Datum und die Uhrzeiten von Beginn und Ende des Besuchs sowie die Besuchten erfasst werden. Diese Daten sind vier Wochen aufzubewahren und anschließend zu vernichten, sofern sie nicht von der nach § 28 Abs. 1 IfSG zuständigen Behörde benötigt werden

Bei Besuchen von Pflegeeinrichtungen dürfen Gesundheitsdaten von Besucher*innen mit Bezug zur Corona-Infektion im Rahmen eines Kurzscreenings erhoben werden. Auch die Erhebung und vierwöchige Aufbewahrung von festgelegten Kontaktdaten für ein Besucherregister ist zulässig.

7.3 Datenschutz im Krankenhaus

Informationen über Krankenhausaufenthalte an Dritte dürfen nur erfolgen, wenn Patient*innen einer Weitergabe zuvor ausdrücklich zugestimmt haben. Hierzu sind entsprechende Informationen im Krankenhausinformationssystem zu hinterlegen.

Bei der Aufnahme im Krankenhaus hat ein Patient angegeben, dass keine Informationen über seinen Krankenhausaufenthalt an externe Dritte herausgegeben werden sollen. Durch einen Fehler im Aufnahmeprozess wurde die Auskunftssperre nicht im Krankenhausinformationssystem vermerkt. Als eine nahe Verwandte anrief, wurde das Telefonat an den Patienten weitergeleitet. Hiergegen hat der Betroffene bei der

LDI NRW Beschwerde gegen das Krankenhaus erhoben.

Aufgrund des Beschwerdeverfahrens wurden die Beschäftigten des Krankenhauses eingehend dahingehend sensibilisiert, dass Auskünfte über Krankenhauspatient*innen nur mit deren ausdrücklicher Zustimmung erfolgen dürfen. Gleichzeitig wurde der Aufnahmeprozess verbessert. Standardmäßig wird nun detailliert abgefragt, ob und an wen welche Auskünfte erteilt werden dürfen. Diese Informationen werden im Krankenhausinformationssystem hinterlegt. Zudem findet eine regelmäßige Überprüfung des Aufnahmeprozesses durch Qualitätsmanagementbeauftragte des Krankenhauses statt. Verbesserungsmöglichkeiten werden zusammen mit der Geschäftsleitung und Datenschutzbeauftragten erarbeitet und umgesetzt. Außerdem wird das Thema „Weitergabe von Patient*innendaten und unbefugte Offenbarungen“ in internen Schulungen für Beschäftigte vertieft.

Ein effektiver Datenschutz im Krankenhaus kann nur sichergestellt werden, wenn die Prozesse auf allen Ebenen überprüft, angepasst und regelmäßig kontrolliert werden.

7.4 Offenbarung von Gesundheitsdaten im Wartebereich eines Krankenhauses

Die LDI NRW erreichen immer wieder Fälle, die belegen, dass Patient*innendaten im Krankenhausbereich nicht mit der erforderlichen Sorgfalt behandelt werden. Dies führt beispielsweise in Wartebereichen oft zu einer unangemessenen Offenbarung von Patient*innendaten.

Die LDI NRW erhielt einen Hinweis, dass in einem Krankenhaus pflegerische Aufnahmegespräche im Wartebereich durchgeführt werden. Hierdurch bekämen alle im Wartebereich anwesenden Personen ungewollt Kenntnis von hochsensiblen Gesundheitsdaten.

Die LDI NRW nahm dies zum Anlass, das Krankenhaus auf die besondere Schutzwürdigkeit von Gesundheitsdaten wegen ihrer hohen Sensibilität hinzuweisen. Es wurde verdeutlicht, dass jederzeit darauf zu achten ist, dass ein angemessener Schutz sichergestellt sein muss, damit keine unberechtigte Kenntnisnahme dieser sensiblen Daten erfolgt. Dabei sind geeignete technische und organisatorische Maßnahmen von den verantwortlichen Krankenhäusern zu ergreifen. Der Stand der Technik, Implementierungskosten sowie Art, Umfang, Umstände und Zwecke der Verarbeitung sind zu berücksichtigen, um entsprechende Maßnahmen zu ergreifen.

Das Krankenhaus hat den Aufnahmeprozess deutlich verbessert. Die Beschäftigten wurden umfassend über den sensiblen Umgang mit Gesundheitsdaten geschult. Bei räumlichen Engpässen kann nun ein speziell für diesen Zweck freistehendes Arztzimmer

genutzt werden. Sollte dies belegt sein, wird das Aufnahmegespräch erst dann geführt, wenn es sich ohne weitere anwesende Personen durchführen lässt. Zudem wird die Nutzung von Sichtschutzwänden erprobt, die aufgrund eines Stoffbezuges die Laustärke von Gesprächen derart dämmen, dass die erforderliche Diskretion eingehalten werden kann. Bei internen Datenschutzschulungen wird anhand dieses Sachverhalts verdeutlicht, dass der Umgang mit Gesundheitsdaten auch im Klinikalltag einer besonderen Umsicht bedarf und stets situationsangemessen umzusetzen ist.

Die Organisation und die Abläufe im Krankenhaus müssen so gestaltet sein, dass unbeteiligte Dritte möglichst keine unbefugte Kenntnis von sensiblen Gesundheitsdaten erlangen können. Dazu sind auch im Klinikalltag praxistaugliche Maßnahmen zu ergreifen.

7.5 Anspruch auf eine Kopie der Patient*innenakte

Häufig benötigen Patient*innen Kopien ihrer Patient*innenakte für weitere Untersuchungen oder zu ihrer eigenen Information. Uns erreichen vermehrt Beschwerden darüber, dass diese Unterlagen von den Verantwortlichen entweder gar nicht oder nur gegen Zahlung eines Entgelts zur Verfügung gestellt werden.

Die Forderung eines Entgelts für die erste Kopie der Patient*innenakte steht im Widerspruch zu der Regelung in Art. 15 Abs. 3 Satz 1 DS-GVO. Hier ist vorgesehen, dass der Verantwortliche im Falle eines An-

trags auf Auskunft zu den bei ihm gespeicherten Daten der jeweiligen Person auch eine Kopie derselben zur Verfügung zu stellen hat.

Art. 15 Abs. 3 Satz. 2 DS-GVO sieht eine Verpflichtung zur Zahlung eines Entgelts lediglich für alle weiteren Kopien vor. Die betroffenen Praxen berufen sich dagegen auf die nationale Vorschrift des § 630g Abs. 2 Bürgerliches Gesetzbuch, der eine Entgeltpflicht für Abschriften aus der Patientenakte festlegt.

Damit besteht ein Konflikt zwischen diesen beiden Regelungen. Zwar sieht Art. 9 Abs. 2 Buchstabe h DS-GVO durchaus eine Möglichkeit vor, medizinische Sachverhalte im nationalen Recht zu regeln. Im Falle sich widersprechender Regelungen ist jedoch das europäische Recht vorrangig anzuwenden. Danach ist die erste Kopie der Patent*innenakte entgeltfrei zur Verfügung zu stellen.

Die LDI NRW konnte in den oben genannten Fällen darauf hinwirken, dass betroffenen Patient*innen eine erste Kopie ihrer Patient*innenakte unentgeltlich zur Verfügung gestellt wurde.

7.6 Geltendmachung von Auskunftsrechten zu Patient*innenakten im Krankenhaus

Immer wieder beschweren sich Patient*innen darüber, dass Ihnen Auskünfte über die Verarbeitung ihrer Daten aus Patient*innenakten von Krankenhäusern verwehrt werden.

Eine Patientin wandte sich an die LDI NRW, da ihr das Krankenhaus, indem sie stationär aufgenommen war, bestimmte Dokumente aus der Patient*innenakte vorenthielt.

Patient*innen haben neben einem Anspruch auf Einsicht in ihre Patientenakte nach § 630g Abs. 1 des Bürgerlichen Gesetzbuches auch ein Recht auf Auskunft über die Verarbeitung der sie betreffenden personenbezogenen Daten nach Art. 15 Abs. 1 DS-GVO.

Grundsätzlich können sie das Recht auf Auskunft selbst gegenüber dem Krankenhaus geltend machen. Soweit die Auskunft verweigert wird, ist es ratsam, sich zunächst an die Datenschutzbeauftragten des betroffenen Krankenhauses zu wenden. Diese sind für die Überprüfung der Einhaltung des Datenschutzes in dem Krankenhaus vor Ort zuständig und kennen sich mit den örtlichen Gegebenheiten aus. Sollte das erfolglos bleiben, können sich Betroffene mit einer Beschwerde an die LDI NRW wenden. Ihr Anliegen wird dann von uns gegenüber dem Krankenhaus weiterverfolgt. Im vorliegenden Fall wurde das Krankenhaus auf die Pflicht zur Auskunftserteilung hingewiesen. Schließlich erhielt die Patientin eine vollständige Auskunft über ihre Daten in der Patient*innenakte.

Patient*innen ist eine vollständige Auskunft über ihre im Krankenhaus verarbeiteten personenbezogenen Daten zu erteilen. Die Auskunft muss unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags zur Verfügung gestellt werden. Nur unter besonderen Umständen kann die Frist um zwei Monate verlängert werden (Art. 12 Abs. 3 Satz 2 DS-GVO).

7.7 Aufbewahrung von Patient*innenakten bei Praxisübernahme nach dem sog. „Zwei-Schrank-Modell“

Die LDI NRW erreichen häufig Anfragen zur datenschutzkonformen Aufbewahrung von Patient*innenakten im Fall einer Praxisübernahme. Hier stellt das sog. „Zwei-Schrank-Modell“ eine praktikable Lösung dar.

Aus dem Behandlungsvertrag ergibt sich gemäß § 630f Abs. 3 des Bürgerlichen Gesetzbuches (BGB) für Ärzt*innen eine vertragliche Nebenpflicht zur Aufbewahrung der Patient*innenunterlagen für die Dauer von zehn Jahren nach Abschluss der Behandlung, soweit nicht nach anderen Vorschriften andere Aufbewahrungsfristen bestehen. Diese Verpflichtung bleibt auch im Falle einer Praxisaufgabe bestehen.

Korrespondierend zu der Aufbewahrungspflicht räumt § 630g Abs. 1 BGB Patient*innen das Recht ein, innerhalb der Aufbewahrungsfrist Einsicht in ihre Patient*innenakten zu nehmen. Zwar trifft die Aufbewahrungspflicht gemäß § 630f Abs. 3 BGB vorrangig die behandelnden Ärzt*innen. Gemäß § 10 Abs. 4 der Berufsordnung für die nordrheinischen Ärzt*innen ha-

ben diese aber nach Aufgabe der Praxis ihre Aufzeichnungen und Untersuchungsbefunde aufzubewahren oder dafür Sorge zu tragen, dass sie in gehörige Obhut gegeben werden. Daraus folgt, dass Praxisnachfolger*innen die Aufzeichnungen unter Verschluss halten müssen. Sie dürfen diese nur mit ausdrücklicher Einwilligung der Patient*innen einsehen oder weitergeben.

Im Falle einer Praxisaufgabe muss einerseits eine Situation geschaffen werden, bei der die Aufbewahrungspflicht unter Beachtung der ärztlichen Schweigepflicht erfüllt wird. Andererseits muss aber auch die Möglichkeit des Zugriffs auf die Patient*innenakten, sei es zum Zwecke der Einsicht durch Patient*innen, sei es zum Zwecke der Fortführung der Behandlung durch Praxisnachfolger*innen, gewahrt bleiben. Hierzu bietet sich das sog. „Zwei-Schrank-Modell“ an. Dabei werden die Akten der Patient*innen, die bereits vor der Praxisübergabe ihr Einverständnis für eine Weiterbehandlung erklärt haben, an die Praxisnachfolger*innen in einem „1. Schrank“ übergeben. Über die übrigen Patient*innenakten im „2. Schrank“ wird vor Übergabe ein Verwahrungsvertrag zwischen Praxisverkäufer*in und Praxisübernehmer*in geschlossen. Darin verpflichten sich die Übernehmer*innen unter Androhung einer Vertragsstrafe, Patient*innenakten aus dem zweiten Schrank nur dann in den ersten Schrank zu übernehmen, wenn die Patient*innen ihr Einverständnis hierzu erteilen. Auf diese Weise wird einerseits der Inhalt der Patient*innenakten gesichert, solange Betroffene keine explizite Einwilligung zur Kenntnisnahme erteilen. Andererseits wird das Recht der Patient*innen gewahrt, unproblematisch Zugriff auf ihre Akten zu bekommen.

Eine theoretische Alternative dazu wäre eine datenschutzkonforme Aufbewahrung der Patient*innenakten durch eine*n Dritte*n an einem anderen Ort. Dies wäre im Rahmen einer Auftragsverarbeitung gemäß Art. 28 DS-GVO auch ohne Einwilligung des Betroffenen möglich.

Obige Ausführungen sind entsprechend auf elektronische Patient*innenakten übertragbar.

Das sog. „Zwei-Schrank-Modell“ stellt eine praktikable Lösung dar, Patient*innenakten sowohl unter Beachtung von Aufbewahrungsfristen und ärztlichen Schweigepflichten als auch unter Wahrung der Möglichkeit des Zugriffs auf die Patient*innenakten zu Einsichts- oder Weiterbehandlungszwecken datenschutzkonform aufzubewahren.

7.8 Speicherung von Kontoauszügen

Das Bundessozialgericht hat klargestellt, dass bei Leistungen der Grundsicherung für Arbeitsuchende Kopien von Kontoauszügen bis zu zehn Jahre lang gespeichert werden dürfen. Jobcenter haben geeignete Vorkehrungen zu treffen, um die Einsicht in die Kontoauszüge auf zulässige Zwecke zu beschränken.

Nach wie vor erreichen uns Anfragen und Beschwerden zum Umgang mit Kontoauszügen bei bedarfsabhängigen Sozialleistungen. Das Bundessozialgericht hat sich nunmehr mit der Frage befasst, wann leistungsberechtigte Personen die Löschung von Kontoauszügen verlangen können (Urteil vom 14. Mai 2020, Az. B 14 AS 7/19 R).

Bei Leistungen der Grundsicherung für Arbeitsuchende und der Sozialhilfe ist eine Anspruchsvoraussetzung, dass die antragstellende Person bedürftig ist, also ihren Lebensunterhalt nicht aus eigenen Mitteln sicherstellen kann. Hierzu muss der zuständige Leistungsträger insbesondere das Einkommen und das Vermögen prüfen. Dies erfolgt unter anderem anhand von Kontoauszügen.

Das Bundessozialgericht hatte bereits in früheren Entscheidungen konkretisiert, dass bestimmte Ausgabepositionen geschwärzt und Kontoauszüge durch den zuständigen Sozialleistungsträger auch gespeichert werden dürfen. Nun bekam das Bundessozialgericht Gelegenheit, sich zur zulässigen Speicherdauer zu positionieren.

Betroffene Personen haben nach Maßgabe des Art. 17 DS-GVO das Recht, die Löschung der sie betreffenden personenbezogenen Daten zu verlangen. Die Verarbeitungsbefugnisse der Sozialleistungsträger richten sich nach den datenschutzrechtlichen Regelungen des Zehnten Buches Sozialgesetzbuch (SGB X). § 67c Abs. 1 Satz 1 SGB X erlaubt die Speicherung, Veränderung oder Nutzung von Sozialdaten, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden gesetzlichen Aufgaben nach dem Sozialgesetzbuch erforderlich ist und für die Zwecke erfolgt, für die die Daten erhoben worden sind.

Das Bundessozialgericht weist darauf hin, dass Leistungsbewilligungen in bestimmten Fällen bis zu zehn Jahre nach Bekanntgabe des Bewilligungsbescheides – auch zu Lasten der leistungsberechtigten Personen – korrigiert werden können. Daher sei auch die Speicherung der Kontoauszüge für die Dauer dieses

Zeitraums erlaubt. Bloße Aktenvermerke über Inhalte der vorgelegten Kontoauszüge seien nach Ansicht des Bundessozialgerichtes keine in gleichem Maße geeignete Alternative.

Allerdings betont das Bundessozialgericht auch, dass die Einsicht in die gespeicherten Kontoauszüge auf zulässige Zwecke beschränkt ist. Sozialleistungsträger sind deswegen nach Art. 25 und Art. 32 DS-GVO verpflichtet, durch geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau zu gewährleisten und insbesondere die Kontoauszüge vor unbefugter Einsichtnahme zu schützen. Dies wird begleitet durch die Kontrolle durch die behördlichen Datenschutzbeauftragten und die Datenschutzaufsichtsbehörden.

Die Frage der zulässigen Speicherdauer von Kontoauszügen ist durch die Entscheidung des Bundessozialgerichtes nunmehr höchstrichterlich geklärt. Sozialleistungsträger haben zu gewährleisten, dass die Kontoauszüge nur zur Erfüllung der ihnen obliegenden gesetzlichen Aufgaben eingesehen werden.

7.9 Zustellung eines Wohngeldbescheides durch öffentliche Bekanntmachung

Die Veröffentlichung personenbezogener Daten im elektronischen Amtsblatt einer Gemeinde zum Zwecke der öffentlichen Zustellung eines Schriftstücks ist nur solange zulässig, bis der Zweck erreicht ist. Sobald das Schriftstück als zugestellt gilt, sind die personenbezogenen Daten zu löschen.

Eine betroffene Person stieß bei der Recherche ihres Namens in einer Internet-Suchmaschine auf das Amtsblatt einer großen kreisfreien Stadt, welches über die städtische Internetseite abgerufen werden konnte. Im Amtsblatt wurde die Zustellung eines Wohngeldbescheides an die betroffene Person im Wege der öffentlichen Bekanntmachung veröffentlicht. Genannt wurden der Name der betroffenen Person, eine frühere Anschrift sowie Datum und Aktenzeichen des Wohngeldbescheides.

Weil die Ausgabe des Amtsblattes bereits mehrere Monate zurücklag, wandte sich die betroffene Person an die Wohngeldstelle und verlangte die Löschung ihrer personenbezogenen Daten aus dem Amtsblatt. Diesen Antrag lehnte die Wohngeldstelle ab.

Daraufhin wandte sich die betroffene Person an uns und bat um Unterstützung. In der von uns angeforderten Stellungnahme berief sich die Wohngeldstelle darauf, dass die Veröffentlichung der personenbezogenen Daten im Amtsblatt weiterhin zulässig sei. Auch sei es zulässig, das Amtsblatt durch Internet-Suchmaschinen indexieren zu lassen.

Diese Auffassung konnte uns nicht überzeugen. § 65 Abs. 2 Zehntes Buch Sozialgesetzbuch (SGB X) verweist auf die landesrechtlichen Zustellungsvorschriften. Die Zustellung durch öffentliche Bekanntmachung richtet sich in NRW nach § 10 des Landeszustellungsgesetzes (LZG NRW). Sie ist als letztes Mittel der Bekanntgabe zulässig, wenn alle Möglichkeiten erschöpft sind, das Schriftstück dem Empfänger in anderer Weise zu übermitteln.

Nach § 10 Abs. 2 Satz 7 LZG NRW gilt das Dokument als zugestellt, wenn seit dem Tag der Bekanntmachung beziehungsweise seit der Veröffentlichung der Benachrichtigung zwei Wochen vergangen sind. In den Akten ist zu vermerken, wann und wie die Benachrichtigung bekannt gemacht wurde und wie lange ein Aushang oder die Bereitstellung im Internet angedauert hat (§ 10 Abs. 2 Satz 6 LZG NRW). Eine weitere Bereitstellung der Daten im Internet ist dann nicht mehr erforderlich und deshalb unzulässig.

Die Wohngeldstelle hielt zunächst an ihrer Auffassung fest. Nachdem wir eine Beanstandung nach § 28 Abs. 2 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) ankündigten, lenkte die Wohngeldstelle ein und machte die Daten der betroffenen Person in der digitalen Fassung des Amtsblattes unkenntlich. Zudem wurde die städtische Hauptsatzung geändert, um künftig die zeitnahe Löschung von Informationen über öffentliche Zustellungen sicherzustellen.

Zwischenzeitlich wurde in § 10 Abs. 2 Landeszustellungsgesetz klargestellt, dass Benachrichtigungen über die öffentliche Zustellung nur noch online und nicht mehr in der Papierfassung des Amtsblattes erfolgen dürfen, weil eine Löschung personenbezogener Daten in der gedruckten Version nicht möglich ist.

Die Bekanntgabe personenbezogener Daten im elektronischen Amtsblatt zu öffentlichen Zustellungen beeinträchtigt das Recht auf Schutz personenbezogener Daten. Sie ist erst dann gestattet, wenn keine andere Möglichkeit besteht, ein Schriftstück dem Empfänger zu übermitteln. Bei Außenstehenden kann die öffentliche Zustellung den Eindruck erwecken, der Adressat sei pflichtvergessen, unzuverlässig oder wolle sich durch „Untertauchen“ dem Zugriff der öffentlichen Verwaltung entziehen. Daher ist die Veröffentlichung strikt auf die Frist von zwei Wochen bis zum Eintritt der Zustellungsfiktion zu begrenzen.

8. Videoüberwachung

Veröffentlichungen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)

Die Datenschutzkonferenz (DSK) hat am 3. September 2020 eine neue „Orientierungshilfe zur Videoüberwachung durch nicht-öffentliche Stellen“ veröffentlicht.

Die bisherige Orientierungshilfe wurde grundlegend überarbeitet und an die Datenschutz-Grundverordnung angepasst. Dabei wurden die Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte des Europäischen Datenschutzausschusses, Version 2.0, angenommen am 29. Januar 2020, berücksichtigt. Neu hinzugekommen sind die Abschnitte zur Überwachung in der Nachbarschaft und zur datenschutzrechtlichen Bewertung von Tür- und Klingelkameras, Drohnen und Wildkameras sowie Dashcams.

Mit der Orientierungshilfe erhalten Betroffene und Verantwortliche Informationen über die datenschutzrechtlichen Voraussetzungen der Videoüberwachung in unterschiedlichen Lebensbereichen. Im Anhang finden sich Muster-Hinweisschilder, die es den Verantwortlichen erleichtern, den Transparenzpflichten gemäß Art. 12 ff. DS-GVO nachzukommen. Darüber hinaus wird eine Checkliste mit den wichtigsten Prüfungspunkten im Vorfeld einer Videoüberwachung bereitgestellt.

Bereits im Jahr 2019 hatte die DSK folgende Orientierungshilfen und Positionspapiere zu speziellen Themen der Videoüberwachung durch nicht-öffentliche Stellen veröffentlicht:

- Orientierungshilfe der Datenschutzaufsichtsbehörden zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen – Stand: 22. Februar 2019
- Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams) – Stand: 28. Januar 2019
- Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen – Stand: 16. Januar 2019
- Orientierungshilfe zur Videoüberwachung in Schwimmbädern – Stand: 8. Januar 2019

Damit hat die DSK wesentliche Themenbereiche an die Datenschutz-Grundverordnung angepasst.

9. Datenschutz am Arbeitsplatz

9.1 Datenschutzüberprüfung von Personaldienstleistern und Leiharbeitsunternehmen

Im 25. Bericht haben wir unter 6.3 auf die Prüfung des Beschäftigtendatenschutzes bei Personaldienstleistungs- und Leiharbeitsunternehmen hingewiesen. Die Auswahl der Unternehmen für die Initiativkontrolle wurde so gewählt, dass eine möglichst breite Abdeckung der Branche erfolgte. Daher wurden große Unternehmen und solche aus besonderen Sparten mit Sitz in NRW ausgewählt.

Im Fokus der Prüfung standen Fragen nach dem Rollenverständnis der geprüften Unternehmen im Hinblick auf ihre datenschutzrechtliche Verantwortlichkeit gegenüber Bewerber*innen und Beschäftigten, der Wahrung von Informations- und Auskunftspflichten gegenüber diesen Personen, dem Zweck und Umfang der Datenerhebung mittels Bewerbungsfragebögen, der Übermittlung von Daten von Bewerber*innen und Beschäftigten an interessierte Arbeitgeber*innen oder Entleiher*innen sowie die Löschung dieser Daten.

Arbeitssuchende wenden sich an Personaldienstleistungs- und Leiharbeitsunternehmen bzw. Verleiher*innen, um dauerhaft oder befristet in ein Arbeitsverhältnis vermittelt zu werden. Hierzu übermitteln sie ihre Bewerbungsunterlagen mit personenbezogenen Daten, wie Daten zur Person, zur Qualifikation, zur gewünschten Tätigkeit und Gehaltsvorstellung. Erhoben werden mitunter aber auch Daten zur gesundheitlichen Eignung für eine bestimmte Tätigkeit. Diese Daten werden an interessierte Arbeitgeber*innen und

Entleiher*innen weitergegeben. Bei Interesse wird der Kontakt mit der arbeitssuchenden Person hergestellt.

1. Gemäß § 1 Abs. 1 Satz 2 Arbeitnehmerüberlassungsgesetz (AÜG) werden Arbeitnehmer*innen zur Arbeitsleistung überlassen, wenn sie in die Arbeitsorganisation der Entleiher*innen eingegliedert sind und deren Weisungen unterliegen. Voraussetzung hierfür ist das Bestehen eines Arbeitsverhältnisses zwischen Leiharbeitnehmer*in und Verleiher*in. Leiharbeitnehmer*innen sind gemäß § 26 Abs. 8 Nr. 1 Bundesdatenschutzgesetz (BDSG) wie „Beschäftige“ zu sehen und sowohl Verleiher*in als auch Entleiher*in sind als Arbeitgeber*in gemäß Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) „Verantwortliche“. Dessen waren sich alle befragten Unternehmen bewusst. Ebenso war ihnen klar, dass Verleiher*in und Entleiher*in jeweils selbständig die Zwecke und Mittel der Datenverarbeitung festlegen. Mit den Zwecken ist das „Warum“ der Verarbeitung gemeint, während Mittel das „Wie“ der Verarbeitung betrifft. Ein Auftragsverarbeitungsverhältnis besteht nicht.

   Die beteiligten Unternehmen können unter bestimmten Umständen gemeinsam Verantwortliche sein. Art. 26 DS-GVO regelt, dass zwei oder mehr Verantwortliche, die gemeinsam die Zwecke und Mittel der Verarbeitung festlegen, gemeinsam Verantwortliche sind. Sie legen in einer Vereinbarung fest, wer welche datenschutzrechtlichen Pflichten erfüllt. Diese Vereinbarung ist keine Rechtsgrundlage für die Datenverarbeitung, sondern regelt lediglich, wer die datenschutzrechtlichen Pflichten der Parteien erfüllt.

   Die gesetzlichen Anforderungen an die Vereinbarung sind überschaubar. Art. 26 DS-GVO verlangt, dass die Verantwortlichen in transparenter Form in einer

Vereinbarung festlegen, wer von ihnen welche Verpflichtung gemäß der DS-GVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person betrifft, und wer welchen Informationspflichten gemäß Art. 13 und 14 DS-GVO nachkommt. In einer solchen Vereinbarung kann auch eine Anlaufstelle für die betroffene Person angegeben werden.

Keines der befragten Leiharbeitsunternehmen hat eine Vereinbarung im vorgenannten Sinn abgeschlossen, da die Voraussetzung einer gemeinsamen Verantwortung mit dem jeweiligen Entleiher nicht vorlag. Nur vereinzelt wurde die Möglichkeit eines solchen Vertrages gesehen und vorsorglich ein Mustervertrag erstellt.

2. Personaldienstleistungs- und Leiharbeitsunternehmen erheben mittels Bewerbungsfragebogen eine Vielzahl von personenbezogenen Daten bei den Bewerber*innen auf der Basis einer Einwilligung. Dies erfolgte entweder online über die Homepage des Unternehmens oder per E-Mail oder Post. Die Bewerber*innen wurden in allen Unternehmen über die genannten Kommunikationswege über die Datenverarbeitung, ihre Informationsrechte nach Art. 13, 14 DS-GVO, ihr Auskunftsrecht nach Art. 15 DS-GVO und auch das Recht auf Datenlöschung gemäß Art. 17 DS-GVO unterrichtet. Alle Unternehmen verfügten über externe, mitunter auch interne betriebliche Datenschutzbeauftragte. Wünschenswert, wenn auch nicht verpflichtend, wäre die Unterrichtungen der Betroffenen, an welche Stelle sie ihr Anliegen richten könnten. In der Regel waren hier die Datenschutzbeauftragten der verantwortlichen Stellen genannt. Unternehmen, die hierzu keine weiteren Angaben machten, werden wir auf diese Option hinweisen.

Die Verpflichtung, im Rahmen von Auskunftsersuchen nach Art. 15 DS-GVO auch Kopien an die betroffenen Personen herauszugeben, wurde durchgehend gesehen und auch im Hinblick auf Leistungsdaten bejaht, sofern kein Geheimhaltungsinteresse entgegenstand (Urteil des Landesarbeitsgerichts Baden-Württemberg vom 20. Dezember 2018, Az. 17 Sa 11/18).

Bei den Bewerbungsfragebögen wurden die Zwecke der Datenerhebung sämtlich erläutert. Zum Teil fehlten Hinweise auf die Freiwilligkeit der Datenerhebung, etwa bei der Schwerbehinderteneigenschaft. Oder es war nicht kenntlich gemacht, dass eine Datenerhebung nur dann erforderlich war, wenn die Information Einfluss auf die Eingehung bzw. Durchführung des Arbeitsverhältnisses haben würde, zum Beispiel bei Erkrankungen oder Behinderungen. Ein weiteres Beispiel hierfür waren Angaben zur Aufenthalts- und Arbeitserlaubnis. Diese sind im Rahmen der Prüfung der gesetzlichen Vorgaben des AÜG nur bei Nicht-EU-Ausländern erforderlich. Die LDI NRW hat den betroffenen Personaldienstleistungs- und Leiharbeitsunternehmen im Hinblick auf die Datenerhebung mittels Bewerbungsfragebogen entsprechende Hinweise gegeben.

3. Die Datenübermittlung an interessierte Arbeitgeber*innen und Entleiher*innen erfolgte in der Regel nur im Hinblick auf die erforderlichen Daten, wie Namen, Vornamen und Qualifikation. Zum Teil wurden nur anonymisierte Bewerbungsdaten oder Profile weitergegeben. Die Information über die Empfänger*innen der Daten verlief sehr unterschiedlich. Überwiegend wurde entsprechend Art. 13 Abs. 1 Buchstabe e DS-GVO nur über die Kategorien von Empfänger*innen

der personenbezogenen Daten, zum Beispiel Branchen, nicht aber die konkreten Unternehmen selbst unterrichtet. Dies ist nur dann hinnehmbar, wenn die Zahl der Empfänger sehr groß oder nur schwer recherchierbar ist oder ein berechtigtes Geheimhaltungsinteresse der Preisgabe konkreter Empfänger entgegensteht.

Im Falle eines Interesses an einer Beschäftigung auf Seiten eines Unternehmens wurden Bewerber*innen hierüber konkret unterrichtet und gezielt darauf angesprochen, ob sie eine weitere Kommunikation oder Kontaktaufnahme mit diesem Unternehmen wünschten.

4. Bei der Datenlöschung zeigte sich, dass die zulässige Frist von sechs Monaten zur Löschung bei abgelehnten Bewerber*innen eingehalten wurde. Allerdings bestand für die Bewerber*innen häufig auch die Möglichkeit, sich freiwillig bei dem Personaldienstleistungs- oder Leiharbeitsunternehmen in einen sog. Bewerbungspool für etwaige weitere Vermittlungsangebote aufnehmen zu lassen. Personaldienstleistungs- und Leiharbeitsunternehmen fragten bei den betroffenen Personen in Abständen von mehreren Wochen oder Monaten nach, ob auch weiterhin Interesse an einer Vermittlung bestehen würde. In der Regel wurden die Bewerbungsdaten bei fehlendem Interesse nach zwölf Monaten gelöscht.

   Vereinzelt wurden die Daten bis zu zwei Jahre bzw. bis auf Widerruf gespeichert. Zwar enthält die DS-GVO keine spezifische Frist für die Gültigkeit einer Einwilligung. Wie lange eine Einwilligung gültig ist, hängt aber von den Umständen ab, besonders vom Kontext, dem Umfang der ursprünglichen Einwilligung

und den Erwartungen der betroffenen Person. Jedenfalls dürfte eine Vermittlungsmöglichkeit von Kandidat*innen nach Ablauf mehrerer Jahre nicht mehr bestehen, so dass es an der Erforderlichkeit der weiteren Datenspeicherung fehlte. Die betroffenen Unternehmen sind hierüber unterrichtet worden. Allgemein ist zu empfehlen, den Bewerber*innen bereits zum Zeitpunkt der Einwilligung in die Speicherung ihrer Bewerbungsdaten in einem Bewerbungspool die Möglichkeit einzuräumen, hierzu bestimmte Zeitfenster, etwa durch Setzen eines Häkchens unter der Erklärung zu bestimmen. Fehlt ein solches Zeitfenster, sollten Personaldienstleister und Leiharbeitsunternehmen nach dem letzten erfolglosen Kontaktversuch mit Bewerber*innen eine konkrete und kurz bemessene Endfrist zur Datenlöschung setzen und diese hierüber unterrichten.

Insgesamt erbrachte die Prüfung der ausgewählten Personaldienstleistungs- und Leiharbeitsunternehmen ein ausgesprochen positives Ergebnis im Hinblick auf das Verständnis von Rollen und Verantwortlichkeiten nach der DS-GVO. Entsprechendes gilt auch in Bezug auf die Implementierung von datenschutzrechtlich erforderlichen und gebotenen Abläufen im Rahmen der Personalvermittlung und -überlassung an Dritte.

Soweit zu bestehenden Prozessen der Erhebung und Speicherung von Bewerbungsdaten Optimierungsbedarf festgestellt wurde, werden wir die betroffenen Unternehmen hierüber unterrichten und entsprechend beraten.

9.2 Videointerviews im Einstellungsverfahren

Videointerviews ohne Aufzeichnung können in Bewerbungsverfahren zulässig sein, sofern sie für den Abschluss eines Beschäftigungsverhältnisses erforderlich sind oder auf der Basis einer freiwilligen Einwilligung der Bewerber*innen durchgeführt werden.

Im Rahmen einer Beratungsanfrage hat die LDI NRW die Zulässigkeit des Videointerviews im Einstellungsverfahren geprüft. Es war vorgesehen, dass Bewerber*innen vor Vereinbarung des Interviewtermins über Alternativen, wie ein Gespräch vor Ort oder ein Telefonat, aufgeklärt werden und Datenschutzhinweise und Informationen zu den technischen Voraussetzungen erhalten. Zudem sollten die Bewerber*innen über den Verwendungszweck der Daten informiert werden. Es sollten auch keine Gesprächsinhalte aufgezeichnet werden. Sollten die Bewerber*innen über keinen Internetanschluss verfügen oder die Durchführung von Videointerviews ablehnen, sollten auch weiterhin andere Alternativen, zum Beispiel persönliche Interviews, zum Einsatz kommen. Es wurde mitgeteilt, dass keine Übermittlung von Gesprächsinhalten und personenbezogenen Daten in die USA stattfinden, da die Daten auf deutschen Servern verarbeitet werden.

Nach § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) ist das Verarbeiten von Beschäftigtendaten durch Arbeitgeber*innen zulässig, wenn es für die Entscheidung über die Begründung des Beschäftigungsverhältnisses erforderlich ist.

Ein Bewerbungsgespräch ist ein geeignetes Instrument für Arbeitgeber*innen, die richtige Person für die

zu besetzende Stelle herauszufinden. Gerade bei einer großen Zahl von Bewerbern*innen war es aufgrund der Pandemie nicht möglich, alle in Betracht kommenden Personen zu einem persönlichen Gespräch einzuladen. Aber auch wenn Bewerber*innen aus weiter Distanz anreisen müssen, kann eine digitale Lösung im beiderseitigen Interesse liegen. Für potentielle Bewerber*innen kann ein Videointerview eine einfache, erste Möglichkeit sein, die schriftlich erfolgte Bewerbung ohne großen Aufwand zu vertiefen. Dies könnte dazu führen, dass mehr Bewerber*innen die Möglichkeit haben, sich persönlich darzustellen und Arbeitgeber*innen dadurch eine qualifiziertere Auswahlentscheidung treffen können.

Die LDI NRW betrachtet es daher im Interesse beider Beteiligter als eine datenschutzrechtlich zulässige Lösung, wenn sich Arbeitgeber*innen mittels des Videointerviews einen persönlichen Eindruck von einem*r Bewerber*in verschaffen können und ihre Entscheidung nicht nur anhand von Bewerbungsunterlagen treffen.

Da keine Aufzeichnungen erfolgen, werden auch nicht mehr oder andere Daten erhoben als bei einem persönlichen Gespräch. Arbeitgeber*innen haben hierbei stets zu berücksichtigen, ob Bewerber*innen über die technischen Möglichkeiten für die Teilnahme an einem Videointerview verfügen.

Im Übrigen greift auch immer die Rechtsgrundlage der Einwilligung der Bewerber*innen gemäß § 26 Abs. 2 BDSG, sofern deren strengere Anforderungen vorliegen. Hierbei muss es sich um eine transparente und informierte Einwilligung handeln und es muss eine echte und glaubhafte Alternative angeboten werden, etwa ein herkömmliches Auswahlverfahren

durch einen persönlichen Vorstellungstermin (siehe hierzu auch 23. Bericht unter 9.1.2). Die Interessenlage zwischen Arbeitgeber*innen und Bewerber*innen sollte gleichgelagert sein und Arbeitgeber*innen sollten eine verbindliche, schriftliche Festlegung darüber treffen, dass bei einer Nichtteilnahme an dem Videointerview keine Nachteile drohen.

Zu beachten ist auch die Perspektive der Mitarbeiter*innen der oder des Verantwortlichen, die bzw. der Videointerviews im Bewerbungsverfahren einsetzen will. Denn auch hier gilt, dass aufgrund des strukturellen Ungleichgewichts zwischen Arbeitgeber*innen und Arbeitnehmer*innen zumeist nicht von einer Freiwilligkeit der Einwilligung ausgegangen werden kann. Arbeitgeber*innen sind im Übrigen auch gegenüber ihren Mitarbeitern*innen, die das Videointerview durchführen müssen, für die Datensicherheit verantwortlich.

