Der Landesbeauftragte für den
DATENSCHUTZ und die
INFORMATIONSFREIHEIT
Rheinland-Pfalz

TÄTIGKEITSBERICHT ZUM DATENSCHUTZ 2020

www.datenschutz.rlp.de

HERAUSGEBER
Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34 | 55116 Mainz
Postfach 30 40 | 55020 Mainz
Telefon +49 (0) 6131 8920 - 0
Telefax +49 (0) 6131 8920 - 299
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

März 2022

INHALT

VORWORT


Prof. Dr. Dieter Kugelmann

Dieser Tätigkeitsbericht betrifft ein besonderes Jahr. Das Jahr 2020 war auch für den Landesbeauftragten für den Datenschutz und die Informationsfreiheit von der Pandemie und ihren Auswirkungen geprägt. Diese Prägung betraf aus meiner Perspektive insbesondere den Digitalisierungsschub, der pandemiebedingte Umstellungen in Politik, Wirtschaft und Gesellschaft ausgelöst hat. Die sprunghafte Zunahme von Homeoffice-Tätigkeiten, der plötzlich erforderliche Fernunterricht in den Schulen und Hochschulen auf der Basis digitaler Technik oder allgemein die lawinenartige Zunahme von Videokonferenzen haben aus Sicht des Datenschutzes Fragen und Probleme hervorgebracht oder nach oben gespült, die bisher weniger beachtet wurden oder unter dem Radar liefen.

In der Konsequenz war meine Behörde stark gefragt und belastet, um auf diese Fragen und Probleme konstruktive Antworten und belastbare Problemlösungen zu entwickeln. Dies ist dank des Engagements der Mitarbeitenden ausgezeichnet gelungen. Wir waren sehr schnell und früh mit Informationen und Hilfestellungen am Puls der Zeit. Dies betraf die Optionen der Kontaktnachverfolgung durch Gästelisten ebenso wie die Auslegung infektionsschutzrechtlicher Vorschriften und in diesem Zusammenhang insbesondere der sich dynamisch ändernden Corona-Bekämpfungsverordnungen etwa im Hinblick auf Zugang zu oder Übermittlung von Daten der Gesundheitsämter. Stets habe ich versucht, die Pandemie mit ihren möglichen schrecklichen Folgen im Blick zu behalten und doch den Datenschutz soweit wie möglich zur Geltung kommen zu lassen. Die Abwägungen, die vielerorts getroffen werden mussten, haben auch unsere Tätigkeiten gekennzeichnet.

Im Ergebnis hat sich oft herausgestellt, dass datenschutzrechtliche Aspekte angemessen in Problemlösungen eingebaut werden können. Die teils in der Öffentlichkeit vorgetragenen angeblichen Konflikte sind bei näherer Betrachtung oftmals nur Scheinkonflikte. Ein Stimmungsbild bietet dazu der in überregionalen Zeitungen abgedruckte offene Brief von der Berliner Kollegin Maja Smoltczyk und mir, der unten abgedruckt ist. Ich möchte nicht verhehlen, dass es durchaus einzelne Punkte gibt, in denen datenschutzrechtliche Bestimmungen klare Vorgaben machen,

die dann auch Handeln von Verantwortlichen in Wirtschaft und Verwaltung in eine bestimmte Richtung lenken. Dies ist aber gerade die Funktion des geltenden Datenschutzrechts. Das Grundrecht auf informationelle Selbstbestimmung bzw. Datenschutz wird durch Krisen nicht außer Kraft gesetzt. Im Gegenteil ist aufgrund der starken Fortentwicklung der Digitalisierung die Bedeutung dieses Grundrechtes in der Pandemie gerade noch einmal besonders deutlich geworden. Pauschale Behauptungen im Hinblick auf angebliche Unvereinbarkeiten helfen hier ebenso wenig weiter wie floskelhafte Wiederholungen von unscharfen Thesen. Ich habe in Bürgersprechstunden, zu denen mich dankenswerter Weise Abgeordnete des rheinland-pfälzischen Landtages eingeladen haben, in der Öffentlichkeitsarbeit allgemein und auch durch konkrete Informationen auf der Webseite und gegenüber handelnden Stellen meine Positionen eingebracht, um zu Problemlösungen beizutragen. Aus meiner Sicht ist es insgesamt gelungen, den Gesundheitsschutz soweit wie möglich zu sichern und dabei den Datenschutz soweit wie möglich zu wahren.