Eine Information der Mitarbeiter*innen und Bewerber*innen über die Rahmenbedingungen der Videointerviews hielten wir im Hinblick auf die Anforderungen des Art. 13 DS-GVO für notwendig. Insgesamt gesehen bewerteten wir die geplante Durchführung von Videointerviews für Bewerbungen unter den beschrieben Voraussetzungen als datenschutzrechtlich zulässig.

Videointerviews im Einstellungsverfahren können eine datenschutzrechtlich zulässige Alternative darstellen. Wichtig ist, dass keine Aufzeichnungen stattfinden und sowohl die Bewerber*innen als auch die Mitarbeiter*innen, die für das Videointerview zuständig sind, hinreichend gem. Art. 13 DS-GVO informiert werden. Der Einsatz von Videointerviews im Einstellungsverfahren lässt sich grundsätzlich auf § 26 Abs.1 S. 1 BDSG stützen. Arbeitgeber*innen haben hierbei stets zu berücksichtigen, ob Bewerber*innen über die technischen Möglichkeiten für die Teilnahme an einem Videointerview verfügen. Alternativ kommt als Rechtsgrundlage auch eine Einwilligung nach § 26 Abs. 2 BDSG in Betracht. Mit Blick auf die Freiwilligkeit sollte bei dieser Variante stets eine Alternative zum Videointerview angeboten werden, zum Beispiel Vorstellungsgespräch, Assessment-Center, psychologischer Test. Empfehlenswert ist, dass das Videointerview in der eigenen Infrastruktur des Unternehmens abläuft.

9.3 Schadenersatz und Benachrichtigungspflicht bei Versand einer E-Mail mit Bewerbungsdaten an falsche Empfänger*innen

Nach einer Entscheidung des Landgerichts Darmstadt (LG Darmstadt) kann der Versand einer E-Mail mit Bewerbungsdaten an einen falschen Empfänger zu einem Anspruch auf Schadenersatz nach Art. 82 DS-GVO führen. Zudem kann für Verantwortliche eine Pflicht nach Art. 34 DS-GVO entstehen, die betroffene Person unverzüglich von der Verletzung des Schutzes ihrer personenbezogenen Daten zu benachrichtigen (Urteil vom 26. Mai 2020, Az. 13 O 244/19).

Der Kläger hatte sich bei dem Verantwortlichen beworben. Der Verantwortliche wollte dem Bewerber eine Nachricht zusenden, aus welcher sich unter anderem Rückschlüsse auf dessen Gehaltsvorstellungen ergaben. Die Nachricht wurde jedoch versehentlich nicht an den Bewerber, sondern an eine dritte Person versendet.

Aus Sicht des Gerichts bestand durch die Versendung der Nachricht an unbeteiligte Dritte nicht nur eine hohe Wahrscheinlichkeit eines Schadenseintritts, vielmehr sei dadurch ein Schaden bereits eingetreten.

Infolge der Weitersendung an eine unbeteiligte dritte Person habe der Kläger die Kontrolle darüber verloren, wer Kenntnis von den Informationen hat. Zu diesen Informationen gehörte der Umstand, dass der Kläger sich bei dem Verantwortlichen beworben hatte. Darüber hinaus habe eine dritte Person Kenntnis über den Bewerbungsvorgang und finanzielle Hintergründe bzw. Vertragsverhandlungen erlangt. Diese

Informationen seien dazu geeignet, den Kläger zu benachteiligen, wenn sie an etwaige Konkurrenten*innen für einen Arbeitsplatz gelangten. Ebenso könne der Ruf bzw. das Ansehen bzw. das weitere berufliche Fortkommen des Klägers geschädigt werden, wenn etwa dessen aktueller Arbeitgeber von der Bewerbung auf eine anderweitige Arbeitsstelle erfahren würde. Das Gericht sah daher einen immateriellen Schaden und einen Anspruch auf Schadenersatz gegeben, ohne dass vom Kläger konkrete Nachteile vorgetragen worden waren.

Der Verantwortliche habe zudem auch gegen die Pflicht zur unverzüglichen Benachrichtigung der betroffenen Person gemäß Art. 34 DS-GVO verstoßen. Eine solche Benachrichtigung hat zu erfolgen, wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Aus Sicht des Gerichts besteht ein hohes Risiko dann, wenn zu erwarten ist, dass bei ungehindertem Geschehensablauf mit hoher Wahrscheinlichkeit ein Schaden für die Rechte und Freiheiten der Betroffenen eintritt. In einem solchen Fall sei es nicht maßgeblich, ob die Datenschutzverletzung auch zu einem besonders hohen Schadensumfang führt. Da ein hohes Risiko bestanden habe, hätte der Betroffene unverzüglich benachrichtigt werden müssen, das heißt ohne schuldhaftes Zögern. Da der Verantwortliche den Bewerber jedoch erst mehrere Wochen nach Kenntniserlangung benachrichtigt habe, sei die Pflicht aus Art. 34 DS-GVO verletzt worden.

Beim Versand von E-Mails oder sonstigen Nachrichten kommt es immer wieder vor, dass diese versehentlich an falsche Empfänger gerichtet werden. Ähnlich gelagert sind Fälle mit offenem Empfängerkreis. Gelangen aufgrund solcher Versehen personenbezogene Daten an unberechtigte Empfänger, so liegt eine unzulässige Verarbeitung und eine Verletzung des Schutzes dieser personenbezogenen Daten vor. Hat diese Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen zur Folge, so sind diese unverzüglich zu benachrichtigen. Aus Sicht des LG Darmstadt tritt dann bereits durch die Versendung einer Nachricht an unbeteiligte Dritte ein Schaden ein. Bei der Beurteilung des voraussichtlichen Risikos spielt nicht allein der Kreis der Empfänger eine Rolle, sondern vor allem auch die Sensibilität der übermittelten Inhalte.

9.4 Unzulässige Verwendung beruflich zugänglicher Daten zur privaten Kontaktaufnahme

Eigentlich eine Selbstverständlichkeit: Kontaktdaten, auf die eine Person aus beruflichen Gründen Zugriff hat – etwa im Zusammenhang mit einem ärztlichen Behandlungsverhältnis oder anhand von Bewerbungsunterlagen – dürfen ohne Einwilligung der betroffenen Person nicht für eine private Kontaktaufnahme genutzt werden. Doch leider kommt es immer wieder zur missbräuchlichen Verwendung solcher Daten für nicht zulässige Zwecke.

Der LDI NRW lagen mehrere Eingaben zur Nutzung von Kontaktdaten vor, die in beruflichem Zusammenhang erlangt, jedoch für private Zwecke verwendet wurden.

In einem Fall hatte die betroffene Person eine Klinik für eine medizinische Behandlung aufgesucht. Insoweit lagen der Klinik unter anderem der Vor- und Nachname der betroffenen Person vor. Die zuständigen Ärzt*innen der Klinik hatten somit aufgrund des Behandlungsverhältnisses Kenntnis von diesen Informationen. Eine dieser Person hat den Vor- und Nachnamen sodann genutzt, um die betroffene Person später im Sozialen Netzwerk Facebook zu suchen und auf privater Ebene zu kontaktieren.

In einem anderen Fall hatte die betroffene Person sich auf eine Arbeitsstelle beworben. Aus den Bewerbungsunterlagen ergab sich auch die private Mobilfunknummer. Es fand ein persönliches Vorstellungsgespräch statt; ein Beschäftigungsverhältnis ergab sich jedoch nicht. Eine Person, die bei dem potenziellen Arbeitgeber Zugriff auf die Bewerbungsunterlagen

hatte, nutzte später die private Mobilfunknummer der betroffenen Person für eine Kontaktaufnahme über den Messenger WhatsApp. Auch diese Kontaktaufnahme geschah aus privater Motivation heraus.

Eine Kontaktaufnahme über Soziale Netzwerke oder Messenger unter Nutzung des Namens oder der Mobilfunknummer stellt eine automatisierte Verarbeitung dieser personenbezogenen Daten dar. Eine solche Verarbeitung ist nur zulässig, wenn hierfür eine Rechtsgrundlage vorliegt.

Eine Einwilligung der betroffenen Person lag in beiden Fällen nicht vor. Da die Datenverarbeitung zu privaten Zwecken erfolgt war, diente sie auch nicht der Erfüllung oder Anbahnung eines Vertrages im Zusammenhang mit dem ärztlichen Behandlungsverhältnis bzw. dem Bewerbungsverhältnis.

Es ist auch kein berechtigtes Interesse erkennbar, die im beruflichen Zusammenhang zugänglich gemachten Daten für private Zwecke zu nutzen. Weiterhin müssen weder Patient*innen noch Bewerber*innen mit einer solchen Datenverarbeitung rechnen. Patient*innen erwarten, dass die Vertraulichkeit aller Informationen gewahrt wird, die im Zusammenhang mit der Behandlung bekanntgemacht werden. Ebenso erwarten Bewerber*innen, dass potenzielle Arbeitgeber*innen bzw. die dort tätigen Personen die erlangten Daten nur zu Zwecken des Bewerbungsverhältnisses verwenden. Daher überwiegt das entgegenstehende Interesse der betroffenen Personen, dass derartige Informationen nicht für Zwecke außerhalb des ärztlichen Behandlungsverhältnisses bzw. des Bewerbungsverhältnisses verwendet werden.

In beiden Fällen wurde in Anbetracht der Gesamtumstände eine Verwarnung ausgesprochen. Diese richtete sich gegen die jeweils handelnde natürliche Person, die in diesen Fällen als datenschutzrechtlich Verantwortlicher einzuordnen war. Da die jeweiligen Daten nur zu beruflichen Zwecken hätten verarbeitet werden dürfen, lag die Nutzung zu rein privaten Zwecken nicht im Bereich der dienstlichen Befugnisse. Diese Datenverarbeitung war daher nicht dem jeweiligen Arbeitgeber zuzurechnen. Vielmehr haben die natürlichen Personen über die Zwecke und Mittel der Datenverarbeitung bestimmt und waren daher selbst Verantwortliche.

Es lag auch keine Ausnahme vom Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) vor. Diese findet zwar gemäß ihres Art. 2 Abs. 2 Buchstabe c keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Dies soll nach Erwägungsgrund 18 Satz 1 DS-GVO der Fall sein, wenn die Verarbeitung ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird (siehe dazu auch 25. Bericht unter 4.7). Hier wurden jedoch jeweils Daten genutzt, die den handelnden Personen gerade aufgrund ihrer beruflichen Tätigkeit bekanntgeworden bzw. verfügbar waren. Die Verwendung der Daten war daher zwar privat motiviert, stand aber zugleich in einem Bezug zur beruflichen Tätigkeit.

Personenbezogene Daten dürfen nur bei Vorliegen einer Rechtsgrundlage und nur für legitime Zwecke verarbeitet werden. Hat eine Person im beruflichen Kontext Zugriff auf personenbezogene Daten, so dürfen diese grundsätzlich auch nur für berufliche Zwecke und im Rahmen des Erforderlichen genutzt werden. Eine Nutzung von beruflich erlangten Informationen zur privaten Kontaktaufnahme ist daher – sofern keine wirksame Einwilligung der betroffenen Person vorliegt – nicht zulässig. Da sich die Zugriffsmöglichkeit auf die Daten gerade aus der beruflichen Tätigkeit ergibt, erfolgt eine Verarbeitung solcher Daten zugleich nicht zur Ausübung ausschließlich persönlicher Tätigkeiten, sondern unterliegt den datenschutzrechtlichen Vorgaben.

9.5 Aufbewahrungsfristen für Stammdaten von Beschäftigten mit Zugang zum Sicherheitsbereich eines Flughafens

Die Speicherung der Stammdaten in Bezug auf Tagesausweissysteme zur Regelung des Zutritts zu sicherheitsrelevanten Bereichen, wie Flughäfen, ist gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO zulässig. Die Aufbewahrungsfrist ist auf zehn Jahre zu begrenzen.

Im Rahmen einer Beschwerde hat die LDI NRW die Zulässigkeit der unbegrenzten Speicherung von Stammdaten von Personal, das Zugang zum Sicherheitsbereich eines Flughafens benötigt, im Tagesausweissystem eines Flughafenbetreibers geprüft. Hintergrund ist, dass die Berechtigung hierzu nach § 10 Luftsicherheitsgesetz (LuftSiG) nicht erteilt bzw. widerrufen wird, wenn Antragssteller*innen für einen Flughafenausweis nicht mehr als zuverlässig gelten.

In diesen Fällen darf der betroffenen Person auch nach Ablauf der gesetzlichen Löschfristen gemäß § 7 Abs. 11 Nr. 1 Buchstabe b bzw. Nr. 2 Buchstabe b LuftSiG der Zugang zum Sicherheitsbereich des Flughafens mit Tagesausweis verwehrt werden. Hierfür ist es erforderlich, dass der Flughafenbetreiber auf die Stammdaten der Betroffenen zurückgreifen kann.

In diesem Zusammenhang war die Frage der Erforderlichkeit und Zulässigkeit der Speicherung von Stammdaten (Vorname, Familienname, vorheriger Name, Geburtsdatum) von Personen zu prüfen, deren Zugangsberechtigung aufgrund von Ablehnung oder Widerruf einer Zuverlässigkeitsüberprüfung (ZÜP) nicht erteilt wurde bzw. erloschen ist.

Die LDI NRW hat hierbei die Belange der Luftsicherheit anerkannt, allerdings auf die fehlende Rechtsgrundlage für eine weitergehende Speicherung der Stammdaten hingewiesen.

Die Speicherung der Stammdaten in Bezug auf das Tagesausweissystem ist grundsätzlich gemäß Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO zulässig. Allerdings kann damit keine Speicherung auf unbestimmte Zeit begründet werden. Die Aufbewahrungsfrist wurde nach Rücksprache mit dem Ministerium für Verkehr des Landes NRW auf zehn Jahre festgelegt. Bezüglich der Rechtsgrundlage für die Speicherung der Stammdaten der Personen, denen die Berechtigung nach § 10 LuftSiG nicht erteilt bzw. widerrufen wurde, wurde von der Luftsicherheitsbehörde mitgeteilt, dass das Bundesministerium des Innern die Problematik mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erörtern und einen gesetzgeberischen Regelungsbedarf prüfen

werde. Zudem wurde der Flughafenbetreiber angewiesen, sein Lösch- und Berechtigungskonzept anzupassen und die damit verbundenen Prozesse zu implementieren.

In sicherheitsrelevanten Bereichen bedarf es einer strengen Zutrittskontrolle für Beschäftigte und Dritte. Zu diesem Zweck ist die Speicherung von personenbezogenen Stammdaten in Ausweissystemen zulässig. Allerdings darf die Datenspeicherung nicht unbefristet erfolgen. Mit der Kontrolle der Datenspeicherung im Bereich der Flugsicherheit konnte erreicht werden, dass über den Einzelfall hinaus ein gesetzlicher Regelungsbedarf für eine derartige Datenspeicherung geprüft wird.

10. Wirtschaft

10.1 Veröffentlichungen

- **Veröffentlichungen der LDI NRW**
  - Personenverwechslungen im Rahmen von Forderungsbeitreibungen
  - Datenverarbeitung in Inkassounternehmen - Antworten auf häufig gestellte Fragen

- **Veröffentlichungen der Datenschutzkonferenz**

  Anforderungen an die Akkreditierung von Zertifizierungsstellen

  Die Datenschutzkonferenz hat die Vorgaben der DIN EN ISO/IEC 17065 zur Akkreditierung von Zertifizierungsstellen aufgrund von Art. 43 DS-GVO ergänzt. Diese Anforderungen wurden vom Europäischen Datenschutzausschuss gebilligt. Dies schafft Rechtssicherheit und Transparenz für die interessierten Stellen und deren potenzielle (End-)Kund*innen. Die Anforderungen zur Akkreditierung gemäß Art. 43 Abs. 3 DS-GVO in Verbindung mit DIN EN ISO/IEC 17065 Version 1.4 vom 8. Oktober 2020 sind auf der Homepage der Datenschutzkonferenz www.datenschutz-konferenz-online.de abrufbar.

- **Veröffentlichungen des Europäischen Datenschutzausschusses**

  EDSA-Leitlinien 7/2020 zu den Begriffen Verantwortlicher und Auftragsverarbeiter

  Die Leitlinien des Europäischen Datenschutzausschusses (EDSA) erläutern anhand von Beispielen,

wann ein Auftragsverhältnis gemäß Art. 28 Datenschutz-Grundverordnung (DS-GVO) vorliegt, welche Rechte und Pflichten die Beteiligten hierbei zu beachten haben und wie die Auftragsverarbeitung von der gemeinsamen Verantwortlichkeit gemäß Art. 26 DS-GVO abzugrenzen ist. Die Leitlinien „Guidelines 07/2020 on the concepts of controller and processor in the GDPR“ sind bislang nur in englischer Sprache auf der Homepage des EDSA www.edpb.europa.eu abrufbar.

10.2 Datenschutzüberprüfung von Versicherungsunternehmen und Kreditinstituten

Um sich einen umfassenden Überblick zur Umsetzung des europäischen Datenschutzrechts zu verschaffen, wurde eine zufällige Auswahl von Versicherungen und Kreditinstituten überprüft.

Im Laufe des Berichtsjahres wollten wir prüfen, wie Unternehmen verschiedener Wirtschaftsbereiche die neue DS-GVO umgesetzt haben. Die Auswahl der Unternehmen erfolgte rein zufällig. Jedes Unternehmen erhielt einen umfassenden Fragebogen mit unterschiedlichen Fragengruppen. Der Fragebogen ist im Anhang abgedruckt.

Bereich Versicherungen

Die Ergebnisse der Auswertung fielen insgesamt sehr erfreulich aus. Alle ausgewählten Versicherungsunternehmen praktizieren „Datenschutz“ verantwortungsvoll in der gesamten Organisation des Unternehmens und sind gut strukturiert. Die Anforderungen der neuen DS-GVO – insbesondere im Bereich Beschwerdemanagement – wurden nahezu vollständig umgesetzt. Eine interne Überprüfung durch die Revision fand teilweise auch statt. Darüber hinaus werden bestehende Prozesse laufend beobachtet und optimiert, um weitere Verbesserungen der wesentlichen Datenverarbeitungsvorgänge zu erreichen. Besonders positiv fiel auf, dass die Belegschaft durch Schulungen, Informationsmaterial, regelmäßige Besprechungen etc. für den Umgang mit personenbezogenen Daten hinreichend sensibilisiert wurde. Im Hinblick auf den Datenschutz insgesamt ein sehr erfreuliches Bild.

Bereich Kreditinstitute

Auch bei den Kreditinstituten verdeutlicht die Querschnittsprüfung den verantwortungsvollen Umgang mit dem Datenschutz. Die von „oben gelebte“, sämtliche Bereiche einbindende Datenschutzorganisation ist mittels aussagekräftiger Organigramme anschaulich und mit gut gewählten Beispielen und Mustern nachvollziehbar dargestellt. Betriebliche Datenschutzbeauftragte berichten fortlaufend und regelmäßig dem Vorstand sowie ad hoc bei besonders bedeutsamen und relevanten Vorgängen. Die Einführung und Umsetzung der DS-GVO wurde in Projektteams begleitet und anschließend durch die Interne Revision geprüft. Verzögerungen wurden transparent und inhaltlich nachvollziehbar dargestellt und Optimierungsmaßnahmen erläutert. Als Rechtsgrundlage für Datenverarbeitungsvorgänge werden zunehmend weniger Einwilligungslösungen und stattdessen gesetzliche Rechtsgrundlagen herangezogen. Das Beschwerdemanagement ist durchweg zentralisiert. Manuelle Prozesse werden auf systemgestützte Prozesse nach und nach migriert. Der Beschwerdebegriff wird weit verstanden; ist der datenschutzrechtliche Bezug identifiziert, werden die für Datenschutzfragen zuständigen Stellen eingebunden. Die betrieblichen Datenschutzbeauftragten stehen mit diesen in einem regelmäßigen Austausch. Die Schulungen der Mitarbeiterschaft erfolgen weitgehend jährlich und werden durch weitere umfangreiche Sensibilisierungsmaßnahmen auch mittels digitaler Konzepte ergänzt. Die implementierten Richtlinien und Prozesse, die der Umsetzung und Einhaltung der DS-GVO dienen, sind gut und nachvollziehbar dargestellt.

Aus dem positiven Gesamteindruck in beiden Wirtschaftsbereichen leiten wir folgende bereichsübergreifende „Best Practices“ ab:

- Datenschutzkoordinator*innen in den Fachbereichen als Scharnierstellen zur oder zum internen Datenschutzbeauftragten.
- Teilnahme der Datenschutzbeauftragen an Vorstandssitzungen, soweit dort datenschutzrechtliche Themen vorgestellt und besprochen werden.
- Ticketbasierte Lösungen zur Bearbeitung von Betroffenenrechten.
- Einrichtung von Portalen für Kunden*innen.
- Reduzierte Eingabemasken als technisch-organisatorische Maßnahme zur Einhaltung des Grundsatzes der Datenminimierung.
- Regelmäßige Schulungen aller Mitarbeitenden einschließlich der Führungskräfte (Online-Schulungen, Präsenzschulungen, Einführungsveranstaltungen, Datenschutztage, Intranet-Informationen, Datenschutzbroschüren, Workshops, Informationsmaterial, Datenschutz-Infothek für den Außendienst).

Versicherungen und Kreditinstitute setzen die Vorschriften der DS-GVO gut um. Da es sich bei Finanzdaten um sensible Daten einer Person handelt, werden wir diese Unternehmen auch weiterhin überprüfen. Denn Datenschutz ist eine kontinuierliche Aufgabe.

10.3 Corona: Stichprobenprüfung in Unternehmen

Die Kontaktdatenerfassung nach der Coronaschutzverordnung NRW (CoronaSchVO NRW) hat in der Bevölkerung zur Sorge über die Sicherheit der eigenen Daten geführt. Daher haben wir im Laufe des Jahres 30 Gastronomie- und Friseurbetriebe in verschiedenen Regionen des Landes geprüft.

Zur Rückverfolgbarkeit möglicher Infektionsketten in Zusammenhang mit dem Coronavirus SARS-CoV-2 sieht die CoronaSchVO NRW für verschiedene Wirtschaftsbereiche eine papiergebundene Erfassung der Kontaktdaten Name, Adresse, Telefonnummer, Zeitraum des Aufenthalts bzw. Zeitpunkt von An- und Abreise vor (sog. einfache Rückverfolgbarkeit). Zusätzlich können die Verantwortlichen hierzu auch eine digitale Datenerfassung anbieten. Bei beiden Varianten sind die Kontaktdaten vier Wochen aufzubewahren und danach vollständig zu vernichten. Auch sind sie vor dem unbefugten Zugriff zu sichern. Die Übermittlung an die für die Nachverfolgung zuständige Behörde erfolgt nur auf dortiges Verlangen.

Wir haben den Unternehmen einen Fragebogen zugeschickt, in dem es insbesondere um folgende Punkte ging:

- Ausreichende Informationen im Sinne von Art. 13, 14 DS-GVO
- Datenschutzkonforme Aufbewahrung und Vernichtung der Listen nach vier Wochen
- Enge Zweckbindung zur Infektionskettennachverfolgung – und nicht etwa zur privaten Kontaktaufnahme

Das Ergebnis der Prüfung ist zufriedenstellend. Die überwiegende Zahl der geprüften Unternehmen lässt die Kontaktdatenlisten nicht offen ausliegen. Für einzelne Tische und jede Gästegruppe stehen Blankolisten zum Ausfüllen bereit, die eingesammelt und sicher aufbewahrt werden. Die regelmäßige Löschung der Daten nach vier Wochen hat sich ebenso etabliert wie die enge Zweckbindung der Kontaktdaten zur Infektionsnachverfolgung.

Ziel der Prüfung war nicht die Sanktionierung, sondern die Information der Wirtschaft, die durch die Pandemie vor besonderen Herausforderungen steht. Bereits mit dem Fragenkatalog sollte deutlich werden, was Unternehmen datenschutzrechtlich zu beachten haben.

In Einzelfällen wurden Defizite festgestellt, die jedoch schnell behoben werden konnten: So mangelte es in der Anfangszeit daran, dass die Kundschaft und die Gäste nicht über den Sinn und Zweck der Datenerfassung, die gesetzliche Rechtsgrundlage sowie über das Prozedere ihrer Aufbewahrung aufgeklärt wurden. Das sind Pflichten, die jedes Unternehmen treffen, das Kundendaten verarbeitet, – und damit grundsätzlich nicht neu sind. Einige Unternehmen erfassten die Kontaktdaten über das elektronische Kassensystem oder die elektronische Kunden*innen-/ Terminverwaltung. Daten von Kund*innen und Kontaktdaten sind jedoch Datenpools mit unterschiedlichen Verarbeitungszwecken und unterschiedlichen Regularien. Sie müssen daher getrennt verarbeitet werden.

Die Prüfung hat zu einer weiteren Sensibilisierung beigetragen. Auch für den Erfolg der Kontaktdatenerfassung selbst ist es wichtig, deutlich zu machen, dass der Datenschutz auch in Zeiten einer Pandemie gilt. Das Vertrauen in den sorgsamen Umgang mit den Daten ist eine wichtige Voraussetzung dafür, dass Kontaktdaten wahrheitsgemäß angegeben werden. Insoweit trägt der Datenschutz zu einer effizienten Rückverfolgbarkeit von Infektionsketten bei.

10.4 Kurzarbeit – ohne Datenschutzbeauftragte geht es nicht

Betriebliche Datenschutzbeauftragte sind auch bei Corona-bedingter Kurzarbeit unverzichtbar in Unternehmen.

Die Corona-Pandemie bleibt nicht ohne Auswirkung auf die Tätigkeit der betrieblichen Datenschutzbeauftragten. Diese sind mit vielen neuen datenschutzrechtlichen Fragestellungen konfrontiert, die sich aus der Corona-bedingten Änderung bisheriger Arbeitsabläufe in einem Unternehmen ergeben. Die Neuorganisation von Arbeitsprozessen, die Zunahme der elektronischen Datenverarbeitung, das Arbeiten im Homeoffice, in Tele-Arbeit und mittels Videokonferenzsystemen sowie nicht zuletzt Fragen des Gesundheitsdatenschutzes bei Beschäftigten und Kund*innen erfordern die Einbindung der betrieblichen Datenschutzbeauftragten.

Umso wichtiger ist es, dass auch das verantwortliche Unternehmen der oder dem Datenschutzbeauftragten die Wahrnehmung der Kontroll- und Beratungsaufgaben ermöglicht. Eine entsprechende Pflicht ist in Art. 38 Abs. 2 Datenschutz-Grundverordnung (DS-

GVO) gesetzlich verankert: Danach unterstützen Verantwortliche und Auftragsverarbeiter Datenschutzbeauftragte bei der Erfüllung ihrer Aufgaben gemäß Art. 39 DS-GVO, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.

Dies gilt auch dann, wenn in einem Unternehmen Kurzarbeit eingeführt wurde. Meistens arbeitet ein Unternehmen in verringertem Umfang weiter. Und selbst wenn ein Unternehmen für bestimmte Zeit seine Tätigkeit einstellt, besteht es weiter, hat Beziehungen zu Beschäftigten, Kund*innen und verarbeitet deren Daten. Deshalb werden Datenschutzbeauftragte weiter gebraucht und müssen ihre Aufgaben erfüllen können.

Auch an der Benennungspflicht nach dem Bundesdatenschutzgesetz (BDSG) ändert sich nichts. Zwar kommt es nach § 38 Abs. 1 BDSG darauf an, dass Personen „in der Regel (…) ständig“ mit der Verarbeitung personenbezogener Daten beschäftigt sind. Mit dieser Formulierung ist aber gerade nicht gemeint, dass kurzzeitige Veränderungen berücksichtigt werden, sondern dass es auf eine langfristige Betrachtung ankommt. Wenn also vor und voraussichtlich auch nach der zeitlich begrenzten Kurzarbeit mindestens 20 Personen gezählt werden, bleibt es auch während der Kurzarbeit bei der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten.

Zwar mag es nach den jeweiligen Umständen geboten sein, den Arbeitsumfang der Beschäftigten zu reduzieren, weil vorübergehend weniger Zeit für die

Aufgabe als Datenschutzbeauftragte*r erforderlich ist. Das Arbeitsfeld der oder des Datenschutzbeauftragten darf jedoch keinesfalls vollständig „brach liegen“. Vielmehr ist zu prüfen, unter welchen Voraussetzungen Datenschutzbeauftragte in der aktuellen Situation ihre Pflichten weiterhin wahrnehmen können. Datenschutzbeauftragte müssen nach wie vor seitens des Verantwortlichen bzw. des Auftragsverarbeiters ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden; sie müssen die Möglichkeit haben, regelmäßig ihre Posteingänge sichten zu können, sowie telefonisch und/oder per E-Mail als Ansprechpartner*in für die Beschäftigten, Kund*innen oder andere betroffene Personen erreichbar sein. Um dies sicherzustellen, sollten geeignete Maßnahmen ergriffen werden, beispielsweise regelmäßiger Zugang zum Büro oder Einrichtung eines Tele-Arbeitsplatzes, Bereitstellen eines Diensthandys, Vereinbarung bestimmter „Sprechzeiten“. Wie viel Zeit Datenschutzbeauftragte unter den aktuellen Umständen benötigen und welche Maßnahmen sachgerecht sind, sollten Arbeitgeber*innen mit ihren Datenschutzbeauftragten abstimmen.

Trotz Kurzarbeit in einem Unternehmen müssen die betrieblichen Datenschutzbeauftragten weiter in der Lage sein, ihre gesetzlichen Aufgaben wahrzunehmen und als Ansprechpartner*innen für Beschäftigte, Kund*innen oder andere Betroffene zur Verfügung zu stehen. Die Verantwortlichen sind gesetzlich verpflichtet, die Datenschutzbeauftragten auch während der Kurzarbeit bei der Erfüllung ihrer Aufgaben zu unterstützen und die entsprechenden Rahmenbedingungen zu schaffen.

10.5 Datenerhebung mittels sog. Fluggast-Aussteigekarten

Maßnahmen im Zusammenhang mit der SARS-CoV-2-Pandemie haben auch im Bereich des Flugverkehrs für Verunsicherung in der Bevölkerung gesorgt.

Uns erreichten zahlreiche Beschwerden von Fluggästen im Zusammenhang mit den sog. Fluggast-Aussteigekarten. Hierbei handelt es sich um Fragebögen in Papierform, mit denen Infektionsketten des Coronavirus SARS-CoV-2 schneller und besser nachvollzogen werden sollen. Flugreisende wurden auf Anordnung des Bundesministeriums für Gesundheit durch Personal der Fluggesellschaften im Flugzeug aufgefordert, Daten zu ihrer Person (Name, Anschrift, Telefonnummer, Informationen zum Flug, Angaben zu Mitreisenden und zum Aufenthaltsort nach Rückkehr) in einen Vordruck des Robert Koch-Instituts einzutragen. Diese ausgefüllten Fluggast-Aussteigekarten wurden sodann am Flughafen zur Weiterübermittlung an die zuständigen Gesundheitsbehörden abgegeben.

Die Fluggast-Aussteigekarten waren für Rückkehrende aus Risikogebieten konzipiert worden. Faktisch sind sie auch bei Fluggästen zum Einsatz gekommen, die sich nicht auf dem Rückflug aus einem Risikogebiet befunden haben. Die Fluggäste sahen bei diesem Vorgehen die Sicherheit Ihrer personenbezogenen Daten gefährdet. Sie bemängelten einen intransparenten Umgang bei der Erfassung ihrer personenbezogenen Daten und beanstandeten eine fehlende Information über Rechtsgrundlage, Verarbeitung und Aufbewahrung ihrer Daten. Vielfach stellten sie die Rechtmäßigkeit der Datenerhebung in Frage.

Die LDI NRW hat in diesen Fällen dahingehend aufgeklärt, dass eine Datenverarbeitung bei Rückkehr aus einem Corona-Risikogebiet auf Art. 6 Abs. 1 Satz 1 Buchstabe c, Abs. 3 DS-GVO gestützt werden kann. Denn § 12 des Gesetzes zur Durchführung der Internationen Gesundheitsvorschriften in Verbindung mit den Corona-Schutz-Verordnungen der Länder wies Fluggesellschaften zur Erhebung der personenbezogenen Daten an, die das Robert Koch-Institut in der Fluggast-Aussteigekarte benannt hatte. Des Weiteren haben wir von den betroffenen Fluggesellschaften Stellungnahmen zur Umsetzung der Informationspflicht über die Erhebung personenbezogener Daten gemäß Art. 13, 14, 21 DS-GVO eingefordert und eine transparente Aufklärung der Fluggäste empfohlen.

Die Fluggast-Aussteigekarte wurde am 8. November 2020 durch eine digitale Einreiseanmeldung ersetzt. Nach den Anordnungen des Bundesministeriums für Gesundheit müssen sich Reisende vor ihrer Einreise nach Deutschland nun elektronisch registrieren (www.einreiseanmeldung.de), wenn sie sich in den letzten zehn Tagen in einem Risikogebiet (www.rki.de/covid-19-risikogebiete) aufgehalten haben. Mit der Einreiseanmeldung erhalten die für den Zielort der Reisenden zuständigen Gesundheitsämter die notwendigen Informationen, um etwa kontrollieren zu können, ob die nach landesrechtlichen Regelungen bestehende Quarantänepflicht eingehalten wird. Die Daten werden dabei verschlüsselt, ausschließlich dem jeweils zuständigen Gesundheitsamt zugänglich gemacht und 14 Tage nach Einreise automatisch gelöscht. Verantwortlicher für die Datenverarbeitungen (Art. 4 Nr. 7 DS-GVO) im Zusammenhang mit der Einreiseanmeldung ist das Robert Koch-Institut. Auf der Homepage der digitalen Einreiseanmeldung ist

eine Datenschutzerklärung abrufbar, die betroffene Personen umfassend über die Verarbeitung ihrer personenbezogenen Daten informiert.

Die LDI NRW begrüßt die Einführung einer digitalen Einreiseanmeldung. Wir erhoffen uns eine verbesserte Sicherheit für die personenbezogenen Daten der Betroffenen und einen transparenteren Umgang mit den personenbezogenen Daten der Betroffenen.

10.6 Corona: Erfassung des Geburtsdatums bei Speditionslieferungen

Die Corona-Pandemie erfordert ein Umdenken bei der Annahme und Bestätigung von Speditionslieferungen per eigenhändiger Unterschrift.

Die LDI NRW erreichten Beschwerden und Beratungsanfragen zu der geänderten Vorgehensweise von Speditionsunternehmen, die bei der Warenauslieferung anstelle der eigenhändigen Unterschrift das vollständige Geburtsdatum der Warenempfänger*innen erfassen.

Die Speditionsunternehmen sind der Auffassung, dies diene in Zeiten der Corona-Pandemie dem Infektionsschutz und schütze so die Gesundheit der Zusteller*innen und Warenempfänger*innen.

Die Prüfung der LDI NRW hat ergeben, dass Speditionsunternehmen dieses Vorgehen auf ein berechtigtes Interesse nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO stützen können. Sie müssen gegenüber ihren Auftraggeber*innen den Nachweis der ordnungsgemäßen Warenauslieferung führen. Häufig handelt

es sich auch um teure Konsumgüter. Neben dem bereits erwähnten Gesundheitsschutz kann so auch ein Bestellbetrug aufgedeckt werden.

Demgegenüber sind die Interessen der Warenempfänger*innen eher geringer zu werten, denn die Erhebung des Geburtsdatums dient der eindeutigen Identifikation und bleibt auf den besonderen Zeitraum der Corona-Pandemie beschränkt. Der Personalausweis wird aus Infektionsschutzgründen nicht von den Zusteller*innen in die Hand genommen, sondern nach Vorzeigen des Personalausweises nur das Geburtsdatum notiert. Das Geburtsdatum verbleibt beim Speditionsunternehmen und wird nur dann an die Auftraggeber*innen weitergegeben, wenn eine ordnungsgemäße Auslieferung bestritten wird.

Eine Speicherung des Geburtsdatums für einen Zeitraum von drei Jahren ist angemessen, da Ansprüche aus dem Vertrag regelmäßig nach drei Jahren verjähren und bis dahin Rechtsstreitigkeiten denkbar sind. Die Information der Warenempfänger*innen über diese Datenverarbeitung nach Art. 13 DS-GVO erfolgt durch entsprechende Hinweise auf der Homepage und im Laufe des Zustellvorgangs. Über die ausnahmsweise Erhebung des Geburtsdatums sind die Kund*innen daher hinreichend unterrichtet.

Gerade mit Blick auf ein gesteigertes Auslieferungsvolumen aufgrund der Corona-Pandemie ist die Erfassung des Geburtsdatums ein geeignetes Mittel, eine erfolgte Warenauslieferung weiterhin unter Beachtung des Infektionsschutzes und des Grundsatzes der Datenminimierung nachzuweisen. Hier wird kein weiteres Datum, sondern lediglich – in Folge eines Ausnahmezustandes – ein anderes Datum erfasst.

10.7 Verhaltensregeln zu Prüf- und Löschfristen des Verbands „Die Wirtschaftsauskunfteien e.V.“

Die DS-GVO beinhaltet eine Reihe unbestimmter Rechtsbegriffe sowie Abwägungserfordernisse, die im Rahmen der praktischen Umsetzung einer Konkretisierung bedürfen. Diese kann mittels branchenspezifischer Verhaltensregeln erfolgen. Die Verhaltensregeln der Wirtschaftsauskunfteien wurden aktualisiert.

Nach Art. 40 Abs. 2 DS-GVO dürfen Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, Verhaltensregeln ausarbeiten. Der Entwurf der Verhaltensregeln kann dann der nach Art. 55 DS-GVO zuständigen Aufsichtsbehörde zur Prüfung und Genehmigung vorgelegt werden. Nach Art. 40 Abs. 1 DS-GVO fördern die Mitgliedstaaten, die Aufsichtsbehörden sowie der Europäische Datenschutzausschuss und die Europäische Kommission die Ausarbeitung von Verhaltensregeln.

Dem ist die LDI NRW in enger Abstimmung mit den Aufsichtsbehörden des Bundes und der Länder nachgekommen und hat zum 25. Mai 2018 die Verhaltensregeln zu Prüf- und Löschfristen des Verbands „Die Wirtschaftsauskunfteien e.V.“ genehmigt, siehe 24. Bericht unter 5.1. Im Rahmen dieser Verhaltensregeln ist es uns gelungen, einige Verbesserungen für betroffene Personen zu erzielen. Inzwischen wurden Änderungen der Verhaltensregeln genehmigt. Es konnte erreicht werden, dass gespeicherte Negativeintragungen zu notleidenden Forderungen nicht mehr drei Jahre nach Ausgleich zum Ende eines Kalenderjahres gelöscht werden sondern auf den Tag genau drei Jahre nach dem Forderungsausgleich.

Dies vermeidet zufällige Ungerechtigkeiten aufgrund unterschiedlich langer Speicherfristen. So konnte nach der vorherigen Praxis die Speicherdauer im Einzelfall bis zu fast einem Jahr länger als drei Jahre andauern.

Zudem wurde mit der Änderungsgenehmigung die Speicherdauer für sog. „Fraud-Daten“ zur Betrugsprävention ebenfalls auf drei Jahre festgesetzt. Vorangegangen war eine Evaluierung der Notwendigkeit dieses Datenbestandes und eine enge Abstimmung mit den Aufsichtsbehörden des Bundes und der Länder über diese dreijährige Speicherfrist.

Die aktualisierte Version der Verhaltensregeln für die Prüf- und Löschfristen von personenbezogenen Daten durch die deutschen Wirtschaftsauskunfteien vom 25.05.2018 (in der Fassung vom 01.01.2020) sowie die Änderungsgenehmigung vom 11.08.2020 sind auf der Homepage der Datenschutzkonferenz www.datenschutzkonferenz-online.de abrufbar.

Mit einer Änderungsgenehmigung der Verhaltensregeln für Wirtschaftsauskunfteien wurden einheitliche und präzise Löschfristen für diesen Bereich eingeführt.

10.8 Checkliste zu Verhaltensregeln – ein Leitfaden für Interessierte und Antragsteller*innen

Unsere Checkliste bringt mehr Rechtssicherheit und Transparenz für die Erstellung von Verhaltensregeln.

Die Datenschutz-Grundverordnung (DS-GVO) enthält eine Reihe unbestimmter Rechtsbegriffe sowie Abwä-

gungserfordernisse, die bei der praktischen Umsetzung konkretisiert werden müssen. Dazu können Verhaltensregeln von Verbänden und anderen Vereinigungen beitragen. Deshalb fördern die Mitgliedstaaten, die Aufsichtsbehörden sowie der Europäische Datenschutzausschuss und die Europäische Kommission die Ausarbeitung von Verhaltensregeln nach Art. 40 DS-GVO.

Antragsberechtigt sind Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsdatenverarbeitern vertreten. Die Verhaltensregeln können der zuständigen Aufsichtsbehörde zur Prüfung und Genehmigung vorgelegt werden.

Genehmigte Verhaltensregeln drücken ein gemeinsames Verständnis der Vereinigung und der genehmigenden Aufsichtsbehörde aus, wie in bestimmten Fällen personenbezogene Daten zulässig verarbeitet werden können. Zwar können Verhaltensregeln keine neue Rechtsgrundlage für eine Datenverarbeitung begründen. Sie können aber die teilweise abstrakten Regelungen der DS-GVO bereichsspezifisch präzisieren und konkretisieren und so ihre Anwendbarkeit fördern. Ferner können genehmigte Verhaltensregeln als Basis für die Übermittlung von personenbezogenen Daten in Drittstaaten herangezogen werden (zusammen mit besonderen Verpflichtungen – vgl. Art. 46 Abs. 2 Buchstabe e DS-GVO – und mit zusätzlichen Maßnahmen, falls erforderlich).

Die LDI NRW hat auf ihrer Homepage www.ldi.nrw.de eine Checkliste für Verhaltensregeln nach Art. 40 DS-GVO veröffentlicht. Sie basiert auf den Leitlinien 1/2019 über Verhaltensregeln und Überwachungsstellen des Europäischen Datenschutzausschusses.

Die Checkliste gibt Interessierten und Antragsteller*innen Anhaltspunkte, welche Inhalte in Verhaltensregeln aufgenommen werden müssen, damit diese genehmigungsfähig sind. Schon bei der Erstellung von Verhaltensregeln ist damit klar, welche Inhalte die Datenschutzaufsichtsbehörde erwartet und bewertet. Das schafft Transparenz und Rechtssicherheit für alle Beteiligten. Auch wir als Genehmigungsbehörde können damit einen Antrag schneller und strukturiert bearbeiten.

Die Checkliste zu Verhaltensregeln ist eine Praxishilfe bei der Erstellung von Verhaltensregeln und zeigt Interessierten, worauf es bei der aufsichtsbehördlichen Überprüfung ankommt.

10.9 Anforderungen zur Akkreditierung von Überwachungsstellen für Verhaltensregeln mit Sitz in Deutschland

Bereits im 25. Bericht unter 5.3 hatten wir über den Stand der Arbeiten an den Akkreditierungsanforderungen für Überwachungsstellen berichtet. Das erforderliche Verfahren auf europäischer Ebene ist nun abgeschlossen. Unternehmen mit Sitz in Nordrhein-Westfalen können ihren Antrag auf Akkreditierung als Überwachungsstelle für Verhaltensregeln (Codes of Conduct - CoC) bei der LDI NRW stellen.

Mit Verhaltensregeln nach Art. 40, 41 DS-GVO schafft die DS-GVO eine Möglichkeit der Selbstregulierung für die Verantwortlichen, die personenbezogene Daten verarbeiten. Verhaltensregeln füllen die abstrakten und allgemeinen Vorgaben der DS-GVO sektor- und branchenspezifisch aus.

Von der zuständigen Datenschutzaufsichtsbehörde genehmigte Verhaltensregeln privilegieren die Unternehmen, die diesen Verhaltensregeln beigetreten sind. So sind zum Beispiel genehmigte Verhaltensregeln ein geeignetes Instrument im Sinne des Art. 46 DS-GVO für die Übermittlung personenbezogener Daten in ein Drittland, wie die Schweiz oder die USA, oder an eine internationale Organisation. Auch stellt die Einhaltung genehmigter Verhaltensregeln durch einen Auftragsverarbeiter eine hinreichende Garantie nach Art. 28 Abs. 1 und 4 DS-GVO dar.

Für die Genehmigung von Verhaltensregeln im Bereich der Wirtschaft ist zusätzlich die Akkreditierung einer Überwachungsstelle erforderlich. Diese Stelle überwacht bei den beigetretenen Unternehmen die

Einhaltung der Verhaltensregeln, für die sie akkreditiert wurde.

Voraussetzung für die Akkreditierung der Überwachungsstelle wiederum ist, dass die Aufsichtsbehörde in ihrem Hoheitsgebiet zunächst die für eine Akkreditierung erforderlichen Anforderungen gemäß Art. 57 Abs. 1 Buchstabe p 1. Alternative DS-GVO abfasst und veröffentlicht.

Die deutschen Aufsichtsbehörden haben den Weg gewählt, diese Aufgabe nach Art. 57 Abs. 1 Buchstabe p 1. Alternative DS-GVO gemeinsam umzusetzen. Die Datenschutzkonferenz hat den Katalog der Akkreditierungsanforderungen in 2019 (Akkreditierungsanforderungen für CoC-Überwachungsstellen) erarbeitet und ihn Ende 2019 dem Europäischen Datenschutzausschuss (EDSA) zugeleitet. Die Anforderungen aus der vom EDSA im Mai 2020 erstellten Stellungnahme 10/2020, abrufbar auf der Homepage des EDSA www.edpb.europa.eu, haben die deutschen Aufsichtsbehörden unverzüglich umgesetzt. Das erforderliche Kohärenzverfahren beim Europäischen Datenschutzausschuss nach Art. 64 Abs. 1 Buchtstabe c DS-GVO wurde damit erfolgreich durchlaufen. Die deutschsprachige Fassung der Akkreditierungsanforderungen für CoC-Überwachungsstellen mit Sitz in Deutschland ist auf der Homepage der Datenschutzkonferenz www.datenschutzkonferenz-online.de abrufbar. Die englischsprachige Fassung der deutschen Akkreditierungsanforderungen wird außerdem in das Register beim Europäischen Datenschutzausschuss eingestellt werden (Art. 70 Abs. 1 Buchstabe y DS-GVO).

Mit dem Abschluss des Verfahrens vor dem EDSA haben die deutschen Aufsichtsbehörden eine weitere wichtige Voraussetzung für die Selbstregulierung der Wirtschaft geschaffen. Unternehmen, die sich auf die Überwachung von Verhaltensregeln spezialisieren möchten, können ihre Leistungen an den deutschen Akkreditierungsanforderungen ausrichten und sie den Wirtschafts- und Branchenvereinigungen anbieten, die solche Verhaltensregeln schaffen wollen.

10.10 Kontrolle von Geschäftsparkplätzen durch private Serviceunternehmen

Parkplätze von Geschäftszentren sind meistens kostenlos – jedoch nur für die eigene Kundschaft und nur für die Dauer des Einkaufs. Die Geschäfte setzen vermehrt auf eine Kontrolle durch private Unternehmen und fordern bei Verstößen nachträglich ein Nutzungsentgelt. Die dafür erforderliche Datenerhebung ist unter bestimmten Umständen datenschutzrechtlich zulässig.

Parkraum wird immer knapper. Damit die zu einem Geschäft gehörenden Parkplätze auch nur von Kund*innen genutzt werden und nicht „wild geparkt“ wird, beauftragen viele Unternehmen private Dienstleister mit der Überwachung ihres Parkraums.

So wird bei der Einfahrt auf den Parkplatz mit großen Schildern auf die Nutzungsbedingungen, die Benutzung von Parkscheiben und die Höchstparkdauer hingewiesen. Kund*innen werden aufgefordert, unverzüglich die Parkscheibe auf die Ankunftszeit einzustellen und gut sichtbar hinter der Frontscheibe des Autos zu hinterlegen. Die von den Geschäften beauf-

tragten privaten Überwachungsunternehmen kontrollieren, ob die Parkscheibe genutzt und die Höchstparkdauer eingehalten wird. Zur Beweisführung erheben sie in der Regel die folgenden Daten: Kennzeichen, Typ und Farbe des Fahrzeugs, Parkplatz, Uhrzeit sowie Fotos von der Windschutzscheibe und dem Armaturenbrett zum Nachweis, ob eine Parkscheibe angebracht wurde.

Bei anderen Geschäftsmodellen wird die Parkzeit über Sensoren erfasst, welche auf dem jeweiligen Parkplatz einer Parkfläche installiert sind. In diesen Fällen finden Kund*innen ebenfalls Hinweisschilder mit Informationen zur Höchstparkdauer vor. Die Zeitmessung startet in dem Moment, in dem das Fahrzeug über dem Sensor geparkt wird und endet, wenn sich das Fahrzeug wieder von dem Parkplatz entfernt. Hierbei handelt es sich um eine reine Erfassung des Magnetfelds. Die Sensoren nehmen keinerlei personen- oder fahrzeugbezogenen Daten auf. Bei Überschreiten der Parkdauer übermittelt der Sensor automatisch ein Signal an eine zentrale Einheit. Erst nachdem das Überwachungsunternehmen eine digitalisierte Meldung erhalten hat, wird der Parkverstoß vor Ort auf der Parkfläche dokumentiert. Erst dann erfolgt eine Verarbeitung von personenbezogenen Daten. Wurde gegen die Nutzungsbedingungen verstoßen, bringen die Beschäftigten des Überwachungsunternehmens eine Zahlungsaufforderung, vergleichbar mit einem Kassenbon, am Fahrzeug an. Diese enthält erste Informationen nach Art. 13, 14 DS-GVO und ggf. einen Link zu weiteren Informationen.

Wird nicht innerhalb eines mehrwöchigen Zeitraums gezahlt, erfolgt bei beiden Geschäftsmodellen eine

Halterabfrage beim Kraftfahrt-Bundesamt (KBA). Anschließend werden ggf. Zahlungserinnerungen und Mahnungen versandt und/oder die Forderung wird an ein Inkassounternehmen zur Beitreibung der Forderung abgegeben. Die datenschutzrechtliche Zulässigkeit ergibt sich aus Art. 6 Abs. 1 Satz 1 Buchstabe b und Buchstabe f DS-GVO (Datenverarbeitung zur Vertragserfüllung, Datenverarbeitung aufgrund berechtigten Interesses).

Das Überwachungsunternehmen handelt im Auftrag der Geschäfts- und Parkplatzinhaber*innen ausschließlich zivilrechtlich. Es wird nicht amtlich tätig. Gemäß § 858 Abs. 1 Bürgerliches Gesetzbuch handelt widerrechtlich, wer dem Besitzer ohne dessen Willen den Besitz entzieht oder ihn im Besitz stört, sofern nicht das Gesetz die Entziehung oder die Störung gestattet. Wird das Fahrzeug entgegen den Parkplatz-Nutzungsbedingungen – also widerrechtlich – abgestellt, ist dies eine verbotene Eigenmacht in diesem Sinne. Mittels der Maßnahmen zur Beweissicherung und der Zahlungsaufforderung setzen Parkplatzinhaber*innen ihr Besitz- oder Eigentumsrecht (Hausrecht) durch. Sofern Fahrzeuge auf diesen beschilderten Kund*innenparkplätzen abgestellt werden, akzeptieren Fahrzeugführende die Parkplatzordnung und gehen damit einen Nutzungsvertrag ein.

Die dafür erforderliche Datenerhebung ist nach Art. 6 Abs. 1 Satz 1 Buchstabe b und f DS-GVO zulässig. Durch die Hinweise bei der Einfahrt und beim Parken sowie durch das abgestufte Vorgehen sind die Interessen der Betroffenen ausreichend gewahrt.

Auch die Halter*innenauskunft beim Kraftfahrt-Bundesamt (KBA) oder bei der Zulassungsbehörde ist zu-

lässig. Für eine Halter*innenanfrage im Wege der einfachen Registerauskunft nach § 39 Abs. 1 Straßenverkehrsgesetz ist lediglich die Darlegung erforderlich, dass „die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt“ werden.

Gegründet auf den Nutzungsvertrag für den Parkraum haben Parkplatzinhaber*innen einen Anspruch auf ein erhöhtes Nutzungsentgelt. Zur Durchsetzung dieses zivilrechtlichen Anspruchs benötigen sie die Halter*innendaten. Dies berechtigt sie zur Abfrage.

Ob nun Halter*innen oder Fahrzeugführende für die Zahlung der Parkgebühren haften, beurteilt sich ausschließlich nach dem Zivilrecht und ist nicht von der Datenschutzaufsicht zu bewerten

Der Bundesgerichtshof hat entschieden (Urteil vom 18. Dezember 2019, Az. XII ZR 13/19): „Den Fahrzeughalter, den der Betreiber eines unentgeltlichen Parkplatzes als Fahrzeugführer auf ein „erhöhtes Parkentgelt“ in Anspruch nimmt, trifft jedoch eine sekundäre Darlegungslast. Um seine Fahrereigenschaft wirksam zu bestreiten, muss er vortragen, wer als Nutzer des Fahrzeugs im fraglichen Zeitpunkt in Betracht kommt“.

Vor der Einfahrt auf einen privaten Parkplatz sollten Fahrzeugführende auf die Hinweisschilder zur Nutzung des Parkplatzes achten. Mittlerweile ist sogar davon auszugehen, dass jeder Geschäftsparkplatz nur noch für den Geschäftsbesuch genutzt werden darf. Die privaten Überwachungsunternehmen haben dafür Sorge zu tragen, dass Beweisfotos nur die für die Anspruchsdurchsetzung notwendigen Informationen abbilden. Weitere personenbezogene Inhalte – etwa auf dem Armaturenbrett liegende Fotos, Ausweise, Schriftstücke – sind zu schwärzen. Datenerhebungen im Zusammenhang mit widerrechtlich geparkten Fahrzeugen auf Kundenparkplätzen sind daher unter Beachtung dieser Voraussetzungen zulässig.

10.11 Zahlungsdienste – Das Zusammenspiel von PSD2 und DS-GVO im Onlinebanking

Der Europäischen Datenschutzausschuss (EDSA) hat am 15. Dezember 2020 seine Leitlinien zum Zusammenspiel der Zweiten Zahlungsdiensterichtlinie und der DS-GVO veröffentlicht (Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR). Die Ergebnisse der vorangegangenen öffentlichen Konsultation sind darin eingeflossen. Damit haben die europäischen Aufsichtsbehörden einen wichtigen Beitrag zur Planungs- und Rechtssicherheit für alle Beteiligen des Zahlungsverkehrs geschaffen.

Die Zweite Zahlungsdienstleistungsrichtlinie (Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 23. Dezember 2015 (PSD2) hebt die Richtlinie 2007/64/EG auf und enthält neue Vorschriften für Verbraucher*innen, Händler*innen und

Unternehmen zur Modernisierung des Rechtsrahmens für den Markt mit Zahlungsdiensten.

Unserem 25. Bericht können Sie unter 5.4 entnehmen, dass ein wichtiges Merkmal der PSD2 die Einführung von Regelungen für die Nutzung von Zahlungsauslösediensten für das Initiieren von Überweisungen im Onlinebanking und von Kontoinformationsdiensten zur Abfrage und Auswertung von Daten auf Konten ist, die bei verschiedenen Zahlungsdienstleistern geführt werden. Ergänzende Informationen für Verbraucher*innen enthält das von der Verbraucherzentrale Bundesverband e.V. beauftragte „Gutachten zur PSD2-Umsetzung in Deutschland - Projekt über Kontoinformations-und Zahlungsauslösedienste“ vom 28. Januar 2021, an dem die LDI NRW mitgewirkt hat.

Bargeld ist zwar sowohl nach Umsatz als auch nach Zahlungsvorgängen bei den Verbraucher*innen in Deutschland bislang das mit Abstand beliebteste Zahlungsmittel. Doch hat bereits die Corona-Pandemie eine deutliche Änderung weg vom Bargeld hin zu elektronischen Zahlungsmitteln bewirkt, wie Kartenzahlung oder mittels Bezahl-Apps wie Apple Pay oder Google Pay. Auch die Nutzung von Kontoinformationsdiensten erfreut sich immer größerer Beliebtheit.

Aus Datenschutzsicht gilt zu bedenken, dass das Geschäftsmodell der neuen Zahlungsdienstleistungen auf der Verarbeitung der Daten der jeweiligen Kontoinhaber*innen beruht. Zum Kerngeschäft von Digitalkonzernen gehört die Auswertung der Daten.

Die PSD2 schafft damit zwar neue Möglichkeiten für die Verbraucher*innen, erhöht die Sicherheit im Zah-

lungsverkehr und fördert Innovation in diesem Bereich. Doch wirft die Anwendung der PSD2 einige Fragen und Bedenken hinsichtlich des Datenschutzes auf; insbesondere muss sichergestellt sein, dass die Verbraucher*innen die vollständige Kontrolle über ihre Daten behalten.

Verantwortliche, die in den Anwendungsbereich der PSD2 fallen, haben bei ihrer Datenverarbeitung stets die Einhaltung der Anforderungen der DS-GVO sicherzustellen, einschließlich der in Art. 5 DS-GVO niedergelegten Datenschutzgrundsätze, insbesondere der Zweckbindung, Datenminimierung und Transparenz.

Die EDSA-Leitlinien beschreiben in diesem Zusammenhang die Bedingungen für die Gewährung des Zugangs zu Zahlungskontoinformationen und für die Verarbeitung personenbezogener Daten durch Zahlungsauslöse- und Kontoinformationsdienste, einschließlich der Anforderungen in Bezug auf die Verarbeitung personenbezogener Daten zu anderen als den ursprünglichen Zwecken, für die die Daten erhoben wurden.

Die Leitlinien befassen sich auch mit den verschiedenen Begriffen der ausdrücklichen Zustimmung nach der PSD2 und dem Begriff der Einwilligung nach der DS-GVO und der Verarbeitung personenbezogener Daten von Dritten (sog. „Silent Party Data“), die nicht Vertragspartei eines Kontoinformations- oder Zahlungsauslösedienstleisters sind. Sie ergänzen damit das bereits am 5. Juli 2018 veröffentlichte Schreiben des EDSA zur PSD2.

Zur Klärung von Bedenken in Zusammenhang mit der Betrugsprävention enthalten die Leitlinien auch einen

Absatz, in dem erläutert wird, dass die Betrugsprävention auch ein Zweck der Verarbeitung gemäß Art. 94 Abs. 1 der PSD2 unter der Voraussetzung sein kann, dass eine solche Verarbeitung erforderlich ist. Im Sinne des Grundsatzes der Datenminimierung empfiehlt der EDSA in seinen Leitlinien den Kontoinformationsdienstleistern die Verwendung digitaler Tools, um Zahlungsinformationsdienstleister in ihrer Verpflichtung zu unterstützen, nur personenbezogene Daten zu erheben, die für die Zwecke, für die sie verarbeitet werden, erforderlich sind. Die Möglichkeit der Nutzung von sog. Dashboards zur besseren Information der Betroffenen ist gleichfalls angesprochen. Ein Datenschutz-Dashboard gibt den Betroffenen die Möglichkeit, einen Überblick über die von ihnen genutzten Drittdienste sowie über Art und Menge der Informationen zu erhalten, auf die der Drittdienst zugegriffen hat. Auch weist der EDSA auf die Möglichkeit hin, das Dashboard so auszugestalten, dass einmal erteilte Zustimmungen zum Kontozugriff widerrufen werden können.

Die Leitlinien des EDSA zum Zusammenspiel der PSD2 und der DS-GVO sind als Hilfestellung für die kontoführenden Zahlungsdienstleister, die Drittdienste – Zahlungsauslösedienste und Kontoinformationsdienste –, die Zahlungsdienstenutzer*innen sowie für die Datenschutzaufsichtsbehörden in den EU-Mitgliedstaaten sehr zu begrüßen.

10.12 Aufzeichnung von Telefongesprächen

Mehrfach hat die LDI NRW darauf hingewirkt, dass Unternehmen Sprachaufzeichnungen von Telefonaten zur Verbesserung ihrer Prozesse und zur Schulung ihres Personals auf ein eindeutiges Einwilligungsverfahren (Opt-in) umstellen.

Die Aufzeichnung von Telefongesprächen ist datenschutzrechtlich nur mit Einwilligungen der Kund*innen zulässig. Siehe hierzu bereits die Entschließung der Datenschutzkonferenz "Aufzeichnung von Telefongesprächen“ vom 23. März 2018.

Teilweise räumen Unternehmen ihrer Kundschaft lediglich eine Widerspruchsmöglichkeit ein. Diese Vorgehensweise und das anschließende Fortsetzen des Telefonats stellen keine datenschutzrechtlich wirksame Einwilligung im Sinne der DS-GVO dar.

Die LDI NRW konnte mehrfach erfolgreich darauf hinwirken, dass Unternehmen ihre Anrufaufzeichnungsprozesse nunmehr datenschutzgerecht gestalten.

Die automatische Benachrichtigung ist dabei so auszugestalten, dass die Anrufaufzeichnung erst und nur dann beginnt, wenn sich die Kund*innen – zum Beispiel durch Betätigung einer bestimmten Taste oder durch Aussprechen eines bestimmten Wortes – hierfür bewusst entscheiden.

10.13 Unzulässige Verwendung beruflich zugänglicher Daten zur privaten Kontaktaufnahme

Eigentlich eine Selbstverständlichkeit: Kontaktdaten, auf die eine Person aus beruflichen Gründen Zugriff hat – etwa im Zusammenhang mit einem ärztlichen Behandlungsverhältnis oder anhand von Bewerbungsunterlagen – dürfen ohne Einwilligung der betroffenen Person nicht für eine private Kontaktaufnahme genutzt werden. Doch leider kommt es immer wieder zur missbräuchlichen Verwendung solcher Daten für nicht zulässige private Zwecke.

Der LDI NRW lagen mehrere Eingaben zur Nutzung von Kontaktdaten vor, die in beruflichem Zusammenhang erlangt, jedoch für private Zwecke verwendet wurden.

In einem Fall hatte die betroffene Person eine Klinik für eine medizinische Behandlung aufgesucht. Insoweit lagen der Klinik unter anderem der Vor- und Nachname der betroffenen Person vor. Die zuständigen Ärzt*innen der Klinik hatten somit aufgrund des Behandlungsverhältnisses Kenntnis von diesen Informationen. Eine dieser Personen hat den Vor- und Nachnamen sodann genutzt, um die betroffene Person später im Sozialen Netzwerk Facebook zu suchen und auf privater Ebene zu kontaktieren.

In einem anderen Fall hatte die betroffene Person sich auf eine Arbeitsstelle beworben. Aus den Bewerbungsunterlagen ergab sich auch die private Mobilfunknummer. Es fand ein persönliches Vorstellungsgespräch statt; ein Beschäftigungsverhältnis ergab sich jedoch nicht. Eine Person, die bei dem potenziellen Arbeitgeber Zugriff auf die Bewerbungsunterlagen

hatte, nutzte später die private Mobilfunknummer der betroffenen Person für eine Kontaktaufnahme über den Messenger WhatsApp. Auch diese Kontaktaufnahme geschah aus privater Motivation heraus.

Eine Kontaktaufnahme über Soziale Netzwerke oder Messenger unter Nutzung des Namens oder der Mobilfunknummer stellt eine automatisierte Verarbeitung dieser personenbezogenen Daten dar. Eine solche Verarbeitung ist nur zulässig, wenn hierfür eine Rechtsgrundlage vorliegt.

Eine Einwilligung der betroffenen Person lag in beiden Fällen nicht vor. Da die Datenverarbeitung zu privaten Zwecken erfolgt war, diente sie auch nicht der Erfüllung oder Anbahnung eines Vertrages im Zusammenhang mit dem ärztlichen Behandlungsverhältnis bzw. dem Bewerbungsverhältnis.

Es ist auch kein berechtigtes Interesse erkennbar, die im beruflichen Zusammenhang zugänglich gemachten Daten für private Zwecke zu nutzen. Weiterhin müssen weder Patient*innen noch Bewerber*innen mit einer solchen Datenverarbeitung rechnen. Patient*innen erwarten, dass die Vertraulichkeit aller Informationen gewahrt wird, die im Zusammenhang mit der Behandlung bekanntgemacht werden. Ebenso erwarten Bewerber*innen, dass potenzielle Arbeitgeber*innen bzw. die dort tätigen Personen die erlangten Daten nur zu Zwecken des Bewerbungsverhältnisses verwenden. Daher überwiegt das entgegenstehende Interesse der betroffenen Personen, dass derartige Informationen nicht für Zwecke außerhalb des ärztlichen Behandlungsverhältnisses bzw. des Bewerbungsverhältnisses verwendet werden.

In beiden Fällen wurde in Anbetracht der Gesamtumstände eine Verwarnung ausgesprochen. Diese richtete sich gegen die jeweils handelnde natürliche Person, die in diesen Fällen als datenschutzrechtlich Verantwortlicher einzuordnen war. Da die jeweiligen Daten nur zu beruflichen Zwecken hätten verarbeitet werden dürfen, lag die Nutzung zu rein privaten Zwecken nicht im Bereich der dienstlichen Befugnisse. Diese Datenverarbeitung war daher nicht dem jeweiligen Arbeitgeber zuzurechnen. Vielmehr haben die natürlichen Personen über die Zwecke und Mittel der Datenverarbeitung bestimmt und waren daher selbst Verantwortliche.

Es lag auch keine Ausnahme vom Anwendungsbereich der Datenschutz-Grundverordnung (DS-GVO) vor. Diese findet zwar gemäß ihres Art. 2 Abs. 2 Buchstabe c keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten. Dies soll nach Erwägungsgrund 18 Satz 1 DS-GVO der Fall sein, wenn die Verarbeitung ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird (siehe dazu auch 25. Bericht unter Ziffer 4.7). Hier wurden jedoch jeweils Daten genutzt, die den handelnden Personen gerade aufgrund deren beruflicher Tätigkeit bekanntgeworden bzw. verfügbar waren. Die Verwendung der Daten war daher zwar privat motiviert, stand aber zugleich in einem Bezug zur beruflichen Tätigkeit.

Personenbezogene Daten dürfen nur bei Vorliegen einer Rechtsgrundlage und nur für legitime Zwecke verarbeitet werden. Hat eine Person im beruflichen Kontext Zugriff auf personenbezogene Daten, so dürfen diese grundsätzlich auch nur für berufliche Zwecke und im Rahmen des insoweit Erforderlichen genutzt werden. Eine Nutzung von beruflich erlangten Informationen zur privaten Kontaktaufnahme ist daher – sofern keine wirksame Einwilligung der betroffenen Person vorliegt – nicht zulässig. Da sich die Zugriffsmöglichkeit auf die Daten gerade aus der beruflichen Tätigkeit ergibt, erfolgt eine Verarbeitung solcher Daten nicht zur Ausübung ausschließlich persönlicher Tätigkeiten, sondern unterliegt den datenschutzrechtlichen Vorgaben.

10.14 Verpfändungserklärung für Mietkautionskonten in der Sparkassenfinanzgruppe

Einzelne Kreditinstitute legen Mietkautionskonten an, indem entsprechende Sparguthaben der Mieter*innen zugunsten der jeweiligen Vermieter*innen als Mietkaution verpfändet werden. Den Abdruck des Geburtsdatums von Vermieter*innen als Pfandgläubiger*innen auf Verpfändungserklärungen von Mietkautionskonten lehnen manche zu Recht ab.

Die unterschiedliche Handhabung einzelner Sparkassen in NRW, neben den weiteren Angaben zur Person der Pfandgläubiger*innen auch deren Geburtsdaten auf der Verpfändungserklärung abzudrucken, veranlasste die LDI NRW mit dem für die Mitgliedsinstitute der Sparkassen-Finanzgruppe zuständigen Verbänden in NRW, dem Sparkassenverband Westfalen-

Lippe (SVWL) und dem Rheinischen Sparkassen- und Giroverband (RSGV), in Kontakt zu treten.

Datenschutzrechtlich zu beanstanden ist es, wenn die Sparkasse das Geburtsdatum der Vermieterin oder des Vermieters als Pfandgläubiger*in auf der für die Mieterin oder den Mieter bestimmten Ausfertigung der Verpfändungserklärung offengelegt.

Selbstverständlich bleibt es jeder Sparkasse unbenommen, Verpfändungserklärungen auch ohne Angabe zum Geburtsdatum auszufertigen. Im datenschutzrechtlichen Sinn ist es auch vertretbar, dass die Sparkasse das Geburtsdatum der Vermieterin oder des Vermieters als weiteres Datum zur eindeutigen Identifizierbarkeit erhebt und ggf. auf der für diesen Personenkreis und auf der für ihre Unterlagen bestimmten Erklärung vermerkt.

Auch ist die Speicherung des Geburtsdatums in den Systemen des Kreditinstituts nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO rechtmäßig. Die Sparkasse hat ein berechtigtes Interesse, die Person des Pfandgläubigers oder der Pfandgläubigerin im Verwertungsfall, also der Kündigung des Guthabens und anschließender Auszahlung, eindeutig identifizieren zu können. Überwiegende entgegenstehende Interessen sind regelmäßig nicht ersichtlich. Es ist im Interesse der Pfandgläubiger*in, bei Pfandreife zügig über das Guthaben verfügen zu können, ohne dass es dann zu Auseinandersetzungen mit der Sparkasse wegen etwaiger Zweifel über ihre Berechtigung kommt. Die Nennung des Geburtsdatums ist ein geeignetes Datum, über das auch im Falle von Namensidentitäten und wechselnder Anschriften Pfandgläubiger*innen eindeutig identifiziert werden können.

Die LDI NRW konnte über die beiden Sparkassenverbände SVWL und RSGV erreichen, dass auf den Formularen des Deutschen Sparkassenverlages (DSV) für die Mietkaution zukünftig das Geburtsdatum der Vermieter*in/Pfandgläubiger*in unter Beachtung des Grundsatzes der Datenminimierung nach Art. 4 Abs. 1 Buchstabe c DS-GVO nicht mehr abgedruckt und insofern nicht mehr gegenüber den Mieter*innen offengelegt wird.

Der regelmäßige Austausch zwischen LDI NRW und Verbandsvertretungen fördert das Verständnis branchenspezifischer Besonderheiten und erleichtert die Umsetzung erforderlicher Maßnahmen zur Verbesserung datenschutzrechtlicher Maßstäbe.

10.15 Ausliegende Abreiseinformationen von Fluggästen im Hotel

An der Hotelrezeption ausliegende Informationen zu Abflugzeiten und – im Falle eines Transfers zum Flughafen – zu Abholzeiten können datenschutzrechtliche Probleme bereiten.

Das offene Aushängen von für jede Person einsehbaren personenbezogenen Daten, wie Name, Alter und Familienzugehörigkeit, ist mit den datenschutzrechtlichen Grundsätzen nicht in Einklang zu bringen. Im Einzelfall kann aber die Offenlegung der Informationen zur Abflugzeit und – im Falle eines Transfers zum Flughafen – die Abholzeit unter Namensnennung in Form eines an der Rezeption hinterlegten Ordners im Sinne des Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO erforderlich sein. Dann sind die ausliegenden Listen auf die nötigsten Informationen zu beschränken, die für eine eindeutige Zuordnung von

Reisenden zu einem konkreten Flug und ggf. auch Transfer erforderlich sind. So sollte zum Beispiel die Namensnennung auf den Familiennamen reduziert und bei Kindern gar auf eine vollständige Namensnennung verzichtet werden.

Bei der Prüfung nach Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO sind entgegenstehende Interessen der von der Datenverarbeitung Betroffenen und die berechtigten Interessen des Verantwortlichen oder Dritten gegeneinander abzuwägen. Das Interesse des Reiseveranstaltungsunternehmens, dafür Sorge zu tragen, dass seine Kund*innen sichere Kenntnis von den sehr kurzfristigen Flugplan- und Kapazitätsänderungen der Airline und des damit verbundenen Flughafentransfers erhalten, fließt in diese datenschutzrechtlich erforderliche Abwägung ein. Auch sind die berechtigten Interessen des Hotels und Reiseveranstaltungsunternehmens an einem reibungslosen, wirtschaftlich vertretbaren Ablauf zu berücksichtigen. Dies gilt zumindest für stark frequentierte Flugdestinationen.

Im Sinne eines reibungslosen Ablaufes und wegen möglicher, erheblicher wirtschaftlichen Nachteile für die Reisenden im Falle eines verspäteten Rücktransfers ist es erforderlich, Falschinformationen bereits im Vorfeld auszuschließen. Regelmäßig wird das Interesse der Reisenden an der korrekten Information zu den Rückreisetransfers größer sein als die Sorge, dass mittels der auf der Abreiseliste hinterlegten personenbezogenen Daten Missbrauch betrieben wird.

Im Rahmen einer Beschwerdebearbeitung hat die LDI NRW über die vorstehenden Grundsätze hinausgehende Maßnahmen erreichen können:

Im Ergebnis werden nun keine Abreiseinformationen mehr an der Hotelrezeption ausgelegt. Das Unternehmen beschränkt sich nun vielmehr auf die persönliche Zustellung der Abflug-/Transferdaten an die Gäste. In der Regel werden nun die Dokumente direkt in der Unterkunft auf die Gästezimmer gelegt und in manchen Fällen – dann ohne Vorgangsnummer und Gästenamen – als Aushang angebracht oder in einer sog. Infomappe am Empfang hinterlegt. Für die nahe Zukunft plant das Unternehmen im Zuge der allgemeinen fortschreitenden Digitalisierung durch Nutzung geeigneter Endgeräte auf der einen und sicherer Servertechnik auf der anderen Seite eine sichere und datenschutzkonforme Lösung bereitzustellen.

Im vertrauensvollen Dialog zwischen Datenschutzaufsicht und den für die Datenverarbeitung Verantwortlichen können neue Maßstäbe datenschutzrechtlicher Standards in der täglichen Praxis geschaffen werden.

10.16 Datenschutzrechtliche Verantwortlichkeit von Steuerberater*innen und Steuerberatungsgesellschaften

Mit der Neufassung des § 11 Steuerberatungsgesetz (StBerG, Bundesgesetzblatt Jahrgang 2019 Teil I S. 2451, 2485) wurde klargestellt, dass Steuerberater*innen und Steuerberatungsgesellschaften bei der Erbringung von Leistungen nach dem Steuerberatungsgesetz stets als datenschutzrechtlich Verantwortliche anzusehen sind und eine Auftragsverarbeitung nicht mehr in Betracht kommt.

Die Verarbeitung personenbezogener Daten durch Steuerberater*innen und Steuerberatungsgesellschaften erfolgt nach § 3 StBerG unter Beachtung der für sie geltenden Berufspflichten weisungsfrei. Dies gilt auch dann, wenn sie im Rahmen ihrer gesetzlichen Pflichten geschäftsmäßig Hilfeleistung in Steuersachen, wie die Lohn und Gehaltsabrechnung, erbringen und dabei personenbezogene Daten ihrer Mandant*innen verarbeiten.

Die Leistung der mit der Lohnbuchführung beauftragten Steuerberater*innen umfasst die eigenverantwortliche Prüfung und Anwendung der gesetzlichen Bestimmungen (BT-Drs 19/14909, Seite 59). Das bedeutet, dass Steuerberater*innen keine Auftragsverarbeiter sind, auch nicht soweit sie die Lohn- und Gehaltsabrechnung für ihre Mandant*innen durchführen. Diese Frage war bisher unter den Aufsichtsbehörden strittig bzw. wurde unterschiedlich beantwortet.