Wie in nahezu allen anderen Einrichtungen und Unternehmen ist auch in meiner Behörde durch die Pandemie eine teils schwierig zu bewältigende Situation entstanden. Auch wir haben in großen Teilen im Homeoffice gearbeitet. Auch wir mussten unsere Abläufe optimieren und umstellen. Deshalb ist auch entsprechendes Verständnis für derartige Vorgänge in anderen Zusammenhängen vorhanden, die manches Mal zu datenschutzrechtlichen Problemen geführt haben. Die Schwierigkeiten für die Arbeit der Behörde haben wir in konsensualem Zusammenwirken hervorragend bewältigt. Meine Mitarbeitenden haben jeden Vertrauensvorschuss zuverlässig eingelöst und die Arbeitsfähigkeit der Behörde insgesamt erhalten. Dafür gebührt ihnen großer Dank. Engagement, Einsatzbereitschaft und Flexibilität sind seit langem Teil des Profils meiner Behörde und werden es auch künftig weiter sein.

Trotz der Pandemie gab es auch im Jahr 2020 ein Alltagsgeschäft, das sich weiter in hohen Zahlen an Beschwerden und Datenpannenmeldungen ausdrückte. Die verschiedenen Aspekte, die in diesem Tätigkeitsbericht aufgeführt sind, verdeutlichen die weiter hohe und noch zunehmende Wichtigkeit von Datenschutz in der modernen Informationsgesellschaft. Die Apps im Zusammenhang mit der Pandemie sind dabei nur die Spitze des Eisberges für vielfältige Problemlagen im Zusammenhang mit derartigen Applikationen insgesamt. Hinzu kommt die Problematik von Cookies. Hier hat die Rechtsprechung einige Klarstellungen herbeigeführt.

Insgesamt ist es ohnehin so, dass die Justiz nach und nach Fragen des Datenschutzrechts aufarbeitet, die aufgrund der Datenschutz-Grundverordnung gestellt werden. Der Prozess hin zu mehr Rechtssicherheit und Verlässlichkeit gewinnt immer stärker an Intensität.

Die Kooperation mit den anderen deutschen Datenschutzaufsichtsbehörden und auf europäischer Ebene verdichtet sich. Dies stellt Herausforderungen an die Behörden, da es darum geht, europaweit vernünftige Lösungen herbeizuführen. Ich stehe dafür, dass Rheinland-Pfalz insoweit eine aktive Rolle spielt. Nur durch aktive Beiträge zu europäischen und deutschlandweiten Lösungen können wir harmonisierte Lösungen erreichen und die Akzeptanz des Datenschutzrechts weiter befördern. Dazu werde ich auch in Zukunft einen Beitrag leisten. Denn eines ist klar: Es gibt ein Leben sowohl mit wie nach der Pandemie. Dieses Leben wird aber digitaler sein als zuvor. Dazu gehört effektiver und konstruktiver Datenschutz.

Prof. Dr. Dieter Kugelmann

Gastbeitrag von Prof. Dr. Dieter Kugelmann, dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz, und Maja Smoltczyk, der Berliner Beauftragten für Datenschutz und Informationsfreiheit

Schluss mit den Attacken auf den Datenschutz!

Es ist ein alt bekanntes Lied. In schwierigen Zeiten, etwa nach einem Terroranschlag, wenn pädophile Straftaten aufgedeckt werden oder jetzt inmitten der Corona-Pandemie, die unsere ganze Welt auf den Kopf stellt, klingen immer wieder dieselben Töne: Der Datenschutz muss gelockert werden! Datenschutz ist Täterschutz! Datenschutz gefährdet Menschenleben! Und beständig stimmen Teile der Wirtschaft mit ein: Der Datenschutz macht das Internet kaputt! Datenschutz bremst die Digitalisierung! Datenschutz verhindert Innovation! Nichts davon ist richtig.