In seiner Sitzung vom 11. Februar 2020 hat sich der Arbeitskreis Wirtschaft der Datenschutzkonferenz erneut mit der datenschutzrechtlichen Einordnung der

Steuerberater*innentätigkeit in der Lohnbuchhaltung befasst. Erörtert wurde neben der gesetzgeberischen Entscheidung zu § 11 StBerG in diesem Zusammenhang auch die Frage der Rechtsgrundlage für die Übermittlung besonderer Kategorien personenbezogener Daten von Beschäftigten im Sinne von Art. 9 Abs. 1 Datenschutz-Grundverordnung (DS-GVO) durch Unternehmen an Steuerberatende, wie etwa Angaben zur Religionszugehörigkeit oder zur Gesundheit im Rahmen der Berechnung von Krankheitszeiten.

Überwiegend wurde hier § 26 Abs. 3 Bundesdatenschutzgesetz (BDSG) als hinreichende Rechtsgrundlage für die Datenübermittlung angesehen.

Wir sehen mit der Mehrheit der Aufsichtsbehörden in § 26 Abs. 3 BDSG eine hinreichende Rechtsgrundlage für die Datenübermittlung.

Steuerberatende sind datenschutzrechtlich Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO unabhängig davon, ob sie in Steuersachen eine beratende steuerrechtliche Hauptleistung oder eine Hilfsleistung wie die Lohn- und Gehaltsabrechnung erbringen.

10.17 Unberechtigte Einsichtnahme einer Sparkassenmitarbeiterin in fremde Konten

Der berufsbedingte Zugang zu Datenbanken verleitet manchmal einzelne Bankmitarbeiter*innen zum unberechtigten Abruf. Hier bedarf es daher fortlaufender Sensibilisierung.

Eine Auszubildende der Sparkasse hat unberechtigterweise Zugriff auf die Kundendaten ihres ehemaligen Freundes sowie dessen Cousins genommen. Nach Kenntnis dieser Vorwürfe durch die Betroffenen hat die Sparkasse mit Hilfe der Revision Ermittlungen aufgenommen. Die Auszubildende wurde zu den Zugriffen befragt. Sie befürchtete, dass ihr ehemaliger Freund wegen ihres privaten Konflikts mit ihm und wegen seines kulturellen Hintergrunds eine größere Summe Bargeld vom Konto abheben wollte, um jemanden zu beauftragen, ihr Gewalt anzutun. Eine Datenweitergabe an Dritte ist nicht erfolgt. Der Auszubildenden wurde von der Bank gekündigt. Zusätzlich zum Verlust des Ausbildungsplatzes erhielt sie von uns eine strenge Verwarnung.

Mitarbeiter*innen müssen sich stets bewusst sein, dass sie nur aufgrund von berufsbedingten Anlässen von den ihnen eingeräumten Möglichkeiten eines Datenbankzugriffs Gebrauch machen dürfen. Eine Zuwiderhandlung ist kein Kavaliersdelikt.

11. Datensicherheit

11.1 Erste Erfahrungen mit dem Webformular für Meldungen von Datenpannen

Seit März 2020 stellt die LDI NRW ein Webformular für Meldungen von Datenpannen zur Verfügung. Zeit für ein erstes Resümee.

Das Webformular stellt seit März 2020 den zentralen Kommunikationsweg für Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DS-GVO und Informationen über Benachrichtigungen nach Art. 34 DS-GVO an die LDI NRW dar. Siehe auch 25. Bericht unter 12.1.

Die LDI NRW ist damit einem vielfach geäußerten Wunsch der meldepflichtigen Stellen nachgekommen. Das Webformular wird von den Verantwortlichen – auch wegen der unmittelbaren Eingangsbestätigung mit Angabe des Aktenzeichens – positiv angenommen. Durch die direkte Weiterleitung der Meldungen an die Sachbearbeitung konnten wir unsere Reaktionszeiten auf Meldungen signifikant verkürzen und somit im Sinne des Schutzgedankens der Art. 33 und 34 DS-GVO bei Bedarf schneller tätig werden. Die zentrale, elektronische Bearbeitung der Meldungen ermöglicht zudem eine effizientere Sachbearbeitung. Damit diese positiven Effekte beibehalten werden können, ist die Nutzung des Webformulars durch Verantwortliche für uns unverzichtbar.

An die LDI NRW wurde vereinzelt der Wunsch herangetragen, dass das Webformular in interne Abstimmungsprozesse der Verantwortlichen integriert werden kann. Das Webformular der LDI NRW ersetzt

keine internen Prozesse zur Aufarbeitung und Bewertung von Datenpannen bei Verantwortlichen und kann diese nur begrenzt unterstützen. Das Webformular kann vor dem Absenden als PDF-Datei exportiert werden und so der internen Abstimmung dienen. Jedoch müssen die exportierten Informationen später erneut in das Webformular (per „Kopieren und Einfügen“) eingetragen werden. Wir empfehlen Verantwortlichen daher im Rahmen ihrer internen Prozesse zum Umgang mit Datenpannen elektronische Dokumente zu nutzen, die den jeweiligen internen Anforderungen gerecht werden. Idealerweise sollten diese Dokumente so gestaltet werden, dass aus diesen per „Kopieren und Einfügen“ die für die Meldung an die LDI NRW relevanten Informationen in das Webformular übernommen werden können.

Für Datenpannen, von denen voraussichtlich kein bzw. nur ein geringes Risiko für die Rechte und Freiheiten natürlicher Personen ausgeht, besteht gemäß Art. 33 Abs. 1 DS-GVO keine Meldepflicht an die LDI NRW. Sofern Verantwortliche im Webformular angeben, dass nur ein geringes Risiko vorliegt, erhalten sie beim Absenden den Hinweis, dass keine Meldepflicht besteht und die Meldung nicht an uns übermittelt wurde. Das ausgefüllte Webformular kann in diesen Fällen ergänzend zur internen Dokumentation der Datenpanne gemäß Art. 33 Abs. 5 DS-GVO als PDF-Datei exportiert werden. Durch die Nicht-Meldung solcher „Bagatellpannen“ werden die Ressourcen der LDI NRW geschont.

Verantwortliche sollten Meldungen von Datenpannen nur noch über das Webformular an die LDI NRW abgeben. Datenpannen, von denen lediglich ein geringes Risiko für die betroffenen Personen ausgeht, müssen von den Verantwortlichen intern dokumentiert werden, jedoch nicht an uns gemeldet werden. Durch den neu eingeführten Meldeweg können bei der LDI NRW die personellen Ressourcen nun effizienter genutzt werden und die Reaktionszeit auf Meldungen von Datenpannen konnte erheblich reduziert werden.

11.2 Bedeutung grundlegender technischer und organisatorischer Maßnahmen

Im vergangenen Jahr sind wir sowohl durch Meldungen nach Art. 33 DS-GVO als auch über Beschwerden über offen im Internet abrufbare personenbezogene Daten informiert worden. So waren zum Beispiel die in einem Online-Shop getätigten Bestellungen der letzten zehn Jahre oder auch die Pizza-Bestellungen eines Lieferdienstes ohne jegliche Authentifizierung für alle abrufbar, die die korrekte URL erraten haben.

Dies war von den jeweiligen Verantwortlichen in dieser Form nicht beabsichtigt. Die Beispiele zeigen aber, dass Fehler, die zur Verletzung des Schutzes personenbezogener Daten führen, jederzeit auftreten können.

Aus diesem Grund hat sich ein sog. „Defense-in-Depth“-Ansatz als gute Praxis etabliert. Bei diesem Konzept werden mehrere Sicherheitsmaßnahmen so kombiniert, dass das Versagen einer Maßnahme

nicht zur Kompromittierung des zu schützenden Gutes führt oder zumindest die Auswirkungen begrenzt werden.

In den genannten Fällen hätte zum Beispiel eine zusätzliche Einschränkung des Zugriffs auf bestimmte IP-Bereiche verhindert, dass die Daten beim Versagen des Passwortschutzes öffentlich zugänglich werden. Wären die Daten, nachdem sie, zum Beispiel zur Kontrolle der Bestellung im Self-Service, nicht mehr auf dem Internet-Server benötigt wurden, auf ein gesondertes System ohne direkte Zugriffsmöglichkeit aus dem Internet verschoben worden, wäre von der Datenpanne immerhin nur noch ein Bruchteil der personenbezogenen Daten betroffen gewesen.

Bei der Entwicklung eines Systems zur Verarbeitung personenbezogener Daten sollte immer davon ausgegangen werden, dass einzelne Sicherheitsmaßnahmen versagen können. Um dies zu kompensieren, sollte immer ein Defense-In-Depth-Ansatz verfolgt werden.

11.3 Wachsamkeit bezüglich Spam-, Viren- und Phishingmails ist weiterhin geboten

Die Anzahl der Meldungen zu Angriffen auf E-Mail-Konten sowie diesbezügliche Beschwerden an die LDI NRW zeigen, dass Spam-, Viren- und Phishingmails ein Dauerproblem sind, auf das Verantwortliche mit geeigneten Maßnahmen reagieren müssen.

Ungefähr 20 Prozent der Meldungen nach Art. 33 DS-GVO an die LDI NRW werden durch Hacker*innenangriffe ausgelöst. Neben Angriffen mit Ransomware stellen Angriffe über Spam-, Viren- und Phishingmails (im folgenden Schadmails) den überwiegenden Teil dieser Meldungen dar.

Die Ziele der Angreifer*innen können dabei sehr unterschiedlich sein. In den meisten Fällen geht es den Angreifer*innen darum, Zugriff auf ein E-Mail-Konto zu erlangen. Damit sind zumeist auch personenbezogene Daten von diesen Angriffen betroffen. Die Schadmails verlocken die Empfänger*innen dazu, eine Datei zu öffnen oder Anmeldedaten auf einer gefälschten Webseite anzugeben. Wird eine solche Datei geöffnet, wird im Hintergrund – häufig unbemerkt – der Computer mit einer Schadsoftware infiziert. Über die Schadsoftware können die Angreifer*innen meist den infizierten Computer oder einzelne Anwendungen kontrollieren.

Eine häufig beobachtete Schadsoftware ist Emotet. Hierbei handelt es sich um einen sog. Makrovirus, der in Office-Dokumente eingebettet und zumeist über täuschend echt aussehende E-Mails verteilt wird. Daneben gibt es inzwischen verschiedene Varianten solcher Schadsoftware, die teilweise nicht bzw. zu spät

von Virenscannern erkannt werden. Mittlerweile werden diese Schadsoftwaretypen so generisch gestaltet, dass Angreifer*innen bei erfolgreicher Infektion weitere Schadsoftware auf die befallenen Computer nachladen und von dort aus weitere Systeme infizieren können.

Haben Angreifer*innen über die Schadsoftware oder erbeutete Zugangsdaten Zugriff auf ein E-Mail-Konto, werden von diesem meist Adressbücher und E-Mail-Korrespondenzen ausgelesen. Das E-Mail-Konto wird dann häufig dazu genutzt, weitere Schadmails von einer validen E-Mail-Adresse zu versenden. Dies geschieht zumeist als Antwort auf vorangegangene E-Mails, so dass die Empfänger*innen nicht direkt erkennen können, dass es sich um Schadmails handelt. Auf diese Weise kann sich der Angriff ausweiten. Auch nachdem der Angriff erkannt wurde und der Zugriff auf den Computer bzw. das E-Mail-Konto für die Angreifer*innen nicht mehr möglich ist, werden die erbeuteten Adressbücher und E-Mail-Korrespondenzen weiterhin verwendet, um weitere – teilweise sehr authentische – Schadmails von anderen E-Mail-Adressen zu versenden. Zudem gelangen die E-Mail-Adressen – auch mit einem größeren zeitlichen Versatz – regelmäßig auf Spam-Verteilerlisten und können für sog. Password-Spraying oder Credential-Stuffing genutzt werden. Bei den letzteren Angriffen werden die E-Mail-Adressen als Benutzernamen zusammen mit häufig verwendeten Passwörtern für Login-Versuche bei verschiedenen Online-Diensten genutzt.

Um den Gefahren solcher Angriffe zu begegnen, müssen Verantwortliche geeignete technische und organisatorische Maßnahmen treffen.

Um einen externen Zugriff durch das Erraten von Passwörtern zu vermeiden, sollten Verantwortliche über Passwortrichtlinien sicherstellen, dass nur starke Passwörter genutzt werden. Zudem sollte geprüft werden, ob bei einem Zugang auf E-Mail-Konten über das Internet (sog. Web-Mail) eine Multi-Faktor-Authentifizierung eingesetzt werden kann. Durch diese Maßnahme wird ein Zugang zu einem E-Mail-Konto meist auch dann noch verhindert, wenn die Angreifer*innen das Passwort des Kontos erlangt haben.

Häufig erfolgen Angriffe von bestimmten IP-Adressen bzw. gewissen IP-Adressbereichen. Diese können ggf. durch entsprechende Firewall-Einstellungen von einem externen Zugriff auf Systeme der Verantwortlichen ausgeschlossen werden. Alternativ können nur Zugriffe von bestimmten IP-Adressbereichen erlaubt werden, aus denen die befugten Zugriffe stattfinden.

Ein weiteres Einfallstor für Angreifer sind Sicherheitslücken oder unsichere Konfigurationen von Office-Anwendungen (beispielsweise durch die Ausführung unsicherer Makros). Hierzu müssen Verantwortliche ein systematisches und kontinuierliches Patch-Management etablieren und eingesetzte Office-Produkte entsprechend sicher konfigurieren.

Nicht zuletzt müssen Verantwortliche ihre Angestellten schulen und sensibilisieren, damit diese Schad-Mails frühzeitig erkennen können. Zudem müssen Angestellte wissen, welche Stellen beim Verantwortlichen bei Auffälligkeiten, die auf einen Hacker*innenangriff hindeuten, zu informieren sind.

Ist es trotz aller vorbeugenden Maßnahmen zu einem erfolgreichen Angriff auf ein E-Mail-Konto gekommen,

empfiehlt die LDI NRW den Verantwortlichen, – unabhängig vom Vorliegen einer Benachrichtigungspflicht nach Art. 34 DS-GVO – die betroffenen Personen schnellstmöglich über den Vorfall zu informieren. Dadurch werden diese nicht nur über den Empfang von Schad-Mails informiert, sondern auch hinsichtlich des Missbrauchs der Daten für mögliche weitere Angriffe (etwa Password-Spraying oder Credential-Stuffing) sensibilisiert. Dies gilt insbesondere vor dem Hintergrund, dass Verantwortliche keine Kontrolle über einmal an Angreifer*innen abgeflossene personenbezogene Daten haben. Durch die Information der betroffenen Personen kann in vielen Fällen eine Ausweitung des Angriffs verhindert werden. Zudem können die Betroffenen dann in ihrer eigenen Sphäre Schutzmaßnahmen treffen.

Sofern personenbezogene Daten von einem solchen Angriff betroffen sind, ist dieser gemäß Art. 33 Abs. 5 DS-GVO intern zu dokumentieren. Sollte ein mehr als geringes Risiko für die betroffenen Personen festgestellt werden, so muss die Datenpanne gemäß Art. 33 Abs. 1 DS-GVO an die LDI NRW gemeldet werden. Hierzu stellen wir ein Webformular zur Verfügung. Siehe hierzu unter 11.1.

Schad-Mails bleiben als Einfallstor für Hacker*innen ein Dauerthema. Die Angriffe werden zunehmend ausgefeilter und werden teilweise auf die Empfänger*innen personalisiert. Mit verschiedenen technischen Maßnahmen kann den Gefahren solcher Schad-Mails wirksam begegnet werden. Vor allem sind die jeweiligen Angestellten regelmäßig bezüglich Schad-Mails zu schulen und zu sensibilisieren. Die Angestellten müssen insbesondere wissen, welche Stellen beim Verantwortlichen in diesen Fällen zu informieren sind. Eine unverzügliche Benachrichtigung der betroffenen Personen trägt zur Eindämmung des Angriffs bei und ermöglicht es den betroffenen Personen in ihrer eigenen Sphäre Schutzmaßnahmen zu treffen.

2. Teil: Informationsfreiheitsbericht

1. Informationsfreiheit und Corona-Pandemie

Im **Jahr 2020** haben uns insgesamt **437 Eingaben** zum Informationsfreiheitsrecht erreicht. Im **Jahr 2019** waren es **373 Eingaben**. Auch der Bereich der Informationsfreiheit stand zum Teil unter dem Eindruck der Pandemie. Nicht erfasst davon sind die zahlreichen telefonischen Beratungen.

So konnten die für 2020 ins Auge gefassten Vortrags- und Fortbildungsveranstaltungen nicht stattfinden; alle diesbezüglichen Planungen und Vorhaben mussten vielmehr auf einen unbestimmten Zeitpunkt nach Ende der pandemiebedingten Einschränkungen verschoben werden.

Inhaltlich gab es die Corona-Pandemie betreffende Anträge auf Zugang zu bei öffentlichen Stellen vorhandenen Informationen, die etwa die Verhältnismäßigkeit von Maskenpflicht bzw. Kontaktverbot, die Crossborder-Taskforce Corona oder Pandemiepläne zum Gegenstand hatten und bei denen wir um Vermittlung gebeten wurden. Gerade in einer solchen besonderen Ausnahmesituation, die die Einschränkung von Grundrechten erfordert, ist es wichtig, demokratische Errungenschaften wie die Informationsfreiheit keinesfalls aus dem Blick zu verlieren oder hintenanzustellen, sondern es gilt vielmehr, sie nachdrücklich zu pflegen und zu fördern. Immerhin kann das Recht auf Informationszugang einen wichtigen Beitrag dazu leisten, dass Bürger*innen staatliche Eingriffsmaßnahmen besser nachvollziehen und deshalb eventuell auch leichter akzeptieren können.

In Pandemiezeiten, in denen personelle und sachliche Ressourcen oftmals verstärkt in speziellen Berei-

chen öffentlicher Stellen eingesetzt werden und deshalb ggf. in anderen Bereichen besonders knapp sind, können Informationszugangsanträge die auskunftspflichtigen Stellen in besonderen Einzelfällen allerdings ggf. schneller als sonst an den Rand ihrer Kapazitätsgrenzen bringen. In diesen Fällen werben wir für eine frühzeitige unmittelbare Kommunikation mit den Antragstellenden, etwa per Telefon. Im persönlichen Gespräch lässt sich vieles oft einfacher und schneller klären, sodass Nerven und Ressourcen auf beiden Seiten geschont werden. Soweit es hierbei einer Beratung und Vermittlung bedarf, steht die LDI NRW selbstverständlich gerne zur Verfügung. Nicht hinnehmbar wäre es dagegen, Informationsanträge gar nicht mehr zu bearbeiten oder die Bearbeitung unangemessen zu verschleppen.

2. Gerichtsentscheidungen zur Informationsfreiheit

2.1 Das OVG NRW sieht Parlamentarier*innen als nicht anspruchsberechtigt nach dem Informationsfreiheitsgesetz NRW (IFG NRW) an

In seinem Beschluss vom 22. Januar 2019 (Az. 15 A 247/18) bestätigt das OVG NRW die Entscheidung des Verwaltungsgerichts Düsseldorf, welches die Klage eines Landtagsabgeordneten auf Informationszugang zu Dokumenten einer Polizeidienststelle abgewiesen hatte. Nach Ansicht beider Gerichte ist der Kläger nicht als natürliche Person im Sinne von § 4 Abs. 1 IFG NRW anzusehen, sondern vielmehr als Mandatsträger, da er seinen Antrag auf Informationszugang auf einem offiziellen Briefbogen als Mitglied des Landtags verfasst und auch entsprechend unterzeichnet hatte. Als solchem stünden ihm ausschließlich organschaftliche Statusrechte zu, die ihm die Möglichkeit gäben, sich mit parlamentarischen Anfragen an die Landesregierung zu wenden. Das IFG NRW hingegen sehe nach seiner gesetzgeberischen Zielsetzung einen Anspruch auf Informationszugang für Bürger*innen vor. Nicht umfasst von dieser Zielsetzung seien Landtagsabgeordnete, da ihr Informationsrecht bereits auf der Grundlage der Landesverfassung gewährleistet werde.

Wir empfehlen in solchen Fällen, den Antrag als Privatperson zu stellen, um eventuellen Irritationen vorzubeugen.

2.2 Das OVG NRW äußert sich zum Tatbestandsmerkmal „Vorhandensein einer amtlichen Information“

In seinem Urteil vom 22. Mai 2019 (Az. 15 A 873/18) bekräftigt das OVG NRW seine bisherige Rechtsprechung zu der Frage, wann eine Information bei einer auskunftspflichtigen Stelle vorhanden ist. Danach genügt für das Vorhandensein einer amtlichen Information die tatsächliche räumliche Verfügbarkeit, und es kommt nicht auf die rechtliche Verfügungsbefugnis der Behörde in dem Sinne an, dass sie „aktenführende Stelle“ sein muss. Dies bedeutet, dass etwa Informationen, die sich nur zu vorübergehenden Zwecken bei der Stelle befinden, gleichfalls vom Informationsanspruch erfasst sind. Als maßgeblichen Zeitpunkt für das Vorhandensein der Information sieht das Gericht den Eingang des Antrags auf Informationszugang bei der auskunftspflichtigen Stelle an.

2.3 Soweit ein Gericht über seine Geschäftsverteilung berät und beschließt, fällt dies nicht in den Anwendungsbereich des IFG NRW

Gemäß § 2 Abs. 2 Satz 1 IFG NRW gilt das Gesetz für Gerichte nur, soweit sie Verwaltungsaufgaben wahrnehmen. Nach einem Beschluss des OVG NRW vom 13. Mai 2019 (Az. 15 E 324/19) unterfällt die Beratung der und die Beschlussfassung über die Geschäftsverteilung durch das Präsidium der richterlichen Selbstverwaltung und ist daher nicht als Verwaltungstätigkeit im Sinne von § 2 Abs. 2 IFG NRW zu qualifizieren. In der Begründung weist das Gericht darauf hin, dass diese Ausnahme vom Anwendungsbereich der Absicherung der richterlichen Unabhängigkeit diene.

In diesem Zusammenhang sei noch auf eine weitere Entscheidung des OVG NRW (Beschluss vom 14. Januar 2019, Az. 15 E 1027/18) verwiesen: Danach ist die Vorhaltung eines nicht mehr aktuellen Geschäftsverteilungsplans eines Landgerichts und dessen Zugänglichmachung an Dritte hingegen als Verwaltungstätigkeit im Sinne von § 2 Abs. 2 Satz 1 IFG NRW anzusehen.

2.4 Subventionen unterfallen nicht per se dem Betriebs- und Geschäftsgeheimnisschutz

Wie bereits zuvor in einer Entscheidung zum Umweltinformationsgesetz (Urteil vom 1. März 2011, Az. 8 A 3357/08) stellt das OVG NRW erneut fest, dass von der öffentlichen Hand gewährte Subventionen für sich genommen grundsätzlich keine Betriebs- oder Geschäftsgeheimnisse im Sinne von § 8 Satz 1 IFG NRW sind (Beschluss vom 14. November 2019, Az. 15 B 946/19).

Das Gericht führt in seiner Begründung aus, dass die Höhe der Subvention als solche kein exklusives kaufmännisches Wissen darstelle. Auch sei nicht ersichtlich, dass sich die Wettbewerbsposition des betroffenen Unternehmens im Falle eines Bekanntwerdens der Subvention verschlechtern würde. Der Förderungsbetrag allein besage nichts über die Stellung des Unternehmens am Markt.

2.5 OVG NRW zur Auskunftspflicht kommunaler Unternehmen

In einem aktuellen Urteil hat sich das OVG NRW mit dem Begriff der „Wahrnehmung einer öffentlich-rechtlichen Aufgabe“ in § 2 Abs. 4 IFG NRW befasst (Urteil vom 17. November 2020, Az. 15 A 4409/18). Nach Auffassung des Gerichts kann eine juristische Person

des Privatrechts auskunftspflichtig sein, ohne dass es dabei einer spezialgesetzlichen Aufgabenzuweisung an die öffentliche Hand bedarf. Das OVG NRW stellt vielmehr darauf ab, dass eine öffentlich-rechtliche Aufgabe durch eine Privatrechtsperson im Sinne von § 2 Abs. 4 IFG NRW wahrgenommen wird, wenn es sich um eine gemeinwohlerhebliche Aufgabe handelt, die im öffentlichen Recht wurzelt, diese Aufgabe durch einen zu ihrer Erfüllung berufenen Hoheitsträger auf ein Privatrechtssubjekt übertragen worden ist und dieses durch den Hoheitsträger beherrscht wird.

2.6 Grand départ – Vertraulichkeitsvereinbarung kann Informationsanspruch nicht einschränken

Ein Kläger hatte Informationszugang zu dem zwischen einer Stadt und einem Unternehmen anlässlich eines großen Radsportereignisses geschlossenen Vertrags beantragt. Die Stadt hatte den Antrag unter anderem mit Hinweis auf § 8 IFG NRW abgelehnt: Der Vertrag unterliege einer strengen Vertraulichkeitsvereinbarung und sei nur einem begrenzten Personenkreis bekannt. Auch habe das betroffene Unternehmen einer Veröffentlichung des Vertrages zum Schutz seiner wirtschaftlichen Interessen widersprochen. Das Verwaltungsgericht Düsseldorf gibt dem Kläger mit seinem Urteil vom 21. Oktober 2019, Az. 29 K 2845/18, recht und verpflichtet die beklagte Stadt, dem Kläger eine Ablichtung des Vertrags zu übersenden.

In Einklang mit vorangegangener OVG-Rechtsprechung (etwa Beschluss des OVG NRW vom 3. Mai 2010, Az. 13a F 31/09) stellt das Verwaltungsgericht Düsseldorf erneut fest, dass ein schützenswertes Geheimhaltungsinteresse insbesondere nicht aus einer

vertraglichen Vertraulichkeitsvereinbarung folgt: „Vertragliche Vereinbarungen vermögen als solche den gesetzlichen Auskunftsanspruch aus § 4 Abs. 1 IFG NRW nicht auszuschließen. Das IFG NRW sieht einen derartigen Ausschlusstatbestand nicht vor. Anderenfalls hätten es die in § 2 IFG NRW genannten Stellen in der Hand, den gesetzlich vorgeschriebenen Auskunftsanspruch – über die Ausnahmetatbestände hinaus – willkürlich einzuschränken. Dies stünde in evidentem Widerspruch zum Zweck des IFG NRW, die Transparenz behördlichen Handelns zu erhöhen und sicherzustellen.“ (Randnummer 56 der Entscheidung des Verwaltungsgerichts Düsseldorf).

Das OVG NRW weist in diesem Zusammenhang auf die Möglichkeit hin, dass die Offenbarung etwaiger Betriebs- oder Geschäftsgeheimnisse durch entsprechende Schwärzungen verhindert werden könnte.

3. Gesetzentwurf für ein Transparenzgesetz

Wiederholt hat die LDI NRW in den letzten Jahren die Forderung nach einer Weiterentwicklung des Informationsfreiheitsgesetz NRW (IFG NRW) zu einem Transparenzgesetz erhoben (siehe etwa 23. Bericht unter 2. und unter 16.2; 24. Bericht unter 2. Teil, 8.). Nun wurde von einer Oppositionsfraktion ein Gesetzentwurf (LT-Drs. 17/8722) in den Landtag eingebracht, der verstärkte Veröffentlichungspflichten vorsieht; leider ist dieser noch nicht ausgereift.

Die Initiative für ein „Gesetz zur Erleichterung des Zugangs zu amtlichen Informationen in Nordrhein-Westfalen“ ist grundsätzlich zu begrüßen, weil sie das wichtige Thema wieder auf die Tagesordnung bringt. Der Gesetzentwurf sieht allerdings eine Ergänzung des IFG NRW um ein paralleles Informationszugangsgesetz NRW vor, das etwa verstärkte Veröffentlichungspflichten sowie ein Informationsregister beinhaltet.

Warum jedoch ein Informationszugangsgesetz NRW neben dem bewährten IFG NRW stehen soll und wie die Gesetze sowie die von ihnen verbürgten Rechte im Einzelnen abzugrenzen wären, ist nicht nachzuvollziehen. Wichtig wäre es aus unserer Sicht vielmehr, das bestehende und bewährte IFG NRW zu einem modernen Transparenzgesetz mit verstärkten Veröffentlichungspflichten auszubauen. Mit dem neuen Gesetz hingegen wäre eine weitere Zersplitterung von Informations- und Transparenzvorschriften verbunden. Schon jetzt finden sich diesbezügliche Regelungen in verschiedenen Gesetzen (IFG NRW, Umweltinformationsgesetz NRW, E-Government-Gesetz NRW, Verbraucherinformationsgesetz), was den

Überblick und die Rechtsanwendung in der Praxis deutlich erschwert.

Zum Zeitpunkt des Redaktionsschlusses hatte das Parlament noch nicht über den Gesetzentwurf entschieden. So oder so bedauern wir, dass hier eine Chance verpasst wurde, die Forderungen der LDI NRW aufzugreifen und umzusetzen.

4. Keine Antwort ist keine Antwort – Informationspflichtige Stellen müssen der LDI NRW Rede und Antwort stehen

Öffentliche Stellen müssen ihrer gesetzlichen Auskunftspflicht gegenüber der LDI NRW nachkommen, damit wir unsere Aufgabe erfüllen können, das Recht auf Information sicherzustellen. Darüber hinaus können sie sich – ebenso wie die Bürger*innen – selbstverständlich auch an uns wenden, um sich in informationsfreiheitsrechtlicher Hinsicht beraten zu lassen.

Das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) sieht auch nach Einführung der Vollregelung in § 13 IFG NRW (siehe 24. Bericht unter 7.) weiterhin ein Vermittlungsverfahren vor. Der LDI NRW bleibt ihre Rolle als Ombudsstelle also erhalten. Dieses Verfahren hat sich in der Vergangenheit bereits bewährt, denn es ist wichtig, dass sich sowohl Antragstellende als auch informationspflichtige Stellen vertrauensvoll an uns wenden können, wenn sie in Sachen Informationsfreiheit eine Beratung oder Unterstützung benötigen.

Gleichzeitig sind öffentliche Stellen allerdings nach § 13 Abs. 4 Satz 2 Nr. 1 IFG NRW ebenfalls weiterhin

zur Kooperation mit der LDI NRW verpflichtet, soweit wir Auskunftsersuchen an sie zur Klärung von informationsfreiheitsrechtlichen Ansprüchen richten. Einige Stellen beachten diese gesetzliche Verpflichtung allerdings nicht immer und sogleich. Manchmal erhalten wir gar keine Rückmeldung auf Auskunftsersuchen. Dies erschwert unsere Arbeit und macht unsere Aufgabenwahrnehmung teilweise sogar unmöglich; in diesen Fällen wird das Informationszugangsverfahren deutlich verzögert. So werden bei uns Ressourcen gebunden, die dringend für andere Eingaben und Aufgaben benötigt würden.

Mittlerweile gehen wir zügiger dazu über, Beanstandungen wegen Nichterteilung der Auskunft auszusprechen, wenn sich die öffentliche Stelle ihrer Pflicht nach § 13 Abs. 4 IFG NRW entziehen möchte.

Damit die LDI NRW ihre Rolle als Ombudsstelle im Rahmen der Wahrnehmung von Informationsfreiheitsrechten ausüben kann, müssen informationspflichtige Stellen ihre gesetzliche Verpflichtung zur Auskunft zeitnah und umfassend erfüllen.

5. Was die öffentliche Stelle nichts angeht – Datenschutz gilt auch bei Informationsanträgen

Mit welcher E-Mail-Adresse Antragstellende ihre Anträge auf Informationszugang versenden, hat die informationspflichtige Stelle grundsätzlich nicht zu interessieren. Auf gar keinen Fall darf sie bei der Verwendung dienstlicher E-Mail-Adressen an Arbeitgeber*innen herantreten und dort die Antragstellenden „anschwärzen“.

Ein Antragsteller schilderte folgenden Fall: Unter seiner beruflichen E-Mail-Adresse hatte er sich mit einem Informationszugangsantrag an eine öffentliche Stelle gewandt. Diese leitete den Antrag unmittelbar an die Geschäftsleitung des Unternehmens weiter, bei dem der Antragsteller beschäftigt ist. Letzterer wurde weder zuvor informiert noch wäre er mit einer solchen Datenübermittlung einverstanden gewesen.

Die informationspflichtige Stelle begründete die Weiterleitung der E-Mail damit, dass sie anzweifele, dass der Antragsteller seine berufliche E-Mail-Adresse für private Anliegen nutzen dürfe. Doch warum sollte die Klärung dieser Frage und die damit verbundene Datenverarbeitung für die Bearbeitung des Informationszugangsantrags erforderlich sein? Misstrauen hinsichtlich der Einhaltung interner Regeln zur Nutzung des Internets am Arbeitsplatz ist in diesem Zusammenhang keinesfalls Sache der informationspflichtigen Stelle. Vielmehr spielt die Wahl der E-Mail-Adresse für die Antragstellung per E-Mail keine Rolle.

Da die Weiterleitung der personenbezogenen E-Mail ohne Einwilligung des Antragstellers erfolgte und auch ansonsten auf keine Rechtsgrundlage gestützt werden konnte, stellt das Vorgehen der öffentlichen Stelle einen Datenschutzverstoß dar.

Bei der Antragstellung nach dem Informationsfreiheitsgesetz NRW müssen sich Antragstellende darauf verlassen können, dass ihre Daten nicht unzulässig an Dritte weitergegeben werden.

6. Minderjährige sind antragsberechtigt

Das Informationsfreiheitsgesetz NRW (IFG NRW) sieht in § 4 Abs. 1 eine Antragsbefugnis für „jede natürliche Person“ vor. Hiernach sind auch Minderjährige antragsbefugt.

In dem zugrundeliegenden Fall hatte die Stadt den Informationszugangsantrag eines 15-Jährigen mit folgender Begründung abgelehnt: Mangels Antragsbefugnis sei der Antrag bereits unzulässig. Da der Antrag auf Informationszugang eine Verfahrenshandlung darstelle, müsse der Antragstellende handlungsfähig, also geschäftsfähig, sein. Diese Voraussetzung läge bei dem erst 15-Jährigen, der nur beschränkt geschäftsfähig sei, nicht vor. Daraufhin hat der Antragsteller fristwahrend Klage beim zuständigen Verwaltungsgericht erhoben, die aktuell noch anhängig ist.

Nach 4 Abs. 1 IFG NRW hat „jede natürliche Person“ grundsätzlich einen Anspruch auf Zugang zu den bei einer öffentlichen Stelle vorhandenen Informationen. Dem eindeutigen Wortlaut des Gesetzes lässt sich nicht entnehmen, dass ausschließlich Volljährige antragsbefugt sind. Auf die verfahrensrechtliche Handlungsfähigkeit, also Geschäftsfähigkeit, kann es daher hier nicht ankommen.

Unabhängig vom Ausgang des verwaltungsgerichtlichen Verfahrens gilt: Eine Demokratie sollte Jugendliche nicht ausschließen, sondern sie frühzeitig an gesellschaftlichen Entwicklungen und politischen Prozessen teilhaben lassen. Dies kann dazu beitragen, dass sie sich stärker mit dem rechtstaatlichen und demokratischen Gesellschaftssystem identifizieren und an wichtige Entscheidungen herangeführt werden. Wenn 14-Jährige eigenverantwortlich über ihre Konfessions- und Religionszugehörigkeit entscheiden sowie sich ggf. strafbar machen können, 15-Jährige Sozialleistungen beantragen und entgegennehmen können und 16-Jährige bei Kommunalwahlen wahlberechtigt sind, spricht alles dafür, Jugendlichen auch Gelegenheit zu geben, sich vorher zu informieren. Dafür bietet das IFG NRW die besten Voraussetzungen.

7. Gebührenrelevanter Verwaltungsaufwand

Die Gewährung von Informationszugang in großem Umfang rechtfertigt nicht immer und ohne Weiteres hohe Gebührenforderungen, wie sich bei einem Informationszugang zum Inhalt von vier Aktenordnern zeigte.

Im Rahmen eines Antrags auf Informationszugang zur Errichtung und zum Betrieb von Windkraftanlagen kam es zu Streitigkeiten bezüglich der Höhe der zur fordernden Gebühren. Auch wenn es unter anderem um Umweltinformationen ging, war vorliegend das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) anzuwenden.

Der informationspflichtige Kreis stellte dem Antragsteller für den Informationszugang zu vier Aktenordnern einen Gebührenbescheid über 300 Euro zu. Bei der Höhe der Gebühr berief er sich auf die Einstufung in eine Tarifstelle zur Verwaltungsgebührenordnung des IFG NRW, die einen Gebührenrahmen von 10 bis 500 Euro vorsieht. Die Höhe der Gebühr begründete er mit dem angefallenen Zeitaufwand und verwies auf die Stundensätze, die im Rahmen eines Runderlasses des Innenministeriums NRW vorgegeben werden. Eine genaue Erläuterung, wie der Betrag zustande kam, fehlte jedoch.

Da der Antragsteller den Kreis vorab ausdrücklich darauf hingewiesen hatte, dass er für diesen Zugang keinesfalls mit einer Gebühr von mehr als 75 Euro rechne, und er nicht zuvor angehört worden war, wandte er sich zwecks Vermittlung an die LDI NRW. Er verwies darauf, dass eine Schwärzung von Betriebs- und Geschäftsgeheimnissen nicht mit dem berechneten Aufwand verbunden sein könne, und vertrat die Auffassung, dass die Höhe der Gebühr eine abschreckende Wirkung erzielen solle.

Im Rahmen eines Auskunftsersuchens baten wir den Kreis um Darlegung, wie groß der Umfang der bewilligten Informationen war und wieviel Stunden für die Bearbeitung des Informationszugangs benötigt wurden. Die Stellungnahme des Kreises erreichte uns wegen eines dortigen Zustellfehlers sehr verspätet, so dass keine zeitnahe Stellungnahme der LDI NRW gegenüber den Beteiligten erfolgen konnte. Der Antragsteller sah sich deshalb gezwungen, gegen den Gebührenbescheid fristwahrend Klage beim Verwaltungsgericht zu erheben.

Neun Wochen nachdem die LDI NRW das Auskunftsersuchen per E-Mail und Post an den Kreis versandt hatte, erreichte uns dessen Stellungnahme. Der Kreis begründete seinen Aufwand damit, dass für die Sichtung und Prüfung von insgesamt vier Aktenordnern ein Aufwand von fünf Arbeitsstunden entstanden sei. Er verwies darauf, dass Verfahren zur Errichtung von Windkraftanlagen im Vergleich zu anderen Verwaltungsvorgängen nach dem Bundesimmissionsschutzgesetz grundsätzlich sehr umfangreich seien. Daher sei nach summarischer Betrachtung eine Gebühr im mittleren Bereich des Gebührenrahmens nicht unangemessen.

Das Verwaltungsgericht gab sich mit der Begründung des Kreises jedoch nicht zufrieden, gab dem Antragsteller Recht und reduzierte die Gebühr auf 50 Euro. Es begründete seine Entscheidung unter anderem damit, dass der nachträglich pauschal angegebene Prüfungsaufwand von fünf Zeitstunden ohne Konkretisierungen und Erläuterungen nicht nachvollziehbar sei. Der Gebührenbescheid lasse nicht hinreichend erkennen, wie der Betrag in Höhe von 300 Euro konkret ermittelt wurde und welche Erwägungen zugrunde gelegt wurden. Weder sei der genaue Prüfungsaufwand im Bescheid bezeichnet noch sei erkennbar, welcher konkrete Zeitaufwand von Beschäftigten aus welcher Laufbahngruppe im Einzelnen berücksichtigt wurde (siehe hierzu Urteil des Verwaltungsgerichts Arnsberg vom 4. Mai 2020, Az. 11 K 1503/19).

Verwaltungsaufwand, der Gebührenforderungen rechtfertigen soll, ist von der informationspflichtigen Stelle stets konkret darzulegen und nachvollziehbar zu begründen.

8. Kriegsgräberlisten – Informationszugang ohne Verletzung des Datenschutzes

Die umfassende Wahrung von Datenschutzbelangen ist auch im Bereich der Informationsfreiheit wichtig. Nicht immer, wenn es um die Offenlegung von Namen geht, steht dem jedoch der Datenschutz entgegen.

In dem konkreten Fall lehnte die Stadt den Antrag auf Einsichtnahme in ihre Kriegsgräberlisten mit der Begründung ab, der Offenbarung stünde der Schutz personenbezogener Daten entgegen. Daraufhin wandte sich der Antragsteller an die LDI NRW.

Wir machten die Stadt auf Folgendes aufmerksam: Der Schutz personenbezogener Daten umfasst ausschließlich Angaben zu lebenden, nicht jedoch bereits verstorbenen Personen. Die in den Kriegsgräberlisten enthaltenen Daten der Verstorbenen sind deshalb nicht vom Schutzbereich des § 9 Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) für personenbezogene Daten umfasst. Dies ergibt sich zum einen aus der Datenschutz-Grundverordnung (DS-GVO), deren Definition des Begriffs „personenbezogene Daten“ auch dem IFG NRW zugrunde zu legen ist. In Erwägungsgrund 27 DS-GVO heißt es ausdrücklich: „Diese Verordnung gilt nicht für die personenbezogenen Daten Verstorbener.“ Zum anderen gibt es zu dieser Frage eindeutige Rechtsprechung des Bundesverwaltungsgerichts, welches etwa in seinem Urteil vom 29. Juni 2017, Az. 7 C 24.15, ausführt, „dass der Begriff der personenbezogenen Daten Verstorbene grundsätzlich nicht erfasst“.

Dass im vorliegenden Fall – wie die Stadt zunächst vorgetragen hatte – auch Daten von lebenden Angehörigen betroffen waren, ließ sich nicht feststellen.

Trotz dieser eindeutigen Rechtslage brauchte es noch einige Überzeugungsarbeit seitens der LDI NRW, bis die Stadt dem Antragsteller – fünf Monate nach unserem ersten Tätigwerden – endlich die gewünschte Einsichtnahme gewährte.

Ein falsch verstandener Datenschutz darf nicht dazu führen, dass berechtigte Informationszugangsanträge abgelehnt werden.

9. Informationszugang zu „externen Beratungskosten“

Bedient sich die öffentliche Hand externer Beratungsunternehmen, stellen sich häufig Fragen zu den Beteiligten und den Kosten. Hier kommt das Informationsfreiheitsgesetz ins Spiel.

Wenn öffentliche Stellen externe Beratungsunternehmen und deren Fachkunde in Anspruch nehmen, mag es hierfür gute Gründe geben. Häufig wird eine solche Inanspruchnahme allerdings von öffentlichen Diskussionen über die Verwendung von Steuermitteln begleitet, und nicht selten werden diesbezüglich Anträge auf Informationszugang gestellt. Umso wichtiger ist es, in diesem Bereich in die Transparenzoffensive zu gehen. Schließlich fördert es die Demokratie und Teilhabe, wenn Bürger*innen die Politik sowie auch die Steuerausgaben durch Nachfragen kontrollieren.

In einem konkreten Fall hatte der Antragsteller eine Stadt um Auskunft zu den Kosten für externe Beratungen gebeten, und es war ein langer Weg vom Antrag bis zum Informationszugang: Zunächst war der Stadt der Begriff des „externen Dienstleisters“ zu unbestimmt, dann berief sie sich darauf, keine vertraulichen Daten weitergeben und nicht gegen den ausdrücklichen Willen der Dienstleistenden handeln zu dürfen. Dabei können selbst vertragliche Vertraulichkeitsvereinbarungen den gesetzlichen Auskunftsanspruch aus § 4 Abs. 1 Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) nicht ausschließen (vgl. Verwaltungsgericht Düsseldorf, Urteil vom 21. Oktober 2019, Az. 29 K 2845/18).

Nach einem sehr ausführlichen Schriftwechsel und einigen Telefonaten konnte die LDI NRW die Stadt erfreulicherweise zum Umdenken bewegen und dem Antragsteller somit die gewünschte Information verschaffen.

Allein der entgegenstehende Wille der beauftragten Unternehmen oder eine im Vertrag enthaltene Vertraulichkeitsvereinbarung rechtfertigen keine Verweigerung der Offenlegung von Beratungskosten. Ein transparenter Umgang mit Beratungsverträgen ist für das Vertrauen der Bürger*innen in die Politik und für die Nachvollziehbarkeit staatlichen Handelns wichtig. Mit Hilfe des IFG NRW kann hier eine demokratische Kontrollfunktion erfüllt werden.

10. 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.

11. Informationszugang im Zusammenhang mit kommunalen Abgaben

Das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) soll staatliches Handeln transparenter machen – auch und gerade in solchen Fällen, in denen die Offenlegung mögliche Defizite ans Tageslicht bringen könnte.

Ein Bürger hatte die Information beantragt, wie viele Beherbergungsbetriebe – hierzu zählen laut städtischer Satzung Hotels, Gasthöfe, Pensionen, Privatzimmer, Jugendherbergen, Ferienwohnungen, Motels sowie Campingplätze, Schiffe und ähnliche Einrichtungen – im Jahr 2018 auf die korrekte Umsetzung der Kulturförderabgabe geprüft worden waren. Diese Abgabe ist eine per Satzung geregelte Steuer, die bei

entgeltlichen Beherbergungen im Stadtgebiet erhoben wird und die allgemein auch als „Bettensteuer“ bekannt ist.

Die Stadt lehnte den Antrag zunächst mit verschiedenen Begründungen ab: Die Information beziehe sich auf den durch § 7 Abs. 2 Buchstabe a IFG NRW geschützten Willensbildungsprozess, enthalte personenbezogene Daten im Sinne des § 9 IFG NRW und unterliege zugleich dem durch die Abgabenordnung geschützten Steuergeheimnis.

Wir entgegneten, dass die schlichte Anzahl der Prüfungen weder Rückschlüsse auf einen internen Willensbildungsprozess noch auf personenbezogene Daten zulasse. Auch das Steuergeheimnis sei nicht tangiert, da allein die Anzahl der Prüfungen keine Hinweise auf steuerliche Verhältnisse einzelner Hotelbetriebe gebe.

Am Ende des ausgiebigen Schriftwechsels mit der Stadt erhielten wir – und damit auch der Antragsteller – die recht einfache Antwort auf die Anfrage: Im Jahr 2018 sei in nur vier Fällen überprüft worden, ob die sog. Bettensteuer korrekt umgesetzt worden war.

Dieser Fall ist ein gutes Beispiel dafür, dass das IFG NRW seinen Zweck, staatliches Handeln zu kontrollieren, erreicht. Leider bedarf es oft noch hartnäckiger Bürger*innen und der Unterstützung der LDI NRW, um Verwaltungshandeln mittels IFG-Antrags transparent zu machen.

12. Bilder einer Ausstellung

Handelt es sich bei einem städtischen Museum um eine Forschungseinrichtung? Wenn und soweit diese Frage im Einzelfall zu bejahen ist, ist das Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) aufgrund der Bereichsausnahme in § 2 Abs. 3 IFG NRW nicht anwendbar. Genau hierum ging es in einem Fall, über den letztlich zwei Gerichte zu befinden hatten. Rechtsklarheit gibt es trotzdem nicht.

Die Antragsteller hatten sich mit einem Informationszugangsantrag an ein städtisches Museum gewandt. Sie begehrten die Vorlage von Gutachten (Provenienzrecherche und -begutachtung), die in Verbindung mit unter Fälschungsverdacht stehenden Kunstwerken erstellt worden waren. Diesen Antrag lehnte die Stadt zunächst ohne Begründung ab.

Das Vermittlungsersuchen durch die LDI NRW bewirkte immerhin, dass die Stadt – drei Monate nach dem Antrag – einen ablehnenden Bescheid erließ. Die Ablehnung begründete sie unter anderem allgemein damit, dass das Museum als Forschungseinrichtung nicht dem Anwendungsbereich des IFG NRW unterfalle.

Dem hielten wir entgegen, dass eine öffentliche Stelle gerade zu Forschungszwecken gegründet sein muss, damit sie als Forschungseinrichtung im Sinne des § 2 Abs. 3 IFG NRW qualifiziert werden kann. Zudem müsse ihre Tätigkeit zumindest hauptsächlich darauf ausgerichtet sein, Forschung zu betreiben. Beide Voraussetzungen waren nach unserer Auffassung bei dem in Rede stehenden Museum nicht erfüllt. Weder war offensichtlich, dass der Gründungszweck explizit

die Forschung umfasst, noch war anhand aktueller Forschungsprojekte ein entsprechender Schwerpunkt erkennbar. Auch die Ausführungen der Stadt enthielten hierzu keine konkreten sachdienlichen Hinweise.

Gegen den Ablehnungsbescheid gingen die Antragsteller im Wege eines einstweiligen Anordnungsverfahrens vor. Das angerufene Verwaltungsgericht (Verwaltungsgericht Köln, Beschluss vom 9. September 2020, Az. 13 L 1463/29) war ebenfalls der Auffassung, dass es sich bei dem Museum um keine Forschungseinrichtung handelt, da sein Hauptzweck nicht die Forschung sei. Die Regelung des § 2 Abs. 3 IFG NRW sei eng auszulegen. Es verpflichtete die Stadt deshalb, den Antragstellern Zugang zu den begehrten Informationen und Gutachten zu gewähren.

Die dagegen gerichtete Beschwerde der Stadt beim OVG NRW (Beschluss vom 16. September 2020, Az. 15 B 1357/20) hatte allerdings Erfolg. Das Gericht sah es als zweifelhaft an, dass der Informationsanspruch bestehe. Vieles spreche dafür, das Museum als Forschungseinrichtung im Sinne des § 2 Abs. 3 IFG NRW anzusehen. So verfüge das Museum über wissenschaftliches Personal und betreibe verschiedene Forschungsprojekte. Zudem dürften nach Auffassung des OVG NRW die Provenienzrecherche und -begutachtung dem Begriff der Forschung zuzurechnen sein. Nach einem weiter gefassten Verständnis des Begriffs der Forschungseinrichtung könnte es ausreichend sein, dass sich das Museum zwar nicht in der Hauptsache, aber jedenfalls auch der Forschung widme.

Rechtsklarheit ist damit zu unserem Bedauern gleichwohl noch nicht geschaffen. Derartige Entscheidun-

gen im Eilverfahren ermöglichen nur vorläufige Sicherungen oder Regelungen auf der Basis einer summarischen Prüfung. Da die Antragsteller letztlich darauf verzichteten, das Hauptsacheverfahren weiter zu verfolgen, wird es kein Urteil in dieser Sache geben.

Ob und inwieweit sich Museen auf die Bereichsausnahme des § 2 Abs. 3 IFG NRW berufen können, ist nicht abschließend geklärt und wird wohl auch zukünftig in jedem Einzelfall unter Berücksichtigung aller konkreten Umstände zu entscheiden sein.

13. Ablehnung eines Informationsantrags wegen Geheimnisses? – Nachgefragt und nachgehakt!

Von den Ablehnungsgründen des Informationsfreiheitsgesetzes Nordrhein-Westfalen (IFG NRW) stellt insbesondere der „Schutz von Betriebs- und Geschäftsgeheimnissen“ im Sinne des § 8 IFG NRW öffentliche Stellen immer wieder vor Herausforderungen.

Ein Kreis hatte mit der kreiseigenen Vermögensverwaltungsgesellschaft einen Darlehensvertrag geschlossen, um dieser die Modernisierung eines bekannten Ausflugsziels inklusive Ausflugslokals zu ermöglichen. Diesen Vertrag einschließlich des vereinbarten Zinssatzes wollte ein Antragsteller einsehen und richtete deshalb einen entsprechenden Antrag an den Kreis.

Der Kreis gewährte ihm zwar den Zugang zu dem Darlehensvertrag, allerdings zunächst nur unter Schwärzung des Zinssatzes. Diese Schwärzung wurde mit dem Hinweis auf § 8 IFG NRW, dem

Schutz von Betriebs- und Geschäftsgeheimnissen, begründet. Nach § 8 Abs. 1 Satz 1 IFG NRW ist der Antrag auf Informationszugang abzulehnen, soweit durch die Übermittlung der Information ein Betriebs- oder Geschäftsgeheimnis offenbart wird und dadurch ein wirtschaftlicher Schaden entstehen würde. Der Kreis argumentierte, dass nicht ausgeschlossen werden könne, dass es einen wirtschaftlichen Schaden durch die Offenlegung des Zinssatzes gebe.

Diese allgemeine Begründung reicht zur Ablehnung nach § 8 IFG NRW aber nicht aus. Ein möglicher wirtschaftlicher Schaden ist erst dann anzunehmen, wenn die in Anspruch genommene öffentliche Stelle konkret und substantiiert darlegen kann, dass sich die Wettbewerbssituation einer Vertragspartei durch die Offenbarung des Betriebs- oder Geschäftsgeheimnisses nachhaltig verschlechtern wird (vgl. OVG NRW, Urteil vom 2. Juni 2015, Az. 15 A 1997/12). Maßgeblich ist dabei, inwieweit mögliche Mitbewerber*innen tatsächlich einen wirtschaftlichen Nutzen aus der Offenlegung der begehrten Information ziehen können.

Dies konnte der Kreis nicht vortragen. Insbesondere konnte er nicht begründen, wem durch die Offenlegung des konkreten Zinssatzes ein wirtschaftlicher Schaden entstehen könnte bzw. inwieweit dies die Wettbewerbssituation einer Vertragspartei nachteilig im Sinne der Entstehung eines wirtschaftlichen Schadens hätte beeinflussen können.

Eine weitere Beratung unsererseits führte schließlich dazu, dass der Kreis den begehrten Zinssatz offenlegte. Der Antragsteller konnte sich mit dieser Information ein eigenes Bild von der Lage machen, und dies war schließlich der Anlass seines Antrags auf Informationszugang gewesen.

Ohne die Unterstützung der LDI NRW hätte der Antragsteller die begehrte Information womöglich nur auf dem Klageweg erhalten. Die informationspflichtige Stelle ließ sich aber von uns beraten und bewilligte schließlich den Antrag auf Informationszugang.

14. Es werde Licht, aber der Plan hierzu bleibt im Dunkeln

Es gibt vieles, was unter den Anwendungsbereich des Informationsfreiheitsgesetzes NRW (IFG NRW) fällt. Dies gilt auch für den Straßenbeleuchtungsplan einer Stadt, und zwar selbst dann, wenn die Beleuchtung von einem Energieunternehmen betrieben wird.

Ein Antragsteller meldet regelmäßig defekte Straßenbeleuchtungen in seiner Umgebung bei der Stadt. Das Meldeverfahren dieser Kommune sieht vor, dass defekte Leuchten an einer Straße, einem Geh- oder Radweg sowie beschädigte Leuchtenmasten oder beschädigtes Leuchtenglas mit Angabe der Straße mitgeteilt werden sollen. Die Stadt beauftragt sodann das zuständige Energieversorgungsunternehmen mit der Instandsetzung.

Der Antragsteller hält dieses Meldeverfahren für bürgerunfreundlich und kompliziert, denn nicht immer kann die defekte Beleuchtung anhand dieser Angaben eindeutig identifiziert werden. Ihn stört unter anderem, dass er einzelne Beleuchtungen nicht konkret, sondern nur ihren ungefähren Standort benennen kann. Deshalb beantragte er bei dem Energieversorgungsunternehmen den Zugang zu der Karte des gesamten Beleuchtungsplans seiner Stadt. Da er von

dem Unternehmen nur den Hinweis auf das ihm bereits bekannte Meldeportal und keine Antwort auf seinen IFG-Antrag erhielt, wandte er sich an die LDI NRW mit der Bitte um Vermittlung.

Wie immer ist in solchen Fällen zweistufig zu prüfen, ob eine Stelle nach Maßgabe des IFG NRW überhaupt informationspflichtig ist und – wenn ja – ob dem geltend gemachten IFG-Anspruch Ausschlussgründe entgegenstehen.

Bei dem Energieversorgungsunternehmen handelt es sich um eine Aktiengesellschaft. Für ein solches Unternehmen des Privatrechts ist der Anwendungsbereich des IFG NRW nur eröffnet, soweit es eine öffentlich-rechtliche Aufgabe wahrnimmt (vgl. § 2 Abs. 4 IFG NRW). Das ist nach einer schon seit Langem vorherrschenden Auffassung der Fall, wenn es sich um die Erfüllung einer gesetzlich zugewiesenen Pflichtaufgabe handelt. Eine konkrete rechtliche Regelung zur Straßenbeleuchtung gibt es etwa für die Beleuchtung von Fußgängerüberwegen: Gemäß § 45 Abs. 5 Satz 2 der Straßenverkehrsordnung ist der Straßenbaulastträger zur Beleuchtung von Fußgängerüberwegen verpflichtet. Straßenbaulastträger innerhalb geschlossener Ortslagen ist in aller Regel die jeweilige Kommune (vgl. § 3 Abs. 3 Satz 3 Straßen- und Wegegesetz NRW). Die grundsätzliche Pflicht der Kommunen zur Beleuchtung von Straßen und Wegen leitet sich aus ihrer Funktion als Straßenbaulastträgerinnen und ihrer Verkehrssicherungspflicht ab. Somit zählt die vom Energieunternehmen betriebene Straßenbeleuchtung zu den öffentlich-rechtlichen Aufgaben. Das IFG NRW ist also anwendbar. Zu demselben Ergebnis der Anwendbarkeit würde im

Übrigen die nunmehr vom OVG NRW zugrunde gelegte Definition der öffentlich-rechtlichen Aufgabe im Sinne des § 2 Abs. 4 IFG NRW führen. Siehe hierzu unter 2.5. Wir wandten uns deshalb mit einem Auskunftsersuchen an das Unternehmen.

Der Antrag wurde jedoch abgelehnt: Der Beleuchtungsplan enthalte auch Daten kritischer Infrastruktur. Ein Bekanntwerden dieser Daten könne dazu führen, dass die öffentliche Sicherheit im Sinne des § 6 Satz 1 Buchstabe a IFG NRW beeinträchtigt würde. Betreiber*innen kritischer Infrastrukturen sind verpflichtet, angemessene technische Vorkehrungen zur Vermeidung von Störungen zu treffen (§ 8a Abs. 1 des Gesetzes über das Bundesamt für Sicherheit und Informationstechnik – BSIG). Ausschnitte des Beleuchtungsplans würden nur dann zur Verfügung gestellt, wenn eine defekte Beleuchtung nicht eindeutig lokalisiert werden könne. Jedoch erfolge dies nur unter Ausschluss der kritischen Daten. Hierbei beruft sich das Unternehmen auf die Verordnung zur Bestimmung kritischer Infrastrukturen nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-KritisV), so dass nicht die gesamte Karte herausgegeben werden könne. In dieser Verordnung werde die Vorgabe in § 10 Abs. 1 Satz 1 des BSIG umgesetzt, wonach die Bewertung einer Infrastruktur als kritisch nach einer vorgegebenen Methodik zu erfolgen habe. Die Tatsache, dass eine kritische Infrastruktur in § 2 Abs. 1 BSI-KritisV erwähnt ist, stelle bereits eine ausreichende Begründung nach § 6 Satz 1 Buchstabe a IFG NRW dar. Allein der Umstand, dass die Versorgung der Allgemeinheit mit Elektrizität (Stromversorgung) in der BSI-KritisV auf-

geführt werde, führe dazu, dass der Beleuchtungsplan mit den kritischen Infrastrukturen nicht in der Gesamtheit bekannt gegeben werden könne.

Dass es auch anders geht, zeigt die Stadt Berlin, die im Geoportal ihren Beleuchtungsplan veröffentlicht hat. Allerdings beinhaltet dieser Plan auch keine Daten kritischer Infrastruktur. In unserem Fall hätte das Unternehmen seinen Plan um diese Daten schwärzen müssen, was jedoch einen unverhältnismäßigen Aufwand erzeugt hätte. Dies hätte einer Aufbereitung von Daten und damit einer Neugenerierung entsprochen und wäre damit nicht mehr vom Informationszugangsanspruch nach dem IFG NRW gedeckt gewesen. Das Unternehmen teilte schließlich mit, dass es an einer Optimierung des Meldeportals für defekte Straßenleuchten arbeite. Vielleicht wird dann doch bald auch der Beleuchtungsplan in seiner Gesamtheit veröffentlicht.

Der Anwendungsbereich des IFG NRW erstreckt sich in vielen Fällen auf private Unternehmen, auch wenn das nicht immer auf den ersten Blick erkennbar ist. Ob der geltend gemachte Informationszugangsanspruch gegen ein solches Unternehmen tatsächlich besteht, muss anhand der im IFG NRW festgeschriebenen Voraussetzungen im Einzelnen geprüft werden.

15. Frist zur Informationsgewährung

Bei umfangreichen Informationszugangsanträgen ist es gelegentlich aus sachlichen Gründen nicht möglich, die vom Gesetzgeber vorgesehene Monatsfrist für die Bearbeitung einzuhalten. Behörden dürfen diese Frist aber nicht nach Belieben überschreiten. Insbesondere dürfen sie nicht einfach abwarten, bis ein Vorgang, auf den sich der Antrag bezieht, insgesamt abgeschlossen ist.

Bürger*innen wenden sich an uns, wenn sie keine oder aber eine aus ihrer Sicht nicht befriedigende Antwort von der informationspflichtigen Stelle erhalten. Im nachfolgend geschilderten Fall begehrte ein Antragsteller den Zugang zu Unterlagen der Genehmigung eines dreitägigen Stadtteilfestes. Der Antrag wurde gestellt, nachdem das Fest schon begonnen hatte, also eine Genehmigung bereits vorlag.

Dennoch gewährte die Stadt den Zugang zu den Unterlagen erst fast ein halbes Jahr später und auch erst, nachdem wir uns mit einem Auskunftsersuchen und zwei weiteren Erinnerungen eingeschaltet hatten. Sie teilte mit, dass „der Vorgang“ erst vier Monate nach Ablauf des Stadtteilfestes abgeschlossen und dies zunächst abgewartet worden sei. Dieses Zuwarten sei auch im Interesse des Antragstellers gewesen, der so umfangreichere Unterlagen erhalten habe. Dem Antragsteller wurden mehr als 60 Seiten ausgehändigt, auf denen teilweise personenbezogene Daten geschwärzt werden mussten.

Der Informationszugang erfolgte viel zu spät. Nach § 5 Abs. 2 Informationsfreiheitsgesetz NRW (IFG NRW) sollen die beantragten Informationen unver-

züglich, spätestens innerhalb eines Monats nach Antragstellung, zugänglich gemacht werden. Ein Informationszugangsantrag umfasst zudem nur solche Unterlagen, die zum Zeitpunkt der Antragstellung bereits vorhanden sind (vgl. §§ 4 Abs. 1, 5 Abs. 1 Satz 1 IFG NRW). Vorliegend war etwa ein Viertel der nach dem halben Jahr zur Verfügung gestellten Unterlagen jedoch erst nach der Antragstellung erstellt worden und überdies auch gar nicht unmittelbar den Genehmigungsunterlagen zuzuordnen.

Im konkreten Fall erfolgte eine erste inhaltliche Reaktion erst zwei Monate nach dem Auskunftsersuchen der LDI NRW. Die Stadt verwies darauf, dass verschiedene Fachämter beteiligt werden mussten. Das ist verständlich, entbindet jedoch nicht von der Einhaltung der gesetzlichen Monatsfrist.

Die Einhaltung der gesetzlichen Monatsfrist steht nicht im Belieben der informationspflichtigen Stelle.

16. Informationen von heute dürfen nicht zu Informationen von gestern werden

Viele öffentliche Stellen schließen mit Unternehmen Verträge, die grundsätzlich dem Anwendungsbereich des Informationsfreiheitsgesetzes Nordrhein-Westfalen (IFG NRW) unterfallen. Dabei sollten die auskunftspflichtigen Stellen nicht von vornherein davon ausgehen, dass die Vertragspartner*innen Bedenken gegen die Offenlegung dieser Vereinbarung haben. In einem Fall zeigte sich der Vertragspartner, ein weltweit tätiges Unternehmen, zur Offenlegung sogar eher bereit als seine kommunale Vertragspartnerin.

Die Stadt hatte eine „Absichtserklärung“ mit einem international tätigen Anbieter von Informations- und Kommunikationstechnik geschlossen. Diese Erklärung dient gemäß der Vereinbarung ausschließlich „Diskussionszwecken“, ist nicht bindend und begründet keine rechtlichen Ansprüche oder Verpflichtungen. Durch eine Pressemitteilung wurde das Interesse der Öffentlichkeit geweckt, insbesondere auch eines Bürgers, der bei der Stadt einen Antrag auf Informationszugang zu dieser Erklärung stellte.

Die Stadt reagierte zunächst nicht auf diesen Antrag. Erst als sich die LDI NRW im Rahmen eines Auskunftsersuchens einschaltete, lehnte sie den Zugang zu diesem Dokument ab, und zwar zuerst unter Hinweis auf § 8 IFG NRW, den Schutz von Betriebs- und Geschäftsgeheimnissen. Danach verwies sie noch auf eine Vertraulichkeitsvereinbarung mit dem Unternehmen. Der Antragsteller erhielt zehn Monate nach Antragstellung einen Ablehnungsbescheid.

Als bei der Stadt ein weiterer Antrag einer anderen Person auf Zugang zu der Absichtserklärung gestellt wurde, entschied sie sich, dem Unternehmen zumindest einmal Gelegenheit zur Stellungnahme zu geben. Daraufhin erklärte sich das Unternehmen mit dem Zugang einverstanden, allerdings unter der Voraussetzung, dass der Antragsteller ein berechtigtes Interesse an der Übersendung nachweise und das Dokument nicht veröffentliche oder an Dritte weitergebe. Dass der Informationsanspruch nach dem IFG NRW unabhängig von einem Interesse der/des Antragstellenden erfüllt werden muss und sie/er im Anschluss an den Informationszugang nach Belieben mit der Information verfahren kann, war dem Unternehmen vermutlich nicht bekannt.

Offenbar fand nun allerdings bei der Stadt ein Umdenken statt, denn sie fragte das Unternehmen erneut. Schließlich entschied sich die Stadt sogar, die Absichtserklärung aus Gründen der Transparenz auf ihrer Internetseite zu veröffentlichen. Es zeigte sich, dass das in Rede stehende Dokument tatsächlich keine Betriebs- und Geschäftsgeheimnisse enthielt.

Weshalb die Stadt den Zugang so lange verweigert hatte, ist im Nachhinein nicht nachvollziehbar. Es mag an den vertraglichen Vertraulichkeitsvereinbarungen gelegen haben, die jedoch nach Maßgabe des IFG NRW keinen Ausschlussgrund darstellen. Zumindest aber hat dieses IFG-Verfahren dazu geführt, dass die Stadt weitere Anfragen zu diesem Themenkomplex fristgerecht beantwortete.

Wir empfehlen den informationspflichtigen Stellen bereits seit vielen Jahren, ihre Vertragspartner*innen im Vorfeld von Vertragsabschlüssen ausdrücklich auf

das IFG NRW und die daraus resultierenden Informationspflichten hinzuweisen, um spätere Irritationen, Auseinandersetzungen und Verwerfungen zu vermeiden. Bei IFG-Anträgen auf Zugang zu Verträgen der öffentlichen Hand sind nicht etwa vertragliche Verschwiegenheitsvereinbarungen, sondern ausschließlich die vom Gesetzgeber im IFG NRW geregelten Verweigerungsgründe maßgeblich.

Werden Informationen proaktiv durch öffentliche Stellen veröffentlicht, erübrigt sich später die Bearbeitung einzelner IFG-Anträge. Das erhöht die Transparenz für die interessierte Öffentlichkeit und erspart den informationspflichtigen Stellen zugleich Kosten, Zeit und Mühen.

Anhang zum Datenschutzbericht

Veröffentlichungen der Datenschutzkonferenz 2020

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 2020

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

- **03.04.2020 – Datenschutz-Grundsätze bei der Bewältigung der Corona-Pandemie**

  Die Corona-Pandemie stellt eine der größten Bewährungsproben für die europäischen Gesellschaften seit Jahrzehnten dar. Alle Mitgliedstaaten der Europäischen Union haben gegenwärtig extreme Herausforderungen zu bewältigen, um die Gesundheit ihrer Bevölkerung zu gewährleisten. Angesichts der bereits getroffenen Maßnahmen wird gleichzeitig der Wert der Freiheitsrechte erlebbar, zu denen auch das Grundrecht auf informationelle Selbstbestimmung gehört.

  Für die Stabilität von Staat und Gesellschaft ist es in dieser Lage unverzichtbar, dass sich die Bürgerinnen und Bürger darauf verlassen können, dass Freiheitsrechte wie das Grundrecht auf informationelle Selbstbestimmung nur so weit und so lange eingeschränkt werden, wie es zwingend erforderlich und angemessen ist, um die Gesundheit der Bevölkerung wirksam zu schützen. Einschneidende Regelungen müssen umkehrbar und eng befristet sein und von den Gesetzgebern und nicht allein durch die Exekutive verantwortet werden.

Was die Rechtfertigung der Verarbeitung personenbezogener Daten nach Maßgabe der europäischen Datenschutz-Grundverordnung anbelangt, stellt sie insbesondere in ihrem Artikel 5 **europaweit einheitliche Grundsätze** bereit, die als Leitfaden für staatliches Handeln auch gerade in Krisenzeiten dienen können, einer effektiven Bekämpfung der Corona-Pandemie nicht entgegenstehen und zugleich einen grundrechtsschonenden Umgang mit personenbezogenen Daten gewährleisten.

Im Zusammenhang mit der Bewältigung der Corona-Krise weist die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder daher auf **folgende wesentliche Rechtmäßigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten** hin:

▪ Krisenzeiten ändern nichts daran, dass die **Verarbeitung** personenbezogener Daten stets auf einer **gesetzlichen Grundlage** zu erfolgen hat. Das bedingt insbesondere, dass die mit einer Verarbeitung verfolgten Zwecke möglichst genau bezeichnet werden.

▪ Die **geplanten Maßnahmen** müssen zudem kritisch auf ihre **Eignung** überprüft werden, um etwa Infektionen zu erfassen, infizierte Personen zu behandeln oder Neuinfektionen zu verhindern. So kann es in Notfalllagen beispielsweise eine geeignete Maßnahme sein, Hilfsorganisationen zu verpflichten, medizinisch ausgebildetes Personal an die für die Gesundheitsversorgung zuständigen Behörden zu melden. Hingegen bestehen erhebliche Zweifel an der Eignung etwa von Maßnahmen, die allein mithilfe von Telekommunikationsverkehrsdaten individuelle Infektionswege nachvollziehen sollen.

▪ Die geplanten Maßnahmen müssen erforderlich sein. Stehen **ebenfalls geeignete Maßnahmen zur Zweckerreichung** zur Verfügung, die **weniger**, oder - wie eine vorherige Anonymisierung - sogar gar **nicht** in die Rechte der Menschen eingreifen,

müssen diese vorrangig umgesetzt werden. Zudem darf die Verarbeitung der personenbezogenen Daten nicht – wie die präventive Überwachung ausnahmslos der gesamten Bevölkerung – **außer Verhältnis zum angestrebten legitimen Zweck** stehen. Daraus folgt, dass besonders stark freiheitseinschränkende Maßnahmen auch an besondere Voraussetzungen geknüpft werden müssen – etwa an die formelle Feststellung einer Gesundheitsnotlage, wie sie nach dem Infektionsschutzrecht in einigen Ländern bereits erfolgt ist.

▪ Zur verhältnismäßigen Ausgestaltung der Verarbeitung von sensiblen Daten gehört es schließlich, dass die speziell zur Bewältigung der Corona-Pandemie getroffenen Maßnahmen umkehrbar in dem Sinne gestaltet werden, dass sie nach Krisenende wieder zurückgenommen werden können und, wenn sie dann unverhältnismäßig sind, sogar müssen. So sind **nicht mehr für die benannten Zwecke benötigte** personenbezogene Daten **unverzüglich** zu **löschen**. Generell sollten zudem **alle Maßnahmen befristet** werden. Dies gilt insbesondere für solche gesetzlichen Maßnahmen, die in besonderem Maße in die Grundrechte der betroffenen Personen eingreifen.

▪ Gesundheitsdaten zählen zu den besonders sensiblen Daten, weil ihre Verwendung für die betroffenen Personen besondere Risiken nicht zuletzt in ihrem gesellschaftlichen Umfeld begründen können. Das europäische **Datenschutzrecht verlangt deshalb geeignete Garantien zum Schutz der betroffenen Personen. Technisch-organisatorische Maßnahmen zum Schutz der Integrität und Vertraulichkeit von Gesundheitsdaten** sind nicht nur **rechtlich geboten**, sondern auch **notwendig**, um eine missbräuchliche Verwendung von Daten zu verhindern und Fehlern in der Verarbeitung entgegenzuwirken. Wichtig ist es auch, im Sinne des Datenschutz-Grundsatzes der Transparenz die betroffenen Personen in verständlicher Weise über die Verarbeitung ihrer Daten zu informieren.

Datenschutz-Grundsätze bieten gerade auch in Krisenzeiten hinreichende Gestaltungsmöglichkeiten für eine rechtskonforme Verarbeitung personenbezogener Daten. Ihre Einhaltung leistet einen Beitrag zur Wahrung der Freiheit in der demokratischen Gesellschaft.

- **16.04.2020 – Polizei 2020 – Risiken sehen, Chancen nutzen!**

  Mit dem von der Innenministerkonferenz beschlossenen Programm Polizei 2020 besteht die Chance, bisherige datenschutzrechtliche Defizite zu beseitigen und den Datenschutz nachhaltig zu verbessern. Die Polizeibehörden in Bund und Ländern haben einen ersten „fachlichen Bebauungsplan“ für das Programm Polizei 2020 vorgelegt. Dieser benennt den Datenschutz als eines der Kernziele. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder begrüßt dies ausdrücklich. Sie vermisst aber ausreichende Vorschläge, wie das Projekt den Datenschutz stärken will. Die Konferenz fordert deshalb, die Ziele und Meilensteine des Programms auch an datenschutzrechtlichen Kernforderungen auszurichten und die Datenschutzaufsicht in diesen Prozess einzubinden.

  Aus Sicht der Datenschutzbehörden sind vorrangig folgende Ziele in den Blick zu nehmen:

  1. Umfassende Bestandsaufnahme

  Eine Projektanalyse umfasst bislang nur Fragen der technischen Machbarkeit. Sie hat insbesondere nicht die Ergebnisse aus den zahlreichen datenschutzrechtlichen Kontrollen und Beratungen der letzten Jahre einbezogen. Dies ist in einer unabhängigen Evaluierung nachzuholen.

  2. Rechtliche Leitplanken

  Mit dem neuen „Datenhaus“ in Polizei 2020 schaffen die Sicherheitsbehörden eine technische Grundlage für umfassende com-

putergestützte Analysen personenbezogener Daten. Diese greifen intensiv in Grundrechte ein und sind deshalb gesetzlich und technisch zu begrenzen. Sie lediglich auf Generalklauseln zu stützen, wird dem Grundrecht auf informationelle Selbstbestimmung nicht gerecht. Die verantwortlichen Stellen müssen die gesetzlich und verfassungsrechtlich implizierten roten Linien bestimmen. Dies ist zwingend erforderlich, bevor Haushaltsmittel in großem Umfang eingesetzt werden.

3. Zwecktrennung

Verarbeiten die Sicherheitsbehörden personenbezogene Daten, muss dafür immer ein konkreter Zweck festgelegt sein. Dies ist der Kern des Datenschutzrechts. Deshalb muss das neue System präzise zwischen den verschiedenen Verarbeitungszwecken Aufgabenerfüllung, Dokumentation und Vorsorge trennen. Insbesondere dürfen für eine konkrete Aufgabe oder zur Dokumentation gespeicherte Daten nicht pauschal in einen Datenvorrat überführt werden oder als Auswerte- und Rechercheplattform genutzt werden.

4. Verbesserung der Datenqualität

Wenn die Polizeibehörden die IT-Struktur neu aufstellen, müssen sie alle Chancen nutzen: Sie müssen vorhandene Datenbestände bereinigen, unnötige Daten aussondern und die Qualität der Daten sichern. Dies gilt auch, wenn alte Daten in die neuen Systeme übertragen werden. Datenschutzkontrollen haben aufgezeigt, dass dies erforderlich ist. Beispiel ist die Falldatei Rauschgift.