Schaut man sich all das genauer an, zeigt sich, dass der reflexartige Schuldverweis auf den Datenschutz nichts weiter ist als der wohlfeile Versuch, für komplexe Probleme eine einfache Lösung zu finden. Dadurch aber wird von den eigentlichen Problemen meist nur abgelenkt. So verfügen die mit der Gefahrenabwehr und Strafverfolgung beauftragten Behörden sicher nicht über zu wenige Überwachungsinstrumente oder gar zu wenig Daten. Oft ist eher das Gegenteil der Fall und sie sind personell und technisch oft gar nicht mehr in der Lage, die Masse an Informationen, über die sie bereits verfügen oder verfügen könnten, rechtzeitig auszuwerten und sinnvoll zu nutzen.

Der Datenschutz macht das Internet nicht kaputt, sondern versucht, die im Laufe der Geschichte mühsam erkämpften Grundrechte der Menschen auch in einer Zeit allumfassender Digitalisierung in die Zukunft zu retten. Das uferlose Sammeln persönlicher Daten, Tracking und Data Mining sind an der Tagesordnung. Wo eigentlich technische Innovationen dem Menschen dienen sollen, macht es eher den Eindruck, als dienten die Menschen – ihre Daten und Profile – den Investoren und Unternehmen. Hier müssen Dinge zusammengebracht werden, die auseinanderzufallen drohen, damit beides gerettet werden kann – die Errungenschaften der Digitalisierung und die bürgerlichen Grundrechte, die die Grundlage unserer freiheitlich-demokratischen Gesellschaft sind.

Pauschale Schuldzuweisungen lenken von den eigentlichen Problemen ab und kehren die Beweislast um. Grundrechte stehen nicht für sich, sondern in einem Wechselverhältnis zu anderen Grundrechten. Bei jeder Einschränkung von Grundrechten muss darauf geachtet werden, dass dies nur im unbedingt notwendigen Umfang geschieht und nur soweit, wie der Schutz anderer

Grundrechte es erfordert. Also müssen die, die in einer bestimmten Situation das Grundrecht auf informationelle Selbstbestimmung einschränken wollen, überzeugende Argumente dafür liefern, damit eine solche Abwägung stattfinden kann. Es mag verführerisch sein, den Datenschutz immer wieder als das eigentliche Problem hinzustellen, wodurch die Datenschützer*innen in Kritik und Rechtfertigungszwang geraten. Eine angemessene Problemlösung jedoch wird dadurch verhindert.

Die Pandemie hat einmal mehr gezeigt, wie der Datenschutz als Sündenbock herhalten muss, wenn Dinge außer Kontrolle geraten sind. Es vergeht kein Tag, an dem nicht behauptet wird, dass die Pandemie leicht in den Griff zu bekommen sei, wenn wir nur den Datenschutz zurechtstutzen würden.

Problematisiert wird nicht, dass die Gesundheitsämter noch immer nicht alle an die digitale Infrastruktur angeschlossen sind, die jedoch Voraussetzung dafür ist, dass die Corona-App einen wirklichen Mehrwert für die Ämter hat. Problematisiert wird auch nicht, dass die Ämter mit den Daten von Corona-Kontaktlisten bereits überfordert sind, wenn eifrig gefordert wird, die App müsste noch viel mehr Daten sammeln.

Problematisiert wird nicht, dass kaum ein kommerzieller Anbieter datenschutzgerechte Lösungen anbietet und Behörden nicht in der Lage sind, solche Lösungen selbst zu schaffen oder es nicht zuwege bringen, entsprechende Lösungen in Ausschreibungen einzufordern. Problematisiert wird auch nicht, dass US-amerikanische Dienste es sich vorbehalten wollen, die Daten von Kindern für eigene, meist kommerzielle, Zwecke zu verarbeiten. Behauptet wird stattdessen, dass die Datenschützer*innen den Kindern das Lernen verbieten wollen.

Auch wenn es noch so oft behauptet wird, bleibt es falsch: Der Datenschutz steht gesellschaftlichen Herausforderungen nicht im Wege. Die Corona-Warnapp wurde in Deutschland mehr als 25 Millionen Mal heruntergeladen und hat nur deshalb eine so hohe Akzeptanz in der Bevölkerung gefunden, weil die Menschen sich darauf verlassen können, dass ihre Daten nicht zu unvorhersehbaren Zwecken missbraucht werden. Zudem kann sie datenschutzgerecht fortentwickelt werden. In anderen europäischen Ländern, in denen dies nicht der Fall ist, sieht es ganz anders aus. In Frankreich z. B. hat sich nur ein Bruchteil der Menschen beteiligt, was auch an dem