5. Datenschutzspezifische Basisdienste

Mit dem Programm Polizei 2020 besteht die Chance, neue technische Grundfunktionalitäten des Datenschutzes als „Basisdienste“ zu implementieren. Notwendig sind z.B. ein „Basisdienst Zwecktrennung“, ein „Basisdienst Datenqualität“ und ein „Basisdienst Aufsicht und Kontrolle".

- **26.08.2020 – Registermodernisierung verfassungskonform umsetzen!**

  Mit dem Gesetz zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung (enthalten im Registermodernisierungsgesetz – RegMoG) plant die Bundesregierung eine Modernisierung der in der Verwaltung geführten Register. Hierzu soll u.a. eine Identifikationsnummer (ID-Nr.) für natürliche Personen als registerübergreifendes Ordnungsmerkmal in alle für die Umsetzung des Onlinezugangsgesetzes relevanten Register von Bund und Ländern eingeführt werden.

  Als übergreifendes Ordnungsmerkmal soll die Steuer-Identifikationsnummer (Steuer-ID) dienen, vor deren fortschreitend ausgedehnter Nutzung die Datenschutzbeauftragten des Bundes und der Länder mehrfach deutlich gewarnt hatten. Die nun geplante ausgedehnte Verwendung der Steuer-ID als einheitliches Personenkennzeichen löst sich vollständig von ihrer ursprünglichen Zweckbestimmung für rein steuerliche Sachverhalte, obwohl sie nur deswegen bislang als verfassungskonform angesehen werden kann.

  Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) wies bereits in ihrer Entschließung vom 12.09.2019 darauf hin, dass die Schaffung solcher einheitlichen und verwaltungsübergreifenden Personenkennzeichen bzw. Identifikatoren (auch in Verbindung mit einer entsprechenden Infrastruktur zum Datenaustausch) die Gefahr birgt, dass personenbezogene Daten in großem Maße leicht verknüpft und zu einem umfassenden Persönlichkeitsprofil vervollständigt werden können.

  Das Bundesverfassungsgericht hat der Einführung derartiger Personenkennzeichen seit jeher enge Schranken auferlegt, die hier missachtet werden. Der Blick auf den Anwendungsumfang

der geplanten Regelung zeigt das Potential der möglichen missbräuchlichen Verwendung.

So verknüpft der Gesetzentwurf bei mehr als 50 Registern die Steuer-ID als zusätzliches Ordnungsmerkmal. Auf diese Weise könnten Daten etwa aus dem Melderegister mit Daten aus dem Versichertenverzeichnis der Krankenkassen sowie dem Register für ergänzende Hilfe zum Lebensunterhalt oder dem Schuldnerverzeichnis abgeglichen und zu einem Persönlichkeitsprofil zusammengefasst werden. Die im Gesetzentwurf vorgesehenen technischen und organisatorischen Sicherungen genügen nicht, um eine solche Profilbildung wirksam zu verhindern. Diese stellen zwar sicher, dass nur autorisierte Behörden die erforderlichen Daten Ende-zu-Ende verschlüsselt übermitteln. Sie bieten aber keinen ausreichenden Schutz gegen die missbräuchliche Zusammenführung der Daten zu einer Person, die aus unterschiedlichen Registern stammen, übrigens auch nicht bei Datenlecks. Zudem ist damit zu rechnen, dass die neue ID-Nr. auch im Wirtschaftsleben weite Verbreitung finden wird, was das Missbrauchsrisiko weiter erhöht.

Die Datenschutzkonferenz hatte demgegenüber „sektorspezifische“ Personenkennziffern gefordert, die datenschutzgerecht und zugleich praxisgeeignet sind, weil sie einerseits einen einseitigen staatlichen Abgleich deutlich erschweren und andererseits eine natürliche Person eindeutig identifizieren.

Obwohl ein solches Modell in der Republik Österreich seit vielen Jahren erfolgreich praktiziert wird, hat die Bundesregierung dies nie ernsthaft erwogen und ohne überzeugende Begründung mit dem pauschalen Verweis auf „rechtliche, technische und organisatorische Komplexität“ abgelehnt.

Auch wenn die Corona-Pandemie zeigt, wie notwendig eine Beschleunigung der Digitalisierung ist, darf dies nicht als Argument

dafür benutzt werden, verfassungsrechtlich notwendige Nachbesserungen unter Hinweis auf den „Eilbedarf“ unter den Tisch fallen zu lassen.

Die Datenschutzkonferenz weist daher nochmals darauf hin, dass die dem Gesetzentwurf zugrundeliegende Architektur im Widerspruch zu verfassungsrechtlichen Regelungen steht. Sie fordert deshalb die Bundesregierung dazu auf, einen Entwurf vorzulegen, der den verfassungsrechtlichen Anforderungen genügt, bevor sie durch Entscheidung des Bundesverfassungsgerichts dazu verpflichtet wird.

- **01.09.2020 – Patientendaten-Schutz-Gesetz: Ohne Nachbesserungen beim Datenschutz für die Versicherten europarechtswidrig!**

  Der Deutsche Bundestag hat am 3. Juli 2020 das Patientendaten-Schutz-Gesetz (PDSG) entgegen der von den unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder geäußerten Kritik beschlossen. Die Kritik richtet sich insbesondere gegen das nur grobgranular ausgestaltete Zugriffsmanagement, die Authentifizierung für die elektronische Patientenakte (EPA) und die Vertreterlösung für Versicherte, die nicht über ein geeignetes Endgerät verfügen.

  Das PDSG soll am 18. September 2020 im Bundesrat abschließend beraten werden. Zentrale Gesetzesregelungen stehen in Widerspruch zu elementaren Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO). Entgegen des derzeitigen Entwurfs müssen die Versicherten bereits zum Zeitpunkt der Einführung der EPA am 1. Januar 2021 die volle Hoheit über ihre Daten erhalten. Dies entspricht auch den im PDSG vom Gesetzgeber selbst formulierten Vorgaben, die Patientensouveränität über die versichertengeführten EPA grundsätzlich ohne Einschränkungen zu wahren und die Nutzung der EPA für alle Versicherten datenschutzgerecht auszugestalten.

Diese Ziele werden mit dem Gesetzentwurf nicht erreicht. Zum Start der EPA werden alle Nutzerinnen und Nutzer in Bezug auf die von den Leistungserbringern (Ärzten etc.) in der elektronischen Patientenakte gespeicherten Daten zu einem „alles oder nichts“ gezwungen, da im Jahr 2021 keine Steuerung auf Dokumentenebene für diese Daten vorgesehen ist. Das bedeutet, dass diejenigen, denen die Versicherten Einsicht in ihre Daten gewähren, alle dort enthaltenen Informationen einsehen können, auch wenn dies in der konkreten Behandlungssituation nicht erforderlich ist.

Erst ein Jahr nach dem Start der EPA, d.h. ab dem 1. Januar 2022, können lediglich Versicherte, die für den Zugriff auf ihre EPA geeignete Endgeräte (Smartphone, Tablet etc.) nutzen, eigenständig eine dokumentengenaue Kontrolle und Rechtevergabe in Bezug auf diese Dokumente durchführen.

Alle anderen Versicherten, die keine geeigneten Endgeräte besitzen oder diese aus Sicherheitsgründen zum Schutz ihrer sensiblen Gesundheitsdaten nicht nutzen möchten (d.h. sogenannte Nicht-Frontend-Nutzer), erhalten auch über den Stichtag 1. Januar 2022 hinaus nicht diese Rechte. Ab dem 1. Januar 2022 ermöglicht das PDSG insoweit den Nicht-Frontend-Nutzern lediglich eine Vertreterlösung. Danach können diese mittels eines Vertreters und dessen mobilem Endgerät ihre Rechte ausüben. Im Vertretungsfall müssten die Versicherten jedoch ihrem Vertreter den vollständigen Zugriff auf ihre Gesundheitsdaten einräumen.

Ein weiterer Kritikpunkt ist das Authentifizierungsverfahren für die EPA und die „Gewährleistung des erforderlichen hohen datenschutzrechtlichen Schutzniveaus“. Da es sich bei den fraglichen Daten um Gesundheitsdaten und damit um höchst sensible persönliche Informationen handelt, muss nach den Vorgaben der DSGVO die Authentifizierung ein höchstmögliches Sicherheitsniveau nach dem Stand der Technik gewährleisten. Dies gilt insbesondere für Authentifizierungsverfahren ohne Einsatz der elektro-

nischen Gesundheitskarte. Wenn dabei alternative Authentifizierungsverfahren genutzt werden, die diesen hohen Standard nicht erfüllen, liegt ein Verstoß gegen die DSGVO vor.

Der Bundesrat hat in seiner Stellungnahme zum PDSG vom 15. Mai 2020 (BR-Drs.164/1/20, s. Ziffer 21. zu Artikel 1 Nummer 31 [§§ 334 ff. SGB V-E9]) die Bundesregierung auf erhebliche Bedenken im Hinblick auf die DSGVO-Konformität des PDSG hingewiesen. Seine Kritik bezieht sich im Wesentlichen auf das zum Start der EPA fehlende feingranulare Zugriffsmanagement und die daraus resultierende Einschränkung der Datensouveränität der Versicherten. Er hat die Bundesregierung aufgefordert, im weiteren Gesetzgebungsverfahren insbesondere den Regelungsvorschlag zum Angebot und zur Einrichtung der EPA (§ 342 SGB V) umfassend bezüglich datenschutzrechtlicher Bedenken zu prüfen.

Auch im Lichte dessen fordern die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder den Bundesrat auf, anlässlich seiner für den 18. September 2020 anberaumten Beratung den Vermittlungsausschuss anzurufen, um notwendige datenschutzrechtliche Verbesserungen des PDSG noch im Gesetzgebungsverfahren zu erwirken.

- **22.09.2020 – Digitale Souveränität der öffentlichen Verwaltung herstellen – Personenbezogene Daten besser schützen**

  Der Begriff „Digitale Souveränität“ wird in der öffentlichen Debatte in verschiedenen Bedeutungen verwendet. Nach der Definition des Kompetenzzentrums Öffentliche IT[1] ist in einem umfassenden Sinne Digitale Souveränität die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der

[1] Kompetenzzentrum Öffentliche IT (Hrsg.), Gabriele Goldacker, Digitale Souveränität, erhältlich unter https://www.oeffentliche-it.de/documents/10181/14412/Digitale+Souver%C3%A4nit%C3%A4t

digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.

Die Rolle der öffentlichen Verwaltung ist die gesetzesgebundene Erfüllung der Staatsaufgaben. Aus der Sicht der Verantwortlichen in der öffentlichen Verwaltung bedeutet Digitale Souveränität insbesondere, eigenständig entscheiden zu können, wie die in Art. 1 Datenschutz-Grundverordnung (DS-GVO) formulierten Ziele im Einklang mit den in Art. 5 DS-GVO festgelegten Grundsätzen für die Verarbeitung personenbezogener Daten, wie Rechtmäßigkeit, Transparenz, Zweckbindung und Sicherheit der Verarbeitung, umzusetzen sind. Dies erfordert nach Ansicht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) Wahlfreiheit und vollständige Kontrolle der Verantwortlichen über die eingesetzten Mittel und Verfahren bei der digitalen Verarbeitung von personenbezogenen Daten, gegebenenfalls unter Hinzuziehung des jeweiligen Auftragsverarbeiters.

Die Digitale Souveränität der öffentlichen Verwaltung ist jedoch nach einer für den Beauftragten der Bundesregierung für Informationstechnik durchgeführten „Strategischen Marktanalyse“[1] beeinträchtigt, „da die Geschäftsbeziehungen der öffentlichen Verwaltung mit externen, meist privaten IT-Anbietern erhebliche Abhängigkeiten verursachen. Danach resultieren diese Abhängigkeiten aus der technischen Beschaffenheit der IT-Landschaft, aus den stark auf Software ausgerichteten Prozessen, aus dem Umstand, dass sich die Beschäftigten an die eingesetzte Software gewöhnt haben, aus Vertragsklauseln sowie aus den bestehenden Marktgegebenheiten.“ Sie bringen Kontrollverlust und eine eingeschränkte Verfügbarkeit, Vertraulichkeit und Integrität der verarbeiteten personenbezogenen Daten mit sich. Auch vor

[1] PwC Strategy& (Germany) GmbH, Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern, erhältlich unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/Aktuelles/20190919_strategische_marktanalyse.pdf?__blob=publicationFile

diesem Hintergrund hat sich der IT-Planungsrat zum Ziel gesetzt, die digitale Souveränität der öffentlichen Verwaltung in ihren Rollen als Nutzer, Bereitsteller und Auftraggeber von digitalen Technologien kontinuierlich zu stärken.

Die Datenschutzkonferenz teilt die Einschätzung des IT-Planungsrats, dass die Digitale Souveränität der öffentlichen Verwaltung beeinträchtigt ist und sieht deren Gewährleistung als ein vordringliches Handlungsfeld an. Aus ihrer Sicht sind datenschutzrechtliche Vorgaben für große Softwareanbieter, die in der „Strategischen Marktanalyse“ empfohlene Diversifizierung durch den Einsatz alternativer Softwareprodukte sowie die Nutzung von Open Source Software besonders erfolgversprechende Handlungsoptionen. Durch den Einsatz von Open Source Software kann die Unabhängigkeit der öffentlichen Verwaltung von marktbeherrschenden Softwareanbietern dauerhaft sichergestellt werden. Konkret fordert die Datenschutzkonferenz Bund, Länder und Kommunen dazu auf, langfristig nur solche Hard- und Software einzusetzen,

- die den Verantwortlichen die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik belässt, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Zustimmung der Verantwortlichen im Einzelfall erfolgen,

- bei der alle zur Verfügung stehenden Sicherheitsfunktionen für Verantwortliche transparent sind und

- die eine Nutzung der Hard- und Software sowie den Zugriff auf personenbezogene Daten ermöglicht, ohne dass Unbefugte davon Kenntnis erhalten und ohne dass unzulässige Nutzungsprofile angelegt werden können.

Kurzfristig erfordert die Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in Bund, Ländern und Kommunen zur

Einhaltung der datenschutzrechtlichen Anforderungen insbesondere:

1. Verbesserte Möglichkeiten der datenschutzrechtlichen Beurteilung von Produkten und Dienstleistungen – sowohl bei der Auswahl als auch im laufenden Betrieb:

- Zertifizierungen können Verantwortlichen die Prüfung und Kontrolle erleichtern, wenn sie sich nicht eigenständig ein valides Bild über die komplexe Funktionsweise von Informationstechnik machen können.
- Die Ministerialebene sollte in die Pflicht genommen werden, Vorgaben für die öffentliche Verwaltung zu machen.
- Zudem sollten Behörden stärker kooperieren, um die erforderliche Expertise selbst bereitstellen zu können.

2. Berücksichtigung der Ziele und Kriterien der Digitalen Souveränität bei der Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen:

- Für die Vergabe und Beschaffung von Hardware, Software, Informations- und Kommunikationstechnik sowie IT-Dienstleistungen sollten im Einklang mit dem europäischen Vergaberecht Ausschreibungskriterien entwickelt werden, um bei der Vergabe solche Anbieter bevorzugt auswählen zu können, welche Digitale Souveränität ermöglichen.

3. Nutzung von offenen Standards durch die Produktentwickler, damit die Verantwortlichen auch tatsächlich in die Lage versetzt werden, Anbieter und Produkte zu wechseln, wenn sie mit deren Produkten und Dienstleistungen die Datenschutzanforderungen nicht (mehr) oder nur ungenügend umsetzen können:

- Die Nutzung von offenen Standards kann durch deren inhärente Transparenz dazu beitragen, die Überprüfbarkeit zu sichern und eine Kontrolle zu erleichtern. Dies betrifft System-

software und insbesondere Datenformate, aber auch Datenbanken und Anwendungssoftware, die auf Software-Plattformen aufsetzen. Offene Standards sind zudem geeignet, unerwünschte Lock-in-Effekte zu vermeiden. Insbesondere können hierbei über die Einrichtung von Bund-/Länder-/Kommunen-übergreifenden Entwicklungsverbünden Aufwände verteilt und Skaleneffekte gehoben werden. Daher sollten Verantwortliche den Einsatz von Produkten und Dienstleistungen bevorzugen, die offene Standards verwenden.

4. Veröffentlichung des Quellcodes und der Spezifikationen öffentlich finanzierter digitaler Entwicklungen:

- Wenn Software oder Hardwarestandards unter finanzieller Beteiligung der öffentlichen Hand entwickelt werden, sollten diese standardmäßig so veröffentlicht werden, dass diese nachvollzogen werden können.
- Standardmäßig sollten diese so ausgestaltet werden, dass eine öffentliche Weiterentwicklung möglich ist (Open Source Lizenzen).

5. Möglichkeiten zur Steuerung des Zugriffs auf Daten, der Konfiguration von Systemen und der Gestaltung von Prozessen:

- Verantwortliche müssen über tatsächliche Steuerungsmöglichkeiten verfügen, insbesondere, um ihre Pflichten nach Art. 25 DS-GVO erfüllen zu können. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen muss elementarer Bestandteil von Dienstleistungen und Produkten sein, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen. Verantwortliche sollten nur solche Produkte und Dienstleistungen beschaffen und nutzen, die diese Prinzipien beachten. Organisationen mit verteilter Verantwortung (etwa Kommunen, Bundesländer oder auch beteiligte Dienstleister wie Konzerne) müssen auch bei zentral beschafften oder betriebenen Komponenten

wie Hardware, Software und Dienstleistungen die erforderlichen Einstellungen vornehmen können, um einen rechtskonformen Betrieb der Verfahren zu gewährleisten. Bei zentral bereitgestellten Anwendungen, etwa in einer derzeit im IT-Planungsrat diskutierten „Verwaltungscloud“, ist es eine notwendige Voraussetzung, dass die jeweiligen datenschutzrechtlichen Vorgaben der Verantwortlichen für Betrieb und Konfiguration individuell umgesetzt werden können. Das ist bei der Konzeption zu berücksichtigen.

Die Datenschutzkonferenz ist der Ansicht, dass die Stärkung der Digitalen Souveränität große strategische Bedeutung für die öffentliche Verwaltung hat und gemeinsam und kontinuierlich vorangetrieben werden muss. Sie fordert Bund, Länder und Kommunen dazu auf, die in der Entschließung aufgeführten Kriterien für eine Stärkung der Digitalen Souveränität der öffentlichen Verwaltung in den Bereichen IT-Beschaffung sowie System- und Fachverfahrensentwicklung zu berücksichtigen.

- **22.09.2020 – Datenschutz braucht Landgerichte auch erstinstanzlich**

  Mit dem „Entwurf eines Gesetzes zur Effektivierung des Bußgeldverfahrens“ (BR-Drs. 107/20 (B)) will der Bundesrat die erstinstanzliche Zuständigkeit der Landgerichte für Geldbußen nach der Datenschutz-Grundverordnung (DSGVO) über 100.000 Euro streichen. Selbst über Geldbußen in dieser Höhe sollen künftig die Amtsgerichte entscheiden.

  Das Ziel der Effektivierung des Bußgeldverfahrens wird mit dem geplanten Gesetz jedoch nicht erreicht werden. Der Gesetzentwurf verkennt in eklatanter Weise die besondere wirtschaftliche, technische und rechtliche Komplexität von DSGVO-Geldbußen. Eine Streichung der landgerichtlichen Zuständigkeit würde die Amtsgerichte zudem nicht etwa entlasten, sondern noch stärker als bisher belasten.

Das Sanktionsrecht der DSGVO ist – anders als der Bundesrat unterstellt – mit der Sanktionierung herkömmlicher deutscher Ordnungswidrigkeiten wie etwa Geldbußen im Straßenverkehr in keiner Weise vergleichbar. Es geht hierbei nicht etwa um die Verfolgung von Bagatelldelikten, sondern um unionsweit höchst relevante Verfahren zum Schutz des freien Datenverkehrs und der Privatsphäre der Bürgerinnen und Bürger. Dabei können teils Millionen von Kundendaten betroffen sein. Datenschutz-Ordnungswidrigkeiten mit Geldbußen über 100.000 Euro weisen wirtschaftlich und technisch eine besondere Komplexität auf und bedürfen daher einer Würdigung durch den Spruchkörper eines Kollegialgerichts. Sie sind viel eher mit Wirtschaftsstrafsachen vergleichbar, die ohnehin den Landgerichten zugewiesen sind. Nicht ohne Grund hat sich der europäische Gesetzgeber bei den Bußgeldvorschriften der DSGVO am Kartellrecht orientiert. Für ähnlich komplexe Ordnungswidrigkeiten in Kartellangelegenheiten ist in Deutschland sogar eine Zuständigkeit der Oberlandesgerichte gegeben. Diese Wertung kommt auch in dem insoweit eindeutigen Wortlaut von § 41 Abs. 2 Satz 1 Bundesdatenschutzgesetzes (BDSG) zum Ausdruck, der eine entsprechende Anwendung der Vorschriften über das Strafverfahren und damit auch eine Besetzung der Strafkammern als sog. große Bußgeldkammern entsprechend § 76 GVG vorsieht.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) fordert daher die Beibehaltung der landgerichtlichen Zuständigkeit für DSGVO-Geldbußen über 100.000 Euro und warnt vor einer Streichung der Vorschrift und deren Folgen.

- **25.11.2020 – Für den Schutz vertraulicher Kommunikation durch eine sichere Ende-zu-Ende-Verschlüsselung – Vorschläge des Rates der Europäischen Union stoppen**

  Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz) tritt Forderungen der Regierungen der Mitgliedstaaten der Europäischen

Union entgegen, Sicherheitsbehörden und Geheimdiensten die Möglichkeit zu eröffnen, auf Inhalte verschlüsselter Kommunikation zuzugreifen. Als Reaktion auf jüngste Terroranschläge soll diesen Behörden und Diensten der Zugriff auf die verschlüsselte Kommunikation ermöglicht werden. Dies umfasst insbesondere auch Messenger-Dienste wie WhatsApp, Threema oder Signal. Nach dem Resolutionsentwurf „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ des Rates der Europäischen Union (Nr. 12143/1/20 vom 6. November 2020) sollen entsprechende Möglichkeiten in Zusammenarbeit mit den Anbietern von Online-Diensten entwickelt werden.

Eine sichere und vertrauenswürdige Verschlüsselung ist essentielle Voraussetzung für eine widerstandsfähige Digitalisierung in Wirtschaft und Verwaltung. Unternehmen müssen sich vor Wirtschaftsspionage schützen können. Eine Schwächung der Verschlüsselungsverfahren könnte jedoch europäische Unternehmen im globalen Markt benachteiligen. Bürgerinnen und Bürger müssen auf eine sichere und integre Nutzung digitaler Verwaltungsleistungen vertrauen können und benötigen hierbei Schutz vor umfassender Überwachung und Datenmissbrauch. Auch die Ziele des Onlinezugangs-gesetzes, Verwaltungsleistungen elektronisch über Verwaltungsportale anzubieten, würden konterkariert, wenn Nutzerinnen und Nutzer dieser Portale sich der Vertraulichkeit der elektronischen Kommunikation nicht sicher sein könnten.

Verschlüsselung ist ebenso ein zentrales Mittel für die Datenübermittlung in Drittländer gemäß den Empfehlungen zu ergänzenden Maßnahmen für Übertragungsinstrumente zur Gewährleistung des EU-Schutzniveaus des Europäischen Datenschutzausschusses als Reaktion auf das "Schrems II"-Urteil des Europäischen Gerichtshofs.

Würden die Vorschläge des Rates der Europäischen Union umgesetzt, würde eine sichere Ende-zu-Ende-Verschlüsselung untergraben und notwendiges Vertrauen zerstört, ohne dass das

angestrebte Ziel, die Ermittlungsmöglichkeiten von Sicherheitsbehörden zu verbessern, nachhaltig und effektiv erreicht wird. Hintertüren in Verschlüsselungsverfahren stellen die Sicherheit und Wirksamkeit dieser gänzlich in Frage. Die Aushöhlung von Verschlüsselungslösungen würde zudem unweigerlich zu einem Ausweichen auf Umgehungstechniken führen, derer sich sowohl Kriminelle und Terroristen als auch technisch versierte Bürgerinnen und Bürger bedienen könnten.

Gleichzeitig würde der Einsatz wirksamer Ende-zu-Ende-Verschlüsselung für technisch weniger versierte Bürgerinnen und Bürger faktisch unmöglich gemacht.

Aus gutem Grund hat sich die Bundesregierung bereits im Jahr 1999 in den Leitlinien deutscher Kryptopolitik zum Einsatz kryptographischer Verfahren bekannt. In Europa wird die Vertraulichkeit der Kommunikation durch das individuelle Recht auf Achtung der Kommunikation in Art. 7 GRCh geschützt. Ergänzend greift für gespeicherte Kommunikationsinhalte das in Art. 8 GRCh garantierte Recht auf Schutz personenbezogener Daten. In Deutschland wird der Grundrechtsschutz beim Einsatz von Kommunikationsdiensten durch das Fernmeldegeheimnis in Art. 10 GG und ergänzend durch das Recht auf informationelle Selbstbestimmung sowie das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. Folgerichtig befürwortete die Bundesregierung im Jahr 2015 erneut den Einsatz von Kryptographie in der Charta zur Stärkung der vertrauenswürdigen Kommunikation.

Die Datenschutzkonferenz sieht keine Veranlassung, dass der Rat der Europäischen Union von diesen grundrechtswahrenden Positionen abweicht, zumal weitere, massiv in die Privatsphäre der Nutzerinnen und Nutzer eingreifende Befugnisse auch nicht erforderlich sind. Der effektive Kampf gegen Terror ist zwar ein legitimes Anliegen, aber den Sicherheitsbehörden stehen für die verfolgten Ziele bereits umfangreiche und sehr eingriffsintensive Instrumente zur Verfügung.

Die Datenschutzkonferenz hat sich wiederholt für den Einsatz sicherer und integrer Verschlüsselung eingesetzt und auf die Unverzichtbarkeit vertrauenswürdiger und integrer Kommunikationsmöglichkeiten hingewiesen. Sie fordert erneut die Bundesregierung und die deutsche EU-Ratspräsidentschaft auf, den Einsatz dem Stand der Technik entsprechender Verschlüsselungslösungen zu fördern und dem Bestreben, solche Lösungen zu schwächen, entschieden entgegenzutreten. Sichere Ende-zu-Ende-Verschlüsselung muss die Regel werden, um gerade im Zeitalter der Digitalisierung eine sichere, vertrauenswürdige und integre Kommunikation in Verwaltung, Wirtschaft, Zivilgesellschaft und Politik zu gewährleisten.

- **25.11.2020 – Betreiber von Webseiten benötigen Rechtssicherheit – Bundesgesetzgeber muss europarechtliche Verpflichtungen der „ePrivacy-Richtlinie“ endlich erfüllen**

  Der Gesetzgeber ist verpflichtet, die EU-Richtlinie über den europäischen Kodex für die elektronische Kommunikation vom 11. Dezember 2018 (RL 2018/1972/EU) bis zum 20. Dezember 2020 umzusetzen.

  Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) fordert den Gesetzgeber auf, endlich Regelungen zu erlassen, um die ePrivacy-Richtlinie[1] vollständig und im Einklang mit der Datenschutz-Grundverordnung (DSGVO) umzusetzen.

  Die DSK hat in der Vergangenheit wiederholt kritisch darauf hingewiesen, dass der Gesetzgeber Art. 5 Abs. 3 ePrivacy-Richtlinie nicht oder nicht ordnungsgemäß umgesetzt hat.[2] Das Urteil des

[1] Richtlinie 2002/58/EG in der letzten Änderung durch die Richtlinie 2009/136/EU

[2] Siehe Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/en/20150205_en_Entschliessung_Cookies.pdf

Bundesgerichtshofs (BGH) vom 28. Mai 2020 (I ZR 7/16 – „Planet49“) verstärkt nach Auffassung der DSK den seit langem bestehenden, dringenden Handlungsbedarf.

Die DSK hat bereits im April 2018 in der Positionsbestimmung „Zur Anwendbarkeit des TMG für nichtöffentliche Stellen ab dem 25. Mai 2018“ den Standpunkt vertreten, dass die Datenschutzvorschriften des Telemediengesetzes neben der Datenschutz-Grundverordnung (DSGVO) nicht mehr anwendbar sind. Eine ausführliche Begründung zu dieser Rechtsauffassung wurde von der DSK in der Orientierungshilfe für Anbieter von Telemedien im März 2019 veröffentlicht.[1]

Der BGH hatte im Planet49-Verfahren einen Streit zu entscheiden, in dem das beklagte Unternehmen personenbezogene Daten über das Nutzungsverhalten von Verbrauchern mittels Cookies zu pseudonymisierten Nutzungsprofilen verarbeitete und diese für personalisierte Werbung nutzte. Nach dem Wortlaut des § 15 Abs. 3 Telemediengesetz (TMG) wäre ein solches Vorgehen dann zulässig, wenn die betroffenen Personen entsprechend informiert wurden und nicht widersprochen haben (sogenannte Widerspruchslösung). Mit Blick auf Art. 5 Abs. 3 ePrivacy-Richtlinie legt der BGH § 15 Abs. 3 TMG dahingehend aus, schon in dem Fehlen einer wirksamen Einwilligung könne ein solcher Widerspruch gesehen werden, weshalb eine aktive Einwilligung erforderlich sei. Unter Zugrundelegung dieser Auslegung von § 15 Abs. 3 TMG wendet er diese Vorschrift neben der DSGVO an. Letztlich ist der BGH der Vorabentscheidung des Europäischen Gerichtshofes gefolgt und bestätigt das grundsätzliche Erfordernis einer wirksamen Einwilligung für das Setzen von Cookies.

[1] Positionsbestimmung der DSK vom 26. April 2018 „Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018“, abrufbar unter: https://www.datenschutzkonferenz-online.de/anwendungshinweise.html), Orientierungshilfe für Anbieter von Telemedien (https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

Schon die Tatsache, dass die DSK und der BGH bei einer sehr praxisrelevanten Rechtsfrage zwar im Ergebnis darin übereinstimmen, dass eine Verarbeitung, wie sie den Gerichten zur Entscheidung vorlag, einwilligungsbedürftig ist, jedoch bei der Herleitung dieses Ergebnisses voneinander abweichende Auffassungen vertreten, verdeutlicht das Ausmaß der Rechtsunklarheit.

Mit der Entscheidung wird die Abgrenzung der Regelungsbereiche zwischen ePrivacy-Richtlinie, DSGVO und den Datenschutzvorschriften des TMG deutlich erschwert. Der BGH stellt ausdrücklich heraus, dass ePrivacy-Richtlinie und DSGVO unterschiedliche Schutzrichtungen verfolgen. Die Vorschriften in den §§ 12 bis 15 TMG knüpfen ausdrücklich an den Begriff der Verarbeitung personenbezogener Daten an. Diese Materie ist auf europäischer Ebene weitgehend abschließend durch die Datenschutz-Grundverordnung geregelt. Art. 5 Abs. 3 ePrivacy-Richtlinie hat hingegen auch Informationen ohne Personenbezug zum Regelungsgegenstand. Es bleibt daher offen, ob § 15 Abs. 3 TMG – entgegen des Wortlautes – auch dann eine Umsetzung des Art. 5 Abs. 3 ePrivacy-Richtlinie darstellen soll, wenn die Informationen, die im Endgerät eines Teilnehmers gespeichert werden oder auf die zugegriffen wird, keinen Personenbezug haben.

§ 15 Abs. 3 TMG bezieht sich ausdrücklich und ausschließlich auf die Erstellung von pseudonymen Nutzungsprofilen für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien. Die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, kann jedoch auch zu anderen Zwecken erfolgen und ist nicht auf die in § 15 Abs. 3 TMG genannten Zwecke beschränkt.

Schließlich fordert Art. 5 Abs. 3 ePrivacy-Richtlinie grundsätzlich ohne Berücksichtigung konkreter Zwecke eine Einwilligung. Lediglich in Art. 5 Abs. 3 Satz 2 ePrivacy-Richtlinie finden sich Ausnahmen von diesem Grundsatz. Dieses Regel-Ausnahme-Prinzip findet sich im TMG nicht wieder.

Webseitenbetreiber und andere Akteure, die ihre Dienste u. a. in Bezug auf „Cookies“ rechtskonform gestalten müssen, brauchen Rechtsklarheit. Der Gesetzgeber ist deshalb aufgefordert, bestehende Rechtsunsicherheiten umgehend durch eine klare und europarechtskonforme Gesetzgebung zu beseitigen.

- **25.11.2020 – Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten**

  Bei der Einrichtung des manuellen Auskunftsverfahrens von Bestandsdaten von Telekommunikationskunden hat der Gesetzgeber wichtige verfassungsrechtliche Vorgaben außer Acht gelassen. Die bisherigen Zugriffsbefugnisse der Sicherheitsbehörden sind zu weitreichend. Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben bereits seit Jahren auf die Unverhältnismäßigkeit entsprechender Regelungen hingewiesen.

  Mit Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 und 1 BvR 2618/13 – („Bestandsdatenauskunft II“) hat das Bundesverfassungsgericht erneut verfassungsrechtliche Vorgaben für die Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens gemacht. Das Gericht bekräftigte, dass sowohl die Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stellen jeweils einer verhältnismäßigen und normenklaren Rechtsgrundlage bedürfen. Die Übermittlungs- und Abrufregelungen müssen – so das Gericht – die Verwendungszwecke hinreichend begrenzen, mithin die Datenverwendung an bestimmte Zwecke, tatbestandliche Eingriffsschwellen und einen hinreichend gewichtigen Rechtsgüterschutz binden (1. Leitsatz). Hierzu gehört, dass für den Einsatz zur Gefahrabwehr und die Tätigkeit der Nachrichtendienste grundsätzlich im Einzelfall eine konkrete Gefahr und für die Strafverfolgung ein Anfangsverdacht vorliegen müssen. Die Zuordnung dynamischer IP-Adressen muss darüber hinaus dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen (4. Leitsatz). Die Übermittlungsvorschrift des § 113 Telekommunikationsgesetz sowie eine Reihe mit ihm korrespondierender fach-

gesetzlicher Abrufregelungen wurden im Hinblick hierauf für mit dem Grundgesetz unvereinbar erklärt.

Zwar bleiben die bisherigen Vorschriften bis zur Neuregelung, längstens jedoch bis 31. Dezember 2021, nach Maßgabe der Entscheidungsgründe weiter anwendbar. Im Interesse der Rechtssicherheit appelliert die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) jedoch an die politisch Verantwortlichen, diese Frist nicht auszureizen, sondern das manuelle Auskunftsverfahren möglichst zeitnah verfassungskonform auszugestalten.

Die DSK hält es zudem für geboten, dass Bundes- und Landesgesetzgeber im Zuge der Umsetzung der Entscheidung nicht nur die unmittelbar von der Entscheidung betroffenen Vorschriften anpassen, sondern alle vergleichbaren Vorschriften, die Grundlage für die Übermittlung und den Abruf von personenbezogenen Daten sein können, im Lichte der Entscheidung des Bundesverfassungsgerichts überprüfen und gegebenenfalls verfassungskonform ausgestalten. Dies betrifft insbesondere Regelungen der Polizei- und Verfassungsschutzgesetze der Länder, die die Erteilung von Auskünften über Daten lediglich an die Erfüllung der Aufgaben der berechtigten Stelle knüpfen. Solche Regelungen sind mit der Gefahr unbegrenzter Verwendungen von Daten verbunden und damit unverhältnismäßig (vgl. BVerfG, o. g. Beschluss vom 27. Mai 2020, Rn. 154, 197). Datenabfragen dürfen nicht länger aufgrund derart unbestimmter Rechtsgrundlagen erfolgen.

Beschlüsse der Datenschutzkonferenz

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

- **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 Widerrufsrechts 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.

  Zur Umsetzung dieser Anforderungen in der Patienteninformation wird vorgeschlagen:

  - Unter 3.2 im ersten Absatz nach Satz 2 einzufügen: "In Biomaterialien kann Ihre Erbsubstanz in Form genetischer Daten enthalten sein. Insofern sind insbesondere die unter 1.4 beschriebenen Risiken für genetische Daten zu beachten. Hierzu

zählt auch ein erhöhtes Risiko einer Rückverfolgbarkeit Ihrer Person anhand dieser Daten."

- Unter 3.3 im ersten Absatz nach Satz 2 einzufügen: "Ihr Recht, über die Verarbeitung Ihrer personenbezogenen Daten selbst zu bestimmen, bleibt von der Eigentumsüber-tragung unberührt. Trotz Eigentumsübertragung können Sie Ihre Einwilligung in die Datenverarbeitung jederzeit widerrufen (siehe Punkt 6) und die Vernichtung Ihrer Biomaterialien verlangen."
- Zudem ist in der Einwilligung und in der Patienteninformation jeweils an geeigneter Stelle auf die Möglichkeit der Registrierung bei einem E-Mail-Verteiler hinzuweisen, der rechtzeitig vor Beginn über neue Forschungsprojekte auf Basis der Daten der Medizininformatik-Initiative informiert.

Ergänzend sollte in der Einwilligungserklärung in dem Kasten unter 3.3 als zweiter Satz aufgenommen werden: "Mein Recht, über die Verarbeitung meiner dem Biomaterial zu entnehmenden personenbezogenen Daten selbst zu bestimmen, bleibt von der Eigentumsübertragung unberührt (siehe Punkt 3.3 der Patienteninformation)."

Als redaktionelle Korrektur wird zudem empfohlen, in der Einwilligungserklärung unter 1.1 zum Stichwort der Codierung auch auf Punkt 1.3 der Patienteninformation zu verweisen, da die Codierung dort beschrieben wird

- **12.05.2020 – Hinweise zum Einsatz von Google Analytics im nicht-öffentlichen Bereich**

Google Analytics ist eines der weitest verbreiteten Tools für Website-Betreiber (Anwender). Mit Hilfe dieses Tools lassen sich umfassende statistische Auswertungen der Webseitennutzung vornehmen. Aus diesem Grund besteht ein großer Beratungsbedarf hinsichtlich des Einsatzes von Google Analytics.

Die Datenschutzaufsichtsbehörden haben vor dem Hintergrund des neuen Rechtsrahmens mit Geltung der DS-GVO den Einsatz

von Google Analytics neu bewertet. Ältere Auffassungen der Datenschutzaufsichtsbehörden, die unter Berücksichtigung der Rechtslage vor dem 25.05.2018 kommuniziert wurden, gelten damit als überholt.[1]

Im Folgenden handelt es sich keinesfalls um eine abschließende Beurteilung. Die folgenden Ausführungen stellen eine Ergänzung der Orientierungshilfe für Anbieter von Telemedien[2] dar und betreffen lediglich die häufigsten Fragestellungen beim Einsatz von Google Analytics. Die folgenden Ausführungen stellen keine Empfehlung zum Einsatz von Google Analytics dar, sondern beschreiben nur die datenschutzrechtlichen Mindestanforderungen, die von Seitenbetreibern nach derzeitigem Stand zwingend eingehalten werden müssen.

Die Auffassungen der Datenschutzaufsichtsbehörden stehen unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung durch den Europäischen Datenschutzausschuss und der Rechtsprechung des EuGH.

Die Ausführungen gelten für den Fall, dass der Anwender von Google-Analytics die von Google derzeit[3] empfohlenen Standardeinstellungen nutzt. Für den Fall, dass der Anwender von Google Analytics von den empfohlenen Einstellungen abweicht und/oder ergänzende Funktionen verwendet (z. B. Google Analytics 360) oder Google die Verarbeitung oder die vertraglichen Grundlagen ändert, wird auf die von den deutschen Datenschutzaufsichtsbehörden veröffentlichten Ausführungen der Orientierungshilfe für Anbieter von Telemedien verwiesen.

[1] Dies gilt insbesondere für die Veröffentlichung des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, „Hinweise für Webseitenbetreiber mit Sitz in Hamburg, die Google Analytics einsetzen“.
[2] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf
[3] Stand: 11.03.2020

I. Personenbezogene Daten

Beim Einsatz von Google Analytics werden immer personenbezogene Daten der Nutzer verarbeitet.

In den Google Analytics-Hilfen[1] erläutert Google, dass Nutzungsdaten keine „personenidentifizierbaren Informationen“ seien. Diese Auffassung steht nicht nur im Widerspruch zur Definition des Begriffs „personenbezogene Daten“ in Art. 4 Nr. 1 der DS-GVO, sondern ist auch missverständlich, da Google im Weiteren Folgendes ausführt:

„Bitte beachten Sie, dass Daten, die Google nicht als personenidentifizierbare Informationen einstuft, im Rahmen der DS-GVO als personenbezogene Daten gelten können.“

Die Datenschutzaufsichtsbehörden weisen daher ausdrücklich darauf hin, dass es sich bei den mit Google Analytics verarbeiteten Daten (Nutzungsdaten und sonstige gerätespezifische Daten, die einem bestimmten Nutzer zugeordnet werden können) um personenbezogene Daten i.S.d. DS-GVO handelt.

II. Verhältnis zwischen Google Analytics-Anwender und Google

Google hat die Verarbeitungsprozesse von Google Analytics fortlaufend angepasst. Dies hat dazu geführt, dass Google Analytics nicht mehr nur ein Tool zur statistischen Analyse (Reichweitenmessung) ist, sondern dem Anwender eine Vielzahl an weiteren Funktionen bietet, mit denen der Anwender verschiedene Zwecke verfolgen kann.

[1] Abrufbar unter der URL: https://support.google.com/analytics/answer/7686480 [Stand: 27.09.2019].

Nach Auffassung der Datenschutzaufsichtsbehörden ist die Verarbeitung im Zusammenhang mit Google Analytics keine Auftragsverarbeitung gemäß Art. 28 DS-GVO. Nach Art. 4 Nr. 7, Art. 28 Abs. 10 DS-GVO hat der Verantwortliche die Zwecke und Mittel der Verarbeitung selbst zu bestimmen. Daraus folgt die Pflicht des Auftragsverarbeiters, die Daten ausschließlich auf Weisung des Verantwortlichen zu verarbeiten (Art. 29 DS-GVO). Beim Einsatz von Google Analytics bestimmt der Website-Betreiber nicht allein über die Zwecke und Mittel der Datenverarbeitung. Diese werden vielmehr zum Teil ausschließlich von Google vorgegeben, sodass Google insoweit selbst verantwortlich ist, und vom Seitenbetreiber vertraglich akzeptiert. Die Verarbeitung beim Einsatz von Google Analytics stellt einen einheitlichen Lebenssachverhalt dar, in dem die verschiedenen Aspekte der Verarbeitung nur als Ganzes einen Sinn ergeben. Dies hat zur Folge, dass die Beteiligten innerhalb einer Verarbeitungstätigkeit nicht ihre Rolle als Auftragsverarbeiter und/oder Verantwortlicher wechseln können.

Zwar bietet Google weiterhin einen Vertrag zur Auftragsverarbeitung an, stellt aber zusätzlich in den „Google Measurement Controller-Controller Data Protection Terms“[1] klar, dass für bestimmte Verarbeitungsprozesse Google und der Anwender (Website-Betreiber) getrennt verantwortlich seien. Zudem stellt Google in den Nutzungsbedingungen[2] klar, dass Google die Daten für eigene Zwecke, insbesondere auch zum Zweck der Bereitstellung seines Webanalyse- und Trackingdienstes, verarbeite. Gemäß Artikel 28 Abs. 10 DS-GVO handelt es sich bei Google damit nicht mehr um einen Auftragsverarbeiter.

[1] Das „Google Measurement Controller-Controller Data Protection Terms“, abrufbar unter: https://support.google.com/analytics/answer/9012600, Fassung vom 4. November 2019, Ziff. 4, gilt u.a. für den Fall, dass Google-Produkte und –Dienste in den Einstellungen zur Datenfreigabe aktiviert sind.
[2] Abrufbar unter: https://marketingplatform.google.com/about/analytics/terms/de/, Fassung vom 17. Juni 2019, Ziff. 6, 7

Unter Berücksichtigung der aktuellen Rechtsprechung des EuGH sind Google und der Google-Analytics-Anwender gemeinsam für die Datenverarbeitung verantwortlich, sodass die Anforderungen des Art. 26 DS-GVO zu beachten sind.

III. Rechtsgrundlage

Der Einsatz von Google Analytics kann in aller Regel nicht auf Art. 6 Abs. 1 lit. b) DS-GVO gestützt werden, da der Einsatz von Google Analytics nicht zur Vertragserfüllung zwischen Website-Betreiber und Nutzer erforderlich ist.

Der Einsatz von Google Analytics ist *in der Regel* auch nicht nach Art. 6 Abs. 1 lit. f) DS-GVO rechtmäßig. Angesichts der konkreten Datenverarbeitungsschritte beim Einsatz von Google Analytics überwiegen die Interessen, Grundrechte und Grundfreiheiten der Nutzer regelmäßig die Interessen der Website-Betreiber. Insbesondere rechnet der Nutzer vernünftigerweise nicht damit, dass seine personenbezogenen Daten mit dem Ziel der Erstellung personenbezogener Werbung und der Verknüpfung mit den aus anderen Zusammenhängen gewonnenen personenbezogenen Daten an Dritte weitergegeben und umfassend ausgewertet werden.[1] Dies geht weit über das hinaus, was im Rahmen des Art. 6 Abs. 1 lit. f) DS-GVO zulässig ist.[2] Die Situation weicht insoweit erheblich von dem Fall einer Statistik-Funktion auf der eigenen Website oder mittels Auftragsverarbeitung ab.

Google verpflichtet in den vertraglichen Regelungen den Anwender von Google Analytics, unter bestimmten Voraussetzungen für den Einsatz des Dienstes eine Einwilligung der Besucher der

[1] Datenschutzerklärung von Google unter: https://policies.google.com/privacy, Fassung wirksam ab dem 15. Oktober 2019, unter der Überschrift „Messung der Leistung“.
[2] Nähere Erläuterungen in der „Orientierungshilfe für Anbieter von Telemedien“.

Webseite einzuholen.[1] Die Datenschutzaufsichtsbehörden weisen ausdrücklich darauf hin, dass es für den rechtmäßigen Einsatz von Google Analytics nicht auf die vertraglichen Vereinbarungen zwischen Google und dem Anwender ankommt. Die Rechtmäßigkeit richtet sich ausschließlich nach dem Gesetz.

Im Ergebnis ist ein rechtmäßiger Einsatz von Google Analytics in der Regel nur aufgrund einer wirksamen Einwilligung der Webseitenbesuchenden gem. Art. 6 Abs. 1 lit. a), Art. 7 DS-GVO möglich.

IV. Maßnahmen

Sofern Website-Betreiber nicht auf alternative und datensparsame Werkzeuge zur Reichweitenmessung ausweichen, sondern weiterhin Google Analytics verwenden, sind insbesondere folgende Maßnahmen umzusetzen:

1) Einholung einer informierten, freiwilligen, aktiven und vorherigen Einwilligung der Nutzer

Eine Einwilligung ist nur wirksam, wenn die Anforderungen gem. Art. 4 Nr. 11, Art. 7 DS-GVO und ggf. Art. 8 DS-GVO erfüllt sind. Das bedeutet insbesondere:

- Website-Betreiber müssen sicherstellen, dass die Einwilligung die **konkrete Verarbeitungstätigkeit** durch die Einbindung

[1] Vgl. „Nutzungsbedingungen“, abrufbar unter: https://marketingplatform.google.com/about/analytics/terms/de/, Fassung vom 17. Juni 2019;
„Richtlinienanforderungen für Google Analytics-Werbefunktionen“, abrufbar unter: https://support.google.com/analytics/answer/2700409, Fassung vom 16. Dezember 2016;
„Richtlinie zur Einwilligung der Nutzer in der EU“, abrufbar unter: https://www.google.com/about/company/user-consent-policy.html, ohne Datum, zuletzt abgerufen am 23. Januar 2020.

von Google Analytics und damit verbundene Übermittlungen des Nutzungsverhaltens an Google LLC erfasst.

- In der Einwilligung muss **klar und deutlich** beschrieben werden, dass die Datenverarbeitung im Wesentlichen durch Google erfolgt, die Daten nicht anonym sind, welche Daten verarbeitet werden und dass Google diese zu beliebigen eigenen Zwecken wie zur Profilbildung nutzt sowie mit anderen Daten wie eventueller Google-Accounts verknüpft. Ein bloßer Hinweis wie z.B. „diese Seite verwendet Cookies, um Ihr Surferlebnis zu verbessern“ oder „verwendet Cookies für Webanalyse und Werbemaßnahmen“ ist nicht ausreichend, sondern irreführend, weil die damit verbundenen Verarbeitungen nicht transparent gemacht werden.
- Nutzer müssen **aktiv** einwilligen, d.h. die Zustimmung darf nicht unterstellt und ohne Zutun des Nutzers voreingestellt sein. Ein Opt-Out-Verfahren reicht nicht aus, vielmehr muss der Nutzer durch aktives Tun (z. B. Anklicken eines Buttons) seine Zustimmung zum Ausdruck bringen. Google muss ausdrücklich als Empfänger der Daten aufgeführt werden. Vor einer aktiven Einwilligung des Nutzers dürfen keine Daten erhoben oder Elemente von Google-Websites nachgeladen werden. Auch das bloße Nutzen einer Website (oder einer App) stellt keine wirksame Einwilligung dar.
- **Freiwillig** ist die Einwilligung nur, wenn die betroffene Person Wahlmöglichkeiten und eine freie Wahl hat. Sie muss eine Einwilligung auch verweigern können, ohne dadurch Nachteile zu erleiden. Die Koppelung einer vertraglichen Dienstleistung an die Einwilligung zu einer für die Vertragserbringung nicht erforderlichen Datenverarbeitung kann gemäß Art. 7 Abs. 4 DS-GVO dazu führen, dass die Einwilligung nicht freiwillig und damit unwirksam ist.

Um die Anforderungen einer wirksamen Einwilligung auf Websites oder in Apps umzusetzen, sind folgende Gestaltungshinweise zu beachten:

- **Klare, nicht irreführende Überschrift** – bloße „Respektbekundungen“ bezüglich der Privatsphäre reichen nicht aus. Es empfehlen sich Überschriften, in denen auf die Tragweite der Entscheidung eingegangen wird, wie beispielsweise *„Datenverarbeitung Ihrer Nutzerdaten durch Google“*.
- **Links** müssen **eindeutig** und unmissverständlich beschrieben sein – wesentliche Elemente/Inhalte insbesondere einer Datenschutzerklärung dürfen nicht durch Links verschleiert werden.
- Der **Gegenstand** der Einwilligung muss **deutlich gemacht** werden: Anwender von Google Analytics müssen deutlich machen, für welchen Zweck Google Analytics verwendet wird, dass die Nutzungsdaten von Google LLC verarbeitet werden, diese Daten in den USA gespeichert werden, sowohl Google als auch staatliche Behörden Zugriff auf diese Daten haben, diese Daten mit anderen Daten des Nutzers wie beispielsweise dem Suchverlauf, persönlichen Accounts, den Nutzungsdaten anderer Geräte und allen anderen Daten, die Google zu diesem Nutzer vorliegen, verknüpft werden.
- Der **Zugriff auf das Impressum und die Datenschutzerklärung** darf nicht verhindert oder eingeschränkt werden.

2) Technische Anforderungen an die Umsetzung des Widerrufs der Einwilligung

Beim Einsatz von Google Analytics muss stets ein einfach und immer zugänglicher Mechanismus (z. B. Schaltfläche) zum Widerruf der einmal vom Nutzer erteilten Einwilligung implementiert sein. Gleiches gilt für Apps, die zum Beginn der Nutzung eine Einwilligung erfragen. Auch hier muss in den Einstellungen eine einfach zugängliche Möglichkeit zum wirksamen Widerruf der Einwilligung vorhanden sein.

Hatte ein Nutzer einmal seine Einwilligung erteilt und widerruft er sie zu einem späteren Zeitpunkt, so ist sicherzustellen, dass

nach dem Widerruf das Google-Analytics-Skript nicht nachgeladen oder ausgeführt wird.

Google stellt ein Browser-Add-On zur Deaktivierung von Google Analytics zur Verfügung. Es ist nicht zulässig, den Nutzer ausschließlich auf dieses Add-On zu verweisen, da dies keine hinreichende Widerrufsmöglichkeit darstellt. Gemäß Art. 7 Abs. 3 S. 4 DS-GVO ist der Widerruf so einfach wie die Erteilung der Einwilligung zu gestalten. Das von Google zur Verfügung gestellte Add-On erfüllt diese Anforderungen nicht, da der Nutzer zum Herunterladen von weiteren Programmen gezwungen wird. Im Übrigen entspricht das Add-On aufgrund der Vielzahl an Browsern und Betriebssystemen weder dem Stand der Technik noch ist es geeignet, um die Datenverarbeitung in Apps zu unterbinden.

3) Transparenz

Anwender müssen gemäß Art. 13 DS-GVO die Nutzer in den Datenschutzbestimmungen umfassend über die Verarbeitung personenbezogener Daten im Rahmen von Google Analytics informieren. Bezüglich der Anforderungen an diese Informationspflicht wird auf die Leitlinie zur Transparenz[1] des Europäischen Datenschutzausschusses sowie auf die Orientierungshilfe für Anbieter von Telemedien verwiesen.

4) Kürzung der IP-Adresse

Zusätzlich zu den o. g. Maßnahmen sollten Anwender von Google Analytics durch entsprechende Einstellungen die Kürzung der IP-Adressen veranlassen. Dazu ist auf jeder Internetseite mit einer Google Analytics-Einbindung der Trackingcode um die Funktion „_anonymizeIp()“ zu ergänzen. Weitere Details können der technischen Anleitung von Google entnommen werden,

[1] Abrufbar unter: https://www.datenschutzkonferenz-online.de/media/wp/20180411_wp260_rev01.docx 6

abrufbar unter: https://developers.google.com/analytics/devguides/collection/gtagjs/ip-anonymization.

Die Kürzung der IP-Adresse stellt eine zusätzliche Maßnahme gem. Art. 25 Abs. 1 DS-GVO zum Schutz der Nutzer dar, sie führt jedoch nicht dazu, dass die vollständige Datenverarbeitung anonymisiert erfolgt. Beim Einsatz von Google Analytics werden neben der IP-Adresse weitere Nutzungsdaten erhoben, die als personenbezogene Daten zu bewerten sind, wie z. B. Identifizierungsmerkmale der einzelnen Nutzer, die auch eine Verknüpfung beispielsweise mit einem vorhandenen Google-Account erlauben. Aus diesem Grund ist in jedem Fall der Anwendungsbereich der DS-GVO eröffnet, sodass Anwender von Google Analytics auch dann verpflichtet sind, die Anforderungen der DS-GVO zu beachten, wenn sie die Kürzung der IP-Adressen veranlasst haben. In der Datenschutzerklärung ist der Umstand, ob die Kürzung der IP-Adressen veranlasst ist, entsprechend anzugeben.

Im Übrigen gelten die Ausführungen der Orientierungshilfe für Anbieter von Telemedien.

- **12.05.2020 – Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Vorabwidersprüche bei StreetView und vergleichbaren Diensten**

  Für die Veröffentlichung von Straßenansichten, einschließlich teilweiser Abbildungen von Häuserfassaden und privaten Grundstücksbereichen, welche an den öffentlichen Straßenraum angrenzen, kann im Rahmen von StreetView und ähnlichen Diensten Art. 6 Abs. 1 Unterabsatz 1 lit. f DSGVO als Rechtsgrundlage in Betracht kommen. Dabei dürfen nur die personenbezogenen Daten veröffentlicht werden, die für die Zweckerreichung zwingend erforderlich sind, so sind Merkmale, die die Identifizierung einer Person ermöglichen, insbesondere Gesichter und KFZ-Kennzeichen, unkenntlich zu machen. Dies ergibt sich bereits

aus Art. 5 Abs. 1 lit. c DS-GVO (Grundsatz der Datenminimierung). Zudem hat der Anbieter vor Beginn der Aufnahmen die Öffentlichkeit in geeigneter Weise zu informieren. Im Rahmen der Interessenabwägung ist ein Verlangen betroffener Personen auf Unkenntlichmachung personenbezogener Daten zu berücksichtigen. Dieses Verlangen kann zumindest ab dem Zeitpunkt der Anfertigung der Aufnahmen durch den Dienst wahrgenommen werden und umfasst auch Abbildungen von Häuserfassaden und privaten Grundstücksbereichen. Art. 21 DS-GVO bleibt unberührt.

Das Verlangen auf Unkenntlichmachung nach Art. 17 Abs. 1 DS-GVO und der Widerspruch nach Art. 21 DS-GVO müssen sowohl online als auch postalisch eingelegt werden können. Auf diese Rechte muss ausdrücklich hingewiesen werden.

- **10.09.2020 – Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie**

  I. AUSGANGSLAGE

  Da eine SARS-CoV-2-Infektion teilweise mit einer spezifisch erhöhten Körpertemperatur der infizierten Person einhergeht, werden zunehmend elektronische Geräte zur Temperaturerfassung als Mittel der Zutrittssteuerung zu bis dahin öffentlich zugänglichen Räumen oder zu Arbeitsstätten eingesetzt.

  Eine kontaktlose Temperaturmessung erfolgt in der Regel per Infrarotmessung und wird entweder mithilfe eines Fieberthermometers oder einer Thermalkamera / Infrarot-Wärmebildkamera[1] vorgenommen. In den nunmehr angedachten Szenarien für den Zugang zu Flughäfen, Geschäften, Behörden, Arbeitsstätten etc. wird insbesondere die Nutzung von Wärmebildkameras in Betracht gezogen, da mittels klassischer Fieberthermometer keine

[1] Sofern im Folgenden allein der Einsatz von Wärmebildkameras oder der elektronischen Temperaturerfassung thematisiert wird, beziehen sich die Ausführungen grundsätzlich stets auf beide Verarbeitungsarten.

Temperaturmessung bei größeren Gruppen erfolgen kann. Sie kann höchstens für die Messung von Einzelpersonen nacheinander, wie z.B. in Vereinzelungsschleusen zum Einsatz kommen, wobei bei einer einzelnen Fiebermessung mittels Thermometer ohne Protokollierung abhängig vom Einsatzszenario die Anwendbarkeit der Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) in Frage stehen kann. **Einzelhandelsunternehmen und Behörden setzen bereits vergleichbare Wärmemessungen ein, um den Zutritt zu ihren Geschäftsräumen zu regulieren.**

ANWENDUNGSBEREICH DES BESCHLUSSES

Der Beschluss betrifft den Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung zur Steuerung oder aus Anlass des Zugangs zu Flughäfen, Geschäften, Behörden und Arbeitsstätten im Rahmen der Corona-Pandemie. Ein**richtungen im Bereich der Gesundheitsversorgung einschließlich der Pflege können besonderen Maßnahmen unterliegen.**

II. ZUSAMMENFASSUNG

Für die elektronische Messung der Körpertemperatur zur allgemeinen Regulierung des Zutritts zu Flughäfen, Geschäften, Behörden und Arbeitsstätten kann zwar Art. 6 Abs. 1 UAbs. 1 Buchst. e, Art. 9 Abs. 2 DSGVO i. V. m. § 3 BDSG und vergleichbaren Vorschriften in den Landesdatenschutzgesetzen (Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe) bzw. Art. 6 Abs. 1 UAbs. 1 Buchst. f, Art. 9 Abs. 2 DSGVO (Verfolgung eines berechtigten Interesses) als Rechtsgrundlage in Betracht kommen. Auch ist die Messung als betriebliche Maßnahme des Arbeitsschutzes bzw. zur Beurteilung der Arbeitsfähigkeit gestützt auf Art. 88 DSGVO i. V. m. § 26 Abs. 3 BDSG (bzw. das Personaldatenschutzrecht des jeweiligen Landes) bzw. § 22 Abs. 1 Nr. 1 Buchst. b BDSG i.V.m. Art. 9 Abs. 2 DSGVO grundsätzlich denkbar. Jedoch fehlt es i.d.R. an der Eignung und

der Erforderlichkeit der Messung. Denn eine erhöhte Körpertemperatur kann nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infektion angesehen werden, und viele Infizierte weisen keine Symptome und damit auch keine erhöhte Temperatur auf. Zudem sind mildere Maßnahmen wie z. B. die Einhaltung der Hygiene- und Abstandsbestimmungen und die anlassbezogene Befragung der Beschäftigten durch den Arbeitgeber denkbar.

III. DATENSCHUTZRECHTLICHE BEWERTUNG

Die elektronische Messung der Körpertemperatur fällt - jedenfalls typischerweise - in den **Anwendungsbereich** der Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO).

Die Messung der Körpertemperatur eines Menschen stellt eine Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 1 und Nr. 2 DSGVO dar.

Lässt ein Verantwortlicher Körpertemperaturmessungen an Personen vornehmen, sind hierdurch regelmäßig **personenbezogene Daten** betroffen. Zwar erfassen die Temperaturmessungen selbst noch keine eindeutig identifizierenden Angaben wie Namen und Anschriften der Personen, die eine entsprechende Messeinrichtung passieren. Typischerweise kann jedoch die betroffene Person dabei anderweitig identifiziert werden, etwa durch Personal, das die Messungen und eventuell Aufzeichnungen vornimmt, durch den Einsatz von Videokameras oder durch Arbeitszeiterfassungsgeräte. Anderes könnte allenfalls gelten, wenn eine automatisierte Temperaturmessung stattfindet, die vollkommen ohne Protokollierung und ohne anderweitige Zuordnung der Werte zu bestimmten oder bestimmbaren Personen erfolgt. Im Zusammenhang mit der Corona-Pandemie würde eine solche Messung allerdings ihren präventiven Zweck verfehlen.

In aller Regel sind die mithilfe einer automatisierten Temperaturmessung erzeugten Daten also personenbezogene Daten im

Sinne von Art. 4 Nr. 1 DSGVO. Erst recht unterstützt die Speicherung von Infrarotkamera-Aufnahmen eine nachträgliche persönliche Identifikation betroffener Personen. Wird eine Wärmebilderfassung gar mit einer herkömmlichen Videoüberwachung verknüpft, ist generell von einem Personenbezug der Bildaufnahmen auszugehen (vgl. BVerwG, Urteil vom 27.03.2019, Az. 6 C 2/18, Absatz 43 der Entscheidungsbegründung).

Die Anwendung der Datenschutz-Grundverordnung setzt nach Art. 2 Abs. 1 DSGVO weiterhin voraus, dass entweder eine automatisierte **Verarbeitung** oder eine nichtautomatisierte Verarbeitung personenbezogener Daten erfolgt, die in einem Dateisystem gespeichert werden oder werden sollen.

Beispiel: Die Erfassung der Körpertemperatur mithilfe eines Wärmebildkamerasystems ist eine automatisierte Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DSGVO – unabhängig davon, ob die Aufnahmen gespeichert werden oder ob ein Live-Monitoring erfolgt (vgl. BVerwG, Urteil vom 27.03.2019, a.a.O., Absatz 43 der Entscheidungsbegründung).

Ausgehend von den beschriebenen Einsatzbedingungen der elektronischen Temperaturerfassung setzen die nachfolgenden Ausführungen die Anwendbarkeit der Datenschutz-Grundverordnung voraus. Sie beziehen sich allerdings nicht auf solche Temperaturmessungen, für die der Anwendungsbereich der Datenschutz-Grundverordnung ausnahmsweise nicht eröffnet ist.

Da die elektronische Temperaturmessung darauf gerichtet ist, Personen zu identifizieren, die mit SARS-CoV-2 infiziert sind, handelt es sich um eine Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DSGVO. Soweit eine solche Verarbeitung von personenbezogenen Gesundheitsdaten erfolgt, ist sie nach Art. 9 Abs. 1 DSGVO grundsätzlich verboten. Dieses **grundsätz-**

liche Verarbeitungsverbot gilt nur dann nicht, wenn die Verarbeitung einen Ausnahmetatbestand des Art. 9 Abs. 2 DSGVO erfüllt.

Im Folgenden werden daher die je nach Anwendungsfall in Betracht kommenden Rechtsgrundlagen näher untersucht, beginnend mit den allgemeinen Verarbeitungsbefugnissen.

Dabei ist neben dem grundsätzlichen Verarbeitungsverbot und den Ausnahmetatbeständen des Art. 9 DSGVO zu beachten, dass eine Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 Buchstabe a, Art. 6 Abs. 1 UAbs. 1 DSGVO nur dann rechtmäßig ist, wenn sie mindestens auf eine **Rechtsgrundlage** im Sinne des Art. 6 Abs. 1 DSGVO gestützt werden kann. Bei der elektronischen Temperaturmessung ist dies regelmäßig **nicht** gegeben. Folgende Erwägungen sind diesbezüglich zu beachten:

- Eine **Einwilligung** im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe a DSGVO kann nur wirksam erteilt werden, wenn die Voraussetzungen der Art. 4 Nr. 11, Art. 7 DSGVO erfüllt sind (zu Einzelheiten vgl. Datenschutzkonferenz, Kurzpapier Nr. 20, Einwilligung nach der DSGVO; Europäischer Datenschutzaus-schuss, WP 259 rev. 01: Leitlinien in Bezug auf die Einwilligung gemäß Verordnung EU 2016/679). Zudem ist zu beachten, dass die Wärmemessung gerade der Erfassung einer etwaigen Erkrankung dient; deshalb hat die betroffene Person ihre Einwilligung ausdrücklich zu erklären (vgl. Art. 9 Abs. 2 Buchstabe a DSGVO).

  Im Zusammenhang mit der Zielsetzung der Zutrittsregulierung mithilfe von Wärmebildmessungen wird die Einwilligung als Verarbeitungsgrundlage schon in praktischer Hinsicht oft ausscheiden, weil es an der **Freiwilligkeit** der Zustimmungserklärung fehlt. Zudem wird die Wirksamkeit der Einwilligung häufig auch daran scheitern, dass eine transparente **Information** der betroffenen Person vor Durchführung des Messvorganges in der Praxis zweifelhaft scheint.

Beispiel: Zahlreiche Beschäftigungsverhältnisse sind stark von einem Ungleichgewicht zwischen den Beschäftigten und ihrem Arbeitgeber bzw. Dienstherrn geprägt (Erwägungsgrund 43 DSGVO). Vor diesem Hintergrund werden die Beschäftigten kaum eine vom Vorgesetzten etablierte Zutrittskontrolle verweigern können, wenn sie zu ihrem Arbeitsplatz gelangen wollen. Anderes kann ausnahmsweise gelten, wenn Arbeitgeber bzw. Dienstherren etwa mithilfe von Betriebs- bzw. Dienstvereinbarungen die Rahmenbedingungen für die Freiwilligkeit einer Einwilligungserklärung von Beschäftigten festlegen.

Beispiel: Die Zutrittsregelung betreffend Behörden- oder Gerichtsgebäuden kann typischerweise nicht auf die Einwilligung gestützt werden, sofern die betroffenen Personen eine gesetzlich vorgesehene, staatliche Leistung in Anspruch nehmen wollen oder gar auf behördliche oder gerichtliche Ladung hin den Zutritt zum jeweiligen Gebäude begehren. Denn insoweit ist die Freiwilligkeit einer Zustimmung stets zweifelhaft und kann durch den Verantwortlichen regelmäßig nicht belegt werden (vgl. Art. 7 Abs. 1, Erwägungsgrund 43 DSGVO). Beispiel: In Bezug auf den Zutritt zum Geschäftslokal eines Unternehmens wird die Einholung einer hier nach Art. 9 Abs. 2 Buchstabe a DSGVO rechtlich gebotenen ausdrücklichen Einwilligung der Kunden häufig bereits aus pragmatischen Erwägungen nicht in Frage kommen. Zudem hängt die Freiwilligkeit auch dann von den Umständen des Einzelfalls ab, wobei die gesetzliche Wertung des Art. 7 Abs. 4 DSGVO zu beachten ist. [1]Soweit der Zutritt zum Geschäftslokal an die Einwilligung zur Temperaturmessung geknüpft wird, kann also nicht ohne weiteres von einer Freiwilligkeit ausgegangen werden.

[1] EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, Rn. 14.

- Auch Art. 6 Abs. 1 UAbs. 1 Buchstabe b DSGVO scheidet als Rechtsgrundlage in aller Regel aus. Bei Zugangskontrollen erfolgt die Temperaturmessung nicht zur Erfüllung eines bestehenden Vertragsverhältnisses zwischen den Parteien.

  Als Verarbeitungsgrundlage kommt der Vertrag am ehesten **bei Beschäftigungsverhältnissen im nichtöffentlichen Sektor und bei Tarifbeschäftigten des öffentlichen Sektors** in Betracht. Insoweit sieht Art. 9 Abs. 2 Buchstabe b DSGVO unter den dort festgelegten Voraussetzungen u.a. eine Ausnahme vom Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO vor, soweit der Verantwortliche oder die betroffene Person einer aus dem Arbeitsrecht folgenden Pflicht nachkommen muss. In Bezug auf die elektronische Temperaturmessung bei Beschäftigten kommt allenfalls in Betracht, dass mit ihr der Arbeitgeber bzw. Dienstherr seine aus dem Arbeitsschutzrecht folgenden Pflichten erfüllen will.

  Eine solche vertragliche Befugnis zur Temperaturmessung kann allerdings nicht weiter reichen als eine rechtliche Verpflichtung des Verantwortlichen im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO.

- Teilweise berufen sich Unternehmen bei der Temperaturmessung darauf, sie sei erforderlich, um eine **rechtliche Verpflichtung** im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO zu erfüllen. Diese Vorschrift stellt selbst keine rechtliche Verarbeitungsgrundlage dar, sondern setzt gemäß Art. 6 Abs. 2, Abs. 3 UAbs. 1 DSGVO eine Rechtsgrundlage im bereichsspezifischen EU-Recht oder im Recht eines Mitgliedstaates voraus. Die in dieser Vorschrift normierte Verpflichtung muss sich unmittelbar auf die Verarbeitung personenbezogener Daten beziehen. Allein der Umstand, dass ein Verantwortlicher, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, reicht demgegenüber nicht aus (vgl. z.B. LSG Hessen, Beschluss vom 29.01.2020, Az. L 4 SO 154/19 B, Absatz 13 der

Entscheidungsgründe). Eine solche rechtliche Verpflichtung der Unternehmen zur Temperaturmessung ist im deutschen Recht nicht ausdrücklich vorgesehen. In Beschäftigungsverhältnissen verpflichtet § 3 Abs. 1 Arbeitsschutzgesetz den Arbeitgeber zwar allgemein dazu, die erforderlichen Maßnahmen des Arbeitsschutzes „*unter Berücksichtigung der Umstände zu treffen, die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen.*“ Ferner ist der Arbeitgeber nach § 618 Bürgerliches Gesetzbuch grundsätzlich verpflichtet, Maßnahmen zum Schutz von Leben und Gesundheit seiner Beschäftigten zu ergreifen. Aus diesen allgemeinen gesetzlichen Vorgaben zum betrieblichen Gesundheitsschutz lässt sich jedoch gerade nicht eine konkrete rechtliche Pflicht im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO ableiten, den Zugang zum Betriebsgelände mithilfe einer elektronischen Temperaturmessung zu regulieren.

Auch unter Berücksichtigung des am 16. April 2020 durch das Bundesministerium für Arbeit und Soziales veröffentlichten „Arbeitsschutzstandard SARS-CoV-2“ oder der sonstigen bereichs- und branchenspezifischen Arbeitsschutz-standards ergibt sich nichts anderes. Ungeachtet dessen, dass darin Temperaturmessungen als betriebliche Maßnahme in Betracht gezogen werden sollen (II. Nr. 13 des Arbeitsschutzstandards SARS-CoV-2: „*insbesondere Fieber, Husten und Atemnot … Anzeichen für eine Infektion mit dem Coronavirus sein (können). Hierzu ist im Betrieb eine möglichst kontaktlose Fiebermessung vorzusehen.*“), begründen sie keine rechtliche Verpflichtung des Arbeitgebers oder Dienstherrn im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO, im Wege der Fiebermessung personenbezogene Daten zu verarbeiten. Denn die Arbeitsschutzstandards SARS-CoV-2 sind kein Rechtssatz, aus denen eine rechtliche Verpflichtung folgt, sondern eine Art Leitlinie der öffentlichen Verwaltung zum Arbeitsschutz.

Damit existiert gegenwärtig keine spezifische rechtliche Verpflichtung für Verantwortliche im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe c DSGVO, elektronische Fiebermessungen durchzuführen.

- Art. 6 Abs. 1 UAbs. 1 Buchstabe d DSGVO gestattet die Verarbeitung personenbezogener Daten, wenn sie erforderlich ist, um **lebenswichtige Interessen der betroffenen Person** oder einer anderen natürlichen Person zu schützen. Bei der im Raum stehenden Verarbeitung von personenbezogenen Gesundheitsdaten durch elektronische Temperaturmessung muss allerdings gem. Art. 9 Abs. 2 Buchstabe c DSGVO die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande sein, ihre Einwilligung in die Verarbeitung zu geben, sodass diese Rechtsgrundlage **nicht** herangezogen werden kann.
- Hingegen kommt in einzelnen Fällen in Betracht, dass die Temperaturmessung für die Wahrnehmung einer **im öffentlichen Interesse liegenden Aufgabe** erforderlich ist, die dem Verantwortlichen übertragen wurde. Dazu stellt Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO selbst keine Verarbeitungsbefug-nis dar, sondern setzt nach Art. 6 Abs. 2 und 3 UAbs. 1 DSGVO eine Rechtsgrundlage voraus. Eine solche Verarbeitungsgrundlage kann grundsätzlich auch in einer Generalklausel bestehen; insbesondere muss sie von EU-Rechts wegen nicht, wie bei der Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung, konkret den Verarbeitungszweck enthalten. Es genügt nach Art. 6 Abs. 3 UAbs. 2 DSGVO, wenn der Zweck der Verarbeitung erforderlich ist, um eine Aufgabe zu erfüllen, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt. Dies setzt immerhin voraus, dass eine solche Aufgabe im Recht des Mitgliedstaats so klar und konkret beschrieben wird, dass aus ihr rechtssicher ein zulässiger Verarbeitungszweck abgeleitet werden kann. Insbesondere darf die gesetzliche Zuständigkeits- und Aufgabenordnung

nicht durch zu unbestimmte Verarbeitungsregeln unterlaufen werden.
Daraus folgt, dass die Verarbeitung aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit gemäß Art. 9 Abs. 2 Buchstabe i DSGVO, § 22 Abs. 1 Nr. 1 Buchstabe c Bundesdatenschutzgesetz (BDSG) keine allgemeine Befugnis von Behörden für die Verarbeitung von Gesundheitsdaten begründet. Diese Vorschriften beziehen sich ihrem Wortlaut und ihrer Entstehungsgeschichte nach auf das öffentliche Gesundheitswesen und auf die Gesundheitsverwaltung.

Dient die Temperaturmessung allerdings der allgemeinen **Zutrittsregulierung zu Gebäuden der öffentlichen Verwaltung**, kommt mangels bereichsspezifischer Vorschriften der Rückgriff auf die datenschutzrechtlichen Generalklauseln in § 3 BDSG und vergleichbaren Vorschriften in den Landesdatenschutz-gesetzen in Betracht. Anknüpfungspunkt wäre insoweit die Aufgabe einer jeder öffentlichen Stelle, einen ordnungsgemäßen – das heißt auch für Besucherinnen und Besucher sowie Beschäftigte möglichst gefahrlosen – Dienst-betrieb zu gewährleisten. Zusätzlich muss eine Verarbeitungsbefugnis im Hinblick auf die nach Art. 9 Abs. 2 DSGVO besonders geschützten Gesundheits-daten vorliegen (etwa, soweit anwendbar, § 22 Abs. 1 Nr. 1 Buchstabe d 10 BDSG). Dabei ist regelmäßig der Grundsatz der Erforderlichkeit zu berücksichtigen, anhand dessen zu prüfen ist, ob das Fiebermessen tatsächlich erforderlich und zielführend zur Erreichung des Zwecks ist. Für die Prüfung der Erforderlichkeit sind Konzepte zu erstellen, die die beabsichtigten Maßnahmen und die damit verfolgten Zwecke schlüssig und nachvollziehbar darlegen. Zusätzlich haben die Behörden dabei die besonderen Regeln zum Schutz sensibler Daten zu beachten. An der Eignung und Erforderlichkeit einer elektronischen Fiebermessung bestehen allerdings erhebliche Zweifel; diese werden weiter unten im

Zusammenhang mit den Ausführungen zu Art. 6 Abs. 1 UAbs.1 Buchstabe f DSGVO näher erörtert.

Die Steuerung des Zutritts zu öffentlichen Verkaufsflächen von Unternehmen lässt sich hingegen regelmäßig **nicht** auf Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO in Verbindung mit der jeweiligen mitgliedstaatlichen Befugnisnorm stützen. **Unternehmen und andere nichtöffentliche Verantwortliche** können sich auf diese Vorschrift nur berufen, wenn ihnen eine Verarbeitungsbefugnis im öffentlichen Interesse oder als Ausübung öffentlicher Gewalt „über-tragen“ ist. Sie müssen anstelle einer Behörde tätig werden, was einen wie auch immer gearteten staatlichen Übertragungsakt voraussetzt. Mit anderen Worten können sich Privatpersonen nicht selbst zum Sachwalter eines öffentlichen Interesses erklären. Deshalb scheidet die Wahrnehmung einer öffentlichen Aufgabe im Sinne des Art. 6 Abs. 1 UAbs. 1 Buchstabe e DSGVO für nichtöffentliche Verantwortliche gegenwärtig als Verarbeitungsgrund aus (vgl. BVerwG, Urteil vom 27.03.2019, a.a.O., Absatz 46 der Entscheidungsbegründung).

- Für Unternehmen und andere nichtöffentliche Stellen steht allerdings Art. 6 Abs. 1 UAbs. 1 Buchstabe f DSGVO zur Verfügung, der – verkürzt ausgedrückt – eine **Verarbeitung auf Grundlage einer Interessenabwägung** dann erlaubt, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und nicht die Interessen der betroffenen Person überwiegen. Verantwortliche des öffentlichen Sektors können sich im Rahmen ihrer Aufgabenerfüllung nicht auf diese Verarbeitungsgrundlage stützen, vgl. Art. 6 Abs. 1 UAbs. 2 DSGVO.

  Im Zusammenhang mit der elektronischen Fiebermessung ist wiederum zu beachten, dass sie als Verarbeitung personenbezogener Gesundheitsdaten nur zulässig sein kann, wenn eine Ausnahme vom grundsätzlichen Verarbeitungsverbot nach Art. 9 Abs. 2 DSGVO besteht. Eine solche Ausnahme ist jedoch allenfalls in seltenen Ausnahmefällen denkbar.

Die Verarbeitungsgrundlage des Art. 6 Abs. 1 UAbs. 1 Buchstabe f DSGVO setzt nach gefestigter Rechtsprechung drei Prüfschritte voraus (vgl. u.a. EuGH, Urteil vom 04.05.2017, Az. C-13/16, Absatz 28 der Entscheidungs-gründe):

Erstens muss die Verarbeitung ein berechtigtes Interesse verfolgen, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses erforderlich sein und drittens dürfen die Interessen, Grundrechte und Grundfreiheiten der betroffenen Person nicht das Verarbeitungsinteresse des Verantwortlichen überwiegen.

Ein **berechtigtes Verarbeitungsinteresse** ist vorliegend zu bejahen, soweit die mit der elektronischen Fiebermessung verbundene Erhebung von Daten zur Abwehr von Gefährdungen für die Belegschaft bzw. der übrigen Kundschaft und damit auch der Aufrechterhaltung des Geschäftsbetriebs dienen soll.

Die **Erforderlichkeit** der Maßnahme hingegen ist regelmäßig nicht zu bejahen. Soweit die Veröffentlichung der Datenschutzkonferenz „Datenschutz-rechtliche Informationen zur Verarbeitung von personenbezogenen Daten durch Arbeitgeber und Dienstherren im Zusammenhang mit der Corona-Pandemie“ insoweit für die Ermittlung der Erforderlichkeit verallgemeinerungsfähig darauf hinweist, dass – unter Beachtung des Gebots der Verhältnismäßigkeit – die „*Erhebung und Verarbeitung personenbezogener Daten (einschließlich Gesundheitsdaten) von Gästen und Besuchern legitim sein könne, insbesondere um festzustellen, ob diese selbst infiziert sind oder im Kontakt mit einer nachweislich infizierten Person standen oder sich im relevanten Zeitraum in einem vom RKI als Risikogebiet eingestuften Gebiet aufgehalten haben*“, beschränkt sich dies auf die zulässige Datenverarbeitung im **un-**

mittelbaren Kontext der mit dem Pandemiegeschehen verbundenen Gesundheitsgefahren. Vor diesem Hintergrund sind Befragungen und auch weitergehende Maßnahmen nicht generell ausgeschlossen, allerdings ist das Tatbestandsmerkmal der Erforderlichkeit im spezifischen Verarbeitungszusammenhang zu beachten.

Bei der Erforderlichkeitsprüfung ist zu beachten, dass eine erhöhte Körpertemperatur nicht zwangsläufig als symptomatisch für eine SARS-CoV-2-Infek-tion angesehen werden kann. Sie kann auch durch zahlreiche andere Ursachen, wie etwa Erkältungen, Stoffwechsel- und Gefäßerkrankungen, Rheuma, entzündliche Prozesse bedingt sein. Zudem weisen nach Angaben des Robert Koch-Instituts (RKI) nur etwa 41 Prozent der Infizierten einen Krankheits-verlauf mit Fieber auf; in der bis zu 14 Tage umfassenden Inkubationszeit weisen die infizierten Personen noch keine Symptome auf oder bleiben über den gesamten Infektionsverlauf vollständig symptomfrei, sind aber aufgrund der Viruslast potentielle Überträger (vgl. https://www.rki.de/DE/Content/In-fAZ/N/Neuartiges_Coronavirus/Steckbrief.html#doc13776792bodyText2, Stand: 12.06.2020).

Ungeachtet dessen, dass Fieber grundsätzlich symptomatisch für eine SARS-CoV-2-Infektion sein kann, kann eine Temperaturmessung mit dem Ziel des Schutzes von Beschäftigten, Kunden oder Besuchern angesichts einer überwiegenden Anzahl symptomfreier Infektionsträger allenfalls als bedingt geeignet erachtet werden. Das RKI rät daher in seinem Epidemiologischen Bulletin 20/2020 vom 14.05.2020 von der Nutzung entsprechender Vorrichtungen an Flughäfen ab, da kein Mehrwert gesehen wird (https://www.rki.de/DE/Con-tent/Infekt/EpidBull/Archiv/2020/Ausgaben/20_20.pdf?__blob=publicationFile).

In diesem Zusammenhang kommt daher der Prüfung besondere Bedeutung zu, ob mildere, weniger eingriffsintensive

Maßnahmen zur Erreichung des verfolgten Zwecks, dem Schutz der Beschäftigten und Kunden, die gleichsam der Zweckerreichung dienen, ersichtlich sind. Angesichts dessen sind die üblichen Maßnahmen im **Einzelhandel**, wie etwa die Begrenzung der Kundenanzahl, das Anbringen von Hinweisschildern zu Verhaltensregeln und Zutrittsbeschränkungen, die Gewährleistung der Einhaltung von Mindestabständen, die Aufforderung zum Tragen eines Mundschutzes, die Anbringung von Trennwänden im Kassenbereich und an Verkaufstresen sowie die Implementierung von Hygienevorgaben zu nennen. Ein derartiges Maßnahmenpaket verspricht gerade auch im Hinblick auf die größere Gefahr der Virus-Exposition aufgrund nicht festgestellter symptomfrei Infizierter einen nachhaltigeren Schutz von Kunden und Beschäftigten als eine eingriffsintensive kameragestützte Erhebung von Gesundheitsdaten.

Im Ergebnis kann daher eine Erforderlichkeit der elektronischen Fieber-messung als Instrument der Zutrittsregulierung zu öffentlichen Verkaufs- und Verkehrsflächen, insbesondere im Bereich der Grundversorgung sowie für Bereiche, deren Nutzung für das tägliche Leben unabdingbar sind (z.B. Bahnhöfe, Flughäfen, Gebäude von Verwaltungsbehörden) nicht bejaht werden.

Bei der Fiebermessung als **betriebliche Maßnahme des Arbeitsschutzes** ist zu beachten, dass ihre rechtliche Zulässigkeit aufgrund der Konkretisierungs-klausel des Art. 88 DSGVO anhand des § 26 BDSG zu beurteilen ist. Für Beschäftigte des öffentlichen Sektors der Länder ist das Personaldatenschutzrecht des jeweiligen Landes maßgeblich; auf dieses wird nachfolgend aber nicht weiter eingegangen. Im Hinblick auf die Erforderlichkeit ist zu berücksichtigen, dass der Verantwortliche als Arbeitgeber bzw. Dienstherr die Feststellung einer erhöhten Körpertemperatur mit nachfolgenden Untersuchungen kombinieren kann, was die Eignung der Maßnahme

etwas erhöht. Nichtsdestotrotz ist im Hinblick auf die Erforderlichkeit zu berücksichtigen, dass symptomfreie Infektionsfälle durch eine elektronische Temperaturerfassung nicht aufgedeckt werden können. Im Übrigen bestünde – je nach Fragestellung und anlassbezogen – als mildere Maßnahme noch die Möglichkeit, nach gesundheitlichen Beeinträchtigungen der Arbeitsfähigkeit zu fragen, wenn dies wegen der Art der auszuübenden Tätigkeit oder der Bedingungen ihrer Ausübung eine wesentliche und entscheidende berufliche Anforderung darstellt. Danach ist anlassbezogen die Frage nach dem Gesundheitszustand eines Beschäftigten zulässig, wenn gezielt die Beschäftigung unzumutbar machende potenzielle Ausfallzeiten oder Einschränkungen der Tätigkeit bestehen oder zu erwarten sind. Weiterhin darf allgemein nach dem Vorliegen von ansteckenden Krankheiten gefragt werden, die Kollegen oder Kunden gefährden könnten.

Bejaht man ungeachtet der vorstehenden Bedenken die Erforderlichkeit ebenso wie das Nichtüberwiegen der schutzwürdigen Interessen der betroffenen Personen, ist zu prüfen, ob das grundsätzliche Verarbeitungsverbot des Art. 9 Abs. 1 DSGVO der Fiebermessung nicht entgegensteht. Nach den bereits gegebenen Hinweisen kommt insoweit gegenwärtig eine Ausnahme vom Verarbeitungsverbot nur noch nach Art. 9 Abs. 2 Buchstabe h DSGVO in Verbindung mit § 22 Abs. 1 Nr. 1 Buchst. b bzw. 26 Abs. 3 BDSG in Betracht. Danach ist eine Verarbeitung personenbezogener Gesundheitsdaten nicht verboten, wenn sie für die **Beurteilung der Arbeitsfähigkeit** erforderlich ist. Die Dokumentation müsste den zentralen Grundsätzen, u.a. der Zweckbindung, der Datenminimierung und Speicherbegrenzung, folgen. Zudem ist die Erfüllung der in Art. 9 Abs. 3 DSGVO, § 22 Absatz 1 Nummer 1 Buchstabe b) BDSG genannten Bedingungen und Garantien geboten. Mit anderen Worten dürfte eine elektronische Fiebermessung nur durch einen betriebsärztlichen Dienst vorgenommen

werden. Dieser dürfte dem Arbeitgeber bzw. Dienstherrn allenfalls mitteilen, welchen Beschäftigten der Zutritt zum Betriebsgelände verweigert worden ist.

Im Bereich des betrieblichen Gesundheitsschutzes sind im Übrigen die Beteiligungsrechte der Interessensvertretungen zu beachten.

Die zulässige Verwendung elektronischer Temperaturmessgeräte hängt schließlich insgesamt von der Erfüllung **weiterer datenschutzrechtlicher Vorgaben** ab, z.B. sind die Regelungen zum Verzeichnis von Verarbeitungstätigkeiten, zur Datenschutz-Folgenabschätzung sowie zur Information nach Art. 12 ff. DSGVO (Hinweisbeschilderung) zu beachten.

Der Verantwortliche hat zudem dafür Sorge zu tragen, dass die Vorgaben des **Datenschutzes durch Technikgestaltung** aus Art. 25 DSGVO und der **Datensicherheit** nach Art. 32 DSGVO erfüllt werden. Hierbei können beispielsweise folgende Gesichtspunkte eine Rolle spielen:

- Geeignete Körperstellen zur Messung: Eine aussagekräftige Erfassung eines kompletten Wärmebilds eines Menschen ist kaum möglich, da z.B. die Kleidung die Infrarot-Abstrahlung verändern kann. In der Regel wird daher an der Stirn oder den Innenwinkeln der Augen gemessen. Es sind somit Spezialkameras nötig, die diese Stellen automatisiert erkennen und anvisieren können.
- Messgenauigkeit: Klassische kontaktlose Stirnthermometer haben häufig größere Abweichungen. Abhängig vom Einsatzkontext müssen daher Systeme zum Einsatz kommen, die eine deutlich höhere Messgenauigkeit haben, als übliche kontaktlose Fieberthermometer für den Hausgebrauch bieten.
- Verfälschung der Messung: Zudem muss berücksichtigt werden, dass neben anderen Erkrankungen auch körperliche Betätigung (Sport, Eile), Umgebungs-bedingungen etc. zu Messunterschieden oder Abweichungen beitragen können.

- Absolute / relative Messung: Es gibt sowohl die Herangehensweise, einen Schwellwert festzulegen, ab dem die Wärmebildkamera positiv detektiert, als auch die Messung und Alarmierung im Vergleich zu den umgebenden Menschen durchzuführen. Im ersteren Fall stellt sich insbesondere die Schwierigkeit, wie der relevante Grenzwert für Fieber festzulegen ist, soweit die Körpertemperatur im Verlauf des Tages schwankt und zudem bei Kindern und Erwachsenen unterschiedlich ausfallen kann.
- Fehlerrate: Aufgrund der technischen Schwierigkeiten der Messung kann es auch unabhängig von der Problematik, dass Infizierte noch keine Symptome zeigen, zu „falsch-positiven“ wie auch „falsch-negativen“ Ergebnissen kommen, beispielsweise abhängig von der Festlegung der Schwellwerte und der Aufstellsituation.
- Auflösung, Bildgenauigkeit: Viele Wärmebildkameras bieten eine sehr hohe Auflösung, so dass sich die Frage stellt, welche zusätzlichen Informationen damit ersichtlich sind, insbesondere wenn ein Echtbild des Gesichts in hoher Auflösung erfasst wird (Erkennung anderer Krankheiten, biometrische Identifikation etc.).
- Automatische Messung / menschlicher Bediener: Aufgrund des Aufwands für die Messung ist davon auszugehen, dass diese nicht vollautomatisiert erfolgen kann, sondern zumindest von menschlichem Personal überwacht werden muss. Zudem ist im Fall einer positiven Detektion in der Regel menschliche Intervention nötig, um die betroffene Person herauszufiltern und weitere Maßnahmen zu ergreifen.

- **22.09.2020 – Anwendung der DSGVO auf Datenverarbeitungen von Parlamenten**

  Anlässlich des Urteils des EuGH vom 9. Juli 2020 (C-272/19) wird der Beschluss der Datenschutzkonferenz vom 5. September 2018 „Anwendung der DSGVO im Bereich von Parlamenten,

Fraktionen, Abgeordneten und politischen Parteien“ bis zur Neuformulierung eines Beschlusses ausgesetzt.

- **26.11.2020 – Telemetriefunktionen und Datenschutz beim Einsatz von Windows 10 Enterprise**

  In der 98. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wurde ein Prüfschema zum datenschutzkonformen Einsatz von Windows 10 beschlossen und anschließend veröffentlicht[1]. Damit soll den Verantwortlichen die Überprüfung der Einhaltung der datenschutzrechtlichen Vorgaben beim Einsatz von Windows 10 erleichtert werden. Eine Arbeitsgruppe der DSK hat unter Beteiligung von LDA Bayern, BfDI, LfDI Mecklenburg-Vorpommern und LfD Niedersachsen seitdem ihre Untersuchung von Windows 10 in Hinblick auf die Telemetriestufe Security, die in der Enterprise-Edition verfügbar ist, fortgesetzt.

  Unabhängig davon hat sich das an einer Laboruntersuchung der Arbeitsgruppe neben dem LfD Bayern als Gast beteiligte BSI selbst in einer umfangreichen Studie (SiSyPHuS-Studie) auch mit Fragstellungen der Windows-10-Telemetriefunktion beschäftigt.

  Untersuchungsergebnisse der DSK-Arbeitsgruppe

  Die Arbeitsgruppe hat die Telemetrie von Windows 10 einer Laboruntersuchung unterzogen, um festzustellen, ob sich die Telemetriedatenübermittlung durch Konfiguration unterbinden lässt. Microsoft hat gegenüber den Aufsichtsbehörden erklärt, dass bei der Nutzung der Telemetriestufe Security keine Telemetriedaten[2] übermittelt werden.

[1] https://www.datenschutzkonferenz-online.de/media/ah/20191106_win10_pruefschema_dsk.pdf
[2] Zum Begriff siehe Bericht Windows 10 Telemetrie-Prüfung mit Nutzerinteraktion (Anlage 1)

Es wurde Windows 10 Enterprise in der Version 1909 in drei Testszenarien untersucht. In allen drei Szenarien wurden Benutzeraktivitäten simuliert, um realistische Ergebnisse zu erzielen.

1. Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Security“, 72 Stunden Testzeitraum
2. Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Basic“, 30 Minuten Testzeitraum
3. Keine Anwendung des „Windows Restricted Traffic Limited Functionality Baseline“, Telemetriestufe „Security“, 72 Stunden Testzeitraum

Die Details der Untersuchung können dem Laborbericht Anlage 1 (Windows 10 Telemetrie-Prüfung mit Nutzerinteraktion) entnommen werden.

Die Untersuchung hat bestätigt, dass im zweiten Prüfszenario die Übermittlung von Telemetriedaten festgestellt werden konnte. Im dritten Szenario wurde ein Verbindungsaufruf zum settings-win.data.microsoft.com Endpunkt festgestellt. Dieser Endpunkt wird laut Aussage von Microsoft von mehreren Windows-10-Systemkomponenten, auch von der Telemetriekomponente, angesteuert. Nutzt die Telemetriekomponente diesen Endpunkt, besteht die Möglichkeit, dass hierüber Konfigurationsdaten heruntergeladen werden, durch die Änderungen am Verhalten des Telemetriedienstes bewirkt werden könnten. Microsoft hat diesen Aufruf gegenüber den Datenschutzaufsichtsbehörden auf Basis eines Microsoft zur Verfügung gestellten Laborszenarios erläutert und erklärt diesen mit einer anderen Systemkomponente abseits der Telemetrie. Microsoft hat auf mündliche Nachfrage gegenüber den Datenschutzaufsichtsbehörden erklärt, dass trotz eines – möglicherweise aufgrund eines Softwarefehlers – unbeabsichtigten Aufrufs an den settings-win.data.microsoft.com Endpunkt von dem Telemetriedienst, bei einem Telemetrielevel „Security“ weiterhin keine Telemetriedatenübermittlung stattfinden würde.

Untersuchungsergebnisse des BSI

In einer den Labortest der Arbeitsgruppe ergänzenden Untersuchung des Windows-10-Enterprise-Datenverkehrs durch das BSI im Januar 2020 wurden Datenübertragungen zu „settings-win.data.microsoft.com“ festgestellt (siehe Anlage 2).

Dabei wurde ein Windows 10 Enterprise System Version 1803 mit Telemetrielevel Security und „Windows Restricted Traffic Limited Functionality Baseline“ genutzt. Es ist jedoch zu beachten, dass die Verbindungen zu „settings-win.data.microsoft.com“ nicht im Klartext analysiert werden konnten und somit die Möglichkeit besteht, dass Microsoft über diesen Kanal Daten exfiltriert oder in unerwünschter Weise Einfluss auf das System nimmt. Vor diesem Hintergrund hält das BSI aufgrund eines Defense-in-Depth-Ansatzes zur Stärkung der Sicherheit der IT-Systeme des Bundes an der Notwendigkeit einer Netztrennung von Windows-10-Clients der Bundesverwaltung, auch zur Abwehr von Schadcodes, fest.

Laut Microsoft wird über den Endpunkt „settings-win.data.microsoft.com“ auch die Konfiguration der Windows-Komponente „Benutzererfahrungen und Telemetrie im verbundenen Modus“ dynamisch aktualisiert.[1] Auch im BSI-Projekt „SiSyPHuS“ ist diese Adresse mehrfach im Zusammenhang mit der dynamischen Konfiguration der Windows-Telemetrie genannt.[2]

Den Feststellungen zur Folge könnte Microsoft darüber das Verhalten des Telemetriedienstes anpassen, Art und Umfang der Datenerhebung konfigurieren oder Kommandos zur Anreicherung der Daten ausführen, ohne dass der Nutzer dem zustimmen müsse oder das kontrollieren könne. Vor diesem Hintergrund

[1] https://docs.microsoft.com/de-de/windows/privacy/manage-windows-1803-endpoints
[2] https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/SiSyPHus/Workpackage4_Telemetry.pdf

sind Verbindungen zu diesem Endpunkt nach der Bewertung des BSI zumindest als bedenklich einzustufen.

Konsequenzen für Verantwortliche

Im veröffentlichten Prüfschema wird erläutert, dass Verantwortliche den Nachweis für die Rechtmäßigkeit etwaiger Übermittlungen personenbezogener Daten an Microsoft erbringen oder die Übermittlung personenbezogener Daten unterbinden müssen.

Zur Unterbindung der Übermittlung personenbezogener Telemetriedaten haben die Verantwortlichen beim Einsatz der Enterprise-Edition die Telemetriestufe Security zu nutzen und mittels vertraglicher, technischer oder organisatorischer Maßnahmen (z. B. durch eine Filterung der Internetzugriffe von Windows-10-Systemen über eine entsprechende Infrastruktur) sicherzustellen, dass nachweislich keine Übermittlung von Telemetriedaten an Microsoft stattfindet.

Angesichts ggf. weiterer offener Fragen, die z. B. mit dem Aufruf der „settings-win.data.microsoft.com“-Datenverbindung verbunden sind oder die auch die SiSyPHuS-Studie des BSI aufwirft, wie des Umstands, dass die vorliegenden Untersuchungen auf Grund laufender Fortentwicklungen der Software natürlich nur eine Momentaufnahme darstellen, können die bisherigen Untersuchungen Verantwortliche nicht abschließend von ihrer aus Art. 5 Abs. 2 DS-GVO abzuleitenden Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten entlasten. Dies gilt erst Recht für Verantwortliche, die Windows 10 in der Pro- und Home-Edition einsetzen, in denen die Telemetriestufe derzeit nicht auf Security gesetzt werden kann. In diesen Fällen bleiben ohnehin andere Maßnahmen zur Unterbindung etwaiger Übermittlungen personenbezogener Telemetriedaten zu prüfen oder die Rechtmäßigkeit der Übermittlung nachzuweisen.

Deshalb sollte Windows 10 in allen angebotenen Editionen die Möglichkeit bieten, die Telemetriedatenverarbeitung durch Konfiguration zu deaktivieren. Dazu und zu den in den Labor-Untersuchungen der DSK und der SiSyPHus-Studie des BSI aufgezeigten verbliebenen Unwägbarkeiten werden die Datenschutzaufsichtsbehörden das weitere Gespräch mit Microsoft führen.

Hinweis: Die Anlagen zu diesem Beschluss sind auf der Homepage der DSK abrufbar https://datenschutzkonferenz-online.de/media/dskb/TOP_30_Beschluss_Windows_10_mit_Anlagen.pdf.

Anhang zum Beitrag 10.2 – Fragebogen zur Datenschutzüberprüfung von Versicherungsunternehmen und Kreditinstituten

1. Allgemeine Informationen

- Name, Rechtsform, Anschrift Ihres Unternehmens:
- Ansprechpartner (Name, Funktion, Telefon, E-Mail)
- Datenschutzbeauftragter (Name, Telefon, E-Mail)

2. Datenschutzorganisation

2.1 Welche Unternehmensbereiche sind mit dem Thema Datenschutz betraut?

2.2 Beschreiben Sie bitte das Zusammenwirken der einzelnen Stellen in datenschutzrechtlichen Angelegenheiten unter Beifügung eines aussagekräftigen Organigramms

2.3 Sofern es einen Datenschutzbeauftragten gibt, wie und in welcher Häufigkeit berichtet er an die Geschäftsführung?

3. Umsetzung der DS-GVO

3.1 Welche Unternehmensbereiche waren oder sind maßgeblich in die Umsetzung der DS-GVO involviert?

3.2 Kreuzen Sie bitte die wesentlichen Maßnahmen an, die Sie im Rahmen der Umsetzung getroffen haben.

- ☐ Sensibilisierungsmaßnahmen
- ☐ interne Datenschutz-Richtlinie
- ☐ Erstellung von Datenschutzhinweisen zur Erfüllung der Informationspflicht
- ☐ Löschkonzept
- ☐ Neuverhandlung Auftragsverarbeitungsverträge
- ☐ Prozess Datenschutz-Folgenabschätzung
- ☐ Anpassung und Erweiterung interner Vorgaben zur Dokumentation
- ☐ Dokumentation der Umsetzung der DS-GVO
- ☐ Überarbeitung/Erstellung von Betriebsvereinbarungen
- ☐ Benennung eines internen bzw. Beauftragung eines externen Datenschutzbeauftragten
- ☐ Prozesse für Betroffenenrechte
- ☐ Prozesse für Beschwerdebearbeitung
- ☐ Prüfung vertraglicher Grundlagen für internationalen Datentransfer
- ☐ Überprüfung/Neuverhandlung der Verträge mit externen Dienstleistern
- ☐ Dokumentation der internen Datenschutzorganisation
- ☐ Prozess für die Meldung von Datenpannen
- ☐ Sonstige:

3.3 Erläutern Sie bitte kurz den Umsetzungsstatus, falls noch nicht bzw. nicht vollständig umgesetzt. Benennen Sie bitte auch die Gründe.

3.4 Hat Ihre Internen Revision oder eine vergleichbare Einheit die Einführung und Umsetzung der DS-GVO in Ihrem Unternehmen geprüft?

4. Zulässigkeit der Datenverarbeitung

4.1 Bitte listen Sie die wesentlichen unternehmensspezifischen Datenverarbeitungen auf und ordnen Sie diesen die Rechtsgrundlagen zu, auf die Sie die Verarbeitung personenbezogener Daten stützen (Artikel 6, 9 DS-GVO inklusive Spezialnormen).

4.2 Sofern Sie auf Basis von Einwilligungen personenbezogene Daten verarbeiten, fügen Sie bitte exemplarisch Ihr(e) Muster bei.

5. Beschwerde-Bearbeitung

5.1 Listen Sie bitte die mit der Bearbeitung datenschutzrechtlicher Beschwerden befassten Stellen Ihres Unternehmens auf.

5.2 Anhand welcher Kriterien stuft Ihr Unternehmen die Rückmeldung eines Kunden als datenschutzrechtliche Beschwerde ein (Beschwerdedefinition)?

5.3 Wie unterscheidet sich die Bearbeitung einer datenschutzrechtlichen Beschwerde von der Bearbeitung einer sonstigen Beschwerde?

6. Betroffenenrechte

6.1 Wie stellen Sie sicher, dass den Betroffenenrechten auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Nachberichtspflicht und Datenübertragbarkeit angemessen nachgekommen wird? Bitte kreuzen Sie zutreffendes an.

☐ Regelungen der Verantwortlichkeiten, Zuständigkeiten und des Kommunikationsverlaufs im Unternehmen

☐ Prozesse zur Beantwortung von Anfragen der Betroffenen (einschließlich Erkennen als Anfrage zu einem Betroffenenrecht z. B. durch Schlüsselwörter, Identifikation der Betroffenen, Bearbeitungsdauer, Rückmeldung an Betroffene u.a.)

☐ Verwenden von Mustern für Antwortschreiben

☐ Prozesse zur Sicherstellung der Einhaltung von Fristen

☐ Prozesse zur Nachverfolgung des Fortschritts der Bearbeitung

☐ Verfahren zur Reaktion, wenn ein(e) Betroffene(r) mit der Beantwortung nicht zufrieden ist

☐ Sensibilisierung der Mitarbeiter

6.2 Skizzieren Sie bitte überblicksartig Ihre wesentlichen Prozesse zu den o. g. Betroffenenrechten. Legen Sie bitte möglichst Nachweise (z. B. Verfahrensbeschreibungen, Mustertexte etc.) bei, die eine Überprüfung Ihrer Angaben ermöglichen.

6.3 Wie kommen Sie Ihren Informationspflichten gegenüber Kunden gem. Art. 13 bzw. 14 DS-GVO nach (z.B. Homepage, Postversand, E-Mail-Link, Aushang)? Bitte fügen Sie exemplarisch Ihre Muster-Texte bei.

6.4 Zu welchem Zeitpunkt informieren Sie Ihre Kunden i. S. v. 6.3?

6.5 Wie werden Missstände und Schwachstellen im Umgang mit Betroffenenrechten kontinuierlich verbessert und die Verbesserungsmaßnahmen auf ihre Wirksamkeit hin überprüft?

7. Sensibilisierungsmaßnahmen

7.1 Stellen Sie sicher, dass Ihre Mitarbeiterinnen und Mitarbeiter für den Umgang mit personenbezogenen Daten hinreichend sensibilisiert sind?

☐ Ja

☐ Nein

7.2 Benennen Sie, wenn zutreffend, die wesentlichen Sensibilisierungsmaßnahmen und machen Sie Angaben zum Ausführungsturnus.

8. Rechenschaftspflicht

8.1 Wie können Sie die Einhaltung der Grundsätze der Datenverarbeitung nachweisen? Benennen Sie die Art der Dokumentation, die Sie für diesen Zweck vorhalten.

8.2 Welche Aspekte bereiten ggf. Schwierigkeiten?

9. Sonstiges

Haben Sie Anregungen an die Aufsicht?

Anhang zum Informationsfreiheitsbericht

Veröffentlichungen der Konferenz der Informationsfreiheitsbeauftragten (IFK) in Deutschland

- **Positionspapier der 37. Konferenz der Informationsfreiheitsbeauftragten (IFK) in Deutschland am 12. Juni 2019 in Saarbrücken**

  Informationszugang in den Behörden erleichtern durch „Informationsfreiheit by Design“

  Der digitale Wandel ist eine der großen Herausforderungen, vor denen die öffentliche Verwaltung heute steht. Gegenwärtig müssen E-Government-Gesetze sowie die Regelungen im Onlinezugangsgesetz umgesetzt werden. Parallel ist ein gestiegenes Interesse an der Transparenz des Verwaltungshandelns festzustellen, das die Gesetzgeber zunehmend aufgreifen. Die öffentliche Verwaltung ist in der Pflicht, das Recht auf Informationszugangsfreiheit umzusetzen. Das Vertrauen in die staatliche Aufgabenerfüllung wird gefestigt, indem Auskunftsersuchen schnell und effizient bearbeitet werden.

  Vor diesem Hintergrund empfiehlt die Konferenz der Informationsfreiheitsbeauftragten in Deutschland (IFK) den öffentlichen Stellen des Bundes und der Länder, die Anforderungen an die Informationsfreiheit bereits von Anfang an in die Gestaltung ihrer IT-Systeme und organisatorischen Prozesse einfließen zu lassen: „Informationsfreiheit by Design“. Die Gesetzgeber werden aufgerufen, die gesetzlichen Grundlagen zu schaffen und notwendige Ressourcen zur Verfügung zu stellen.

  Definition

  Zu „Informationsfreiheit by Design“ zählt die Gesamtheit technischer und organisatorischer Instrumente unter Berücksichtigung des Stands der Technik, die der Wahrnehmung und Erfüllung der

Rechte nach den Informationsfreiheits- und Informationszugangsgesetzen, Umweltinformationsgesetzen und Transparenzgesetzen des Bundes und der Länder dienen. Damit unterstützt „Informationsfreiheit by Design“ einerseits informationspflichtige Stellen bei der Erfüllung eines beantragten Informationszugangs sowie bei der Umsetzung von Veröffentlichungspflichten, andererseits wird für Antragstellende der Informationszugang erleichtert.

Rahmenbedingungen

Für den Bereich der Verarbeitung personenbezogener Daten hat der europäische Verordnungsgeber das Prinzip des Datenschutzes durch Technikgestaltung – also „Datenschutz by Design“ – normiert. Auf dem Gebiet der Informationsfreiheit bestehen ebenfalls Regelungen, aus denen für informationspflichtige Stellen technische und organisatorische Verpflichtungen resultieren. Hierzu zählen je nach Regelungsinhalt der landes- und bundesrechtlichen Bestimmungen etwa

- proaktive Veröffentlichungspflichten,
- das Hinwirken auf eine Speicherung von Informationen in elektronischen Datenbanken,
- die Benennung von Ansprechpartnern oder anderen informationspflichtigen Stellen,
- die Bereitstellung von Verzeichnissen über verfügbare Informationen,
- die Einrichtung von öffentlich zugänglichen Informationsnetzen und –portalen,
- die Berücksichtigung der Kennzeichnung von Informationen durch Dritte als „schutzbedürftig“ und
- die Ermöglichung eines beschränkten Informationszugangs bei nur teilweise entgegenstehenden öffentlichen oder privaten Interessen.

Weiterhin soll die Beachtung der Grundsätze der ordnungsgemäßen Aktenführung dazu dienen, den zeitlichen Bereitstellungsaufwand zu begrenzen und die Kosten des Informationszugangs zu verringern.

Maßnahmen

Maßnahmen zu „Informationsfreiheit by Design“ können bei der Erfüllung dieser technischen und organisatorischen Verpflichtungen eine Hilfestellung bieten. So sollte die Auffindbarkeit von Informationen bei den informationspflichtigen Stellen z. B. durch effiziente Aktensystematik und elektronische Suchfunktionen gewährleistet sein. In Aktensystemen könnte bei Aufnahme neuer Informationen eine Kennzeichnung sensibler Abschnitte oder Aktenteile erfolgen, die eine gesonderte Prüfung auf geheimhaltungsbedürfige Teile erleichtert. Informationen sollten nach Möglichkeit in den Aktensystemen kategorisiert werden, was in bestimmten Verwaltungsbereichen etwa durch die Führung von Teilakten denkbar ist, die Teil einer Hauptakte sind. Veröffentlichungsfähige Informationen sollten durch die informationspflichtige Stelle proaktiv, etwa über ein Informationsportal, für die Allgemeinheit zur Verfügung gestellt werden.

Mit dem Ansatz „Informationsfreiheit by Design“ können standardisierte Lösungen für wiederkehrende Fragestellungen entwickelt werden, wodurch der Aufwand auf Verwaltungsseite reduziert wird. Diese Systemgestaltung obliegt dabei nicht nur den Verantwortlichen der öffentlichen Verwaltung, sondern auch den Entwicklerinnen und Entwicklern von Software-Lösungen für öffentliche Verwaltungen, bei denen Anforderungen der Informationsfreiheit von Anfang an in die Konzepte und Implementierungen aufgenommen werden sollten.

- **Entschließung der 37. Konferenz der Informationsfreiheitsbeauftragten (IFK) in Deutschland am 12. Juni 2019 in Saarbrücken**

  Transparenz im Rahmen politischer Entscheidungsprozesse – Verpflichtendes Lobbyregister einführen

  Die parlamentarische Demokratie lebt von der offenen und deshalb öffentlichen Diskussion verschiedener, oftmals unterschiedlicher Interessen, die im Rahmen der Gesetzgebung von den Parlamentsmitgliedern gegeneinander abgewogen werden müssen. Angesichts der Komplexität der sozialen und wirtschaftlichen Realität und der Regelungsmaterien kann es im demokratischen Willensbildungsprozess oftmals hilfreich sein, auf die Expertise von unterschiedlichen Personen, Gruppierungen und Beteiligten aus Gesellschaft und Wirtschaft zurückgreifen zu können. Die Art und Weise einer solchen Einflussnahme muss jedoch transparent sein. Die Bürgerinnen und Bürger sollen wissen, wer im Laufe des Entstehungsprozesses an der Formulierung eines Gesetzentwurfs beteiligt war und wer in wessen Auftrag und mit welchen Mitteln auf politische Entscheidungen einzuwirken versucht. Verflechtungen insbesondere zwischen Politik und Wirtschaft sind erkennbar zu machen, damit verdeckte Einflussnahmen erschwert sowie eine öffentliche Kontrolle ermöglicht wird.

  Deshalb bestehen bereits in einigen Staaten Regelungen zur Führung von Lobbyregistern. Aus Sicht der Informationsfreiheitsbeauftragten in Deutschland ist es für ein demokratisches Gemeinwesen geboten, verpflichtend Register einzuführen, in die Informationen über Interessenvertretungen und deren Aktivitäten einzutragen sind. Darin sind mindestens die Namen der natürlichen und juristischen Personen unter Angabe ihrer Organisationsform, der Schwerpunkt der inhaltlichen oder beruflichen Tätigkeit und zumindest die wesentlichen Inhalte des Beitrags zum jeweiligen Gesetzgebungsverfahren zu veröffentlichen. Die damit hergestellte Transparenz stärkt das Vertrauen der Menschen in

die Politik, ermöglicht demokratische Kontrolle und erhöht die Akzeptanz politischer – insbesondere gesetzgeberischer – Entscheidungen.

Die Konferenz der Informationsfreiheitsbeauftragten fordert den Bundes- und die Landesgesetzgeber deshalb dazu auf, etwa in Anlehnung an das Thüringer Beteiligtentransparenzdokumentationsgesetz vom 7. Februar 2019 gesetzliche Rahmenbedingungen zur Einführung eines verpflichtenden Lobbyregisters zu verabschieden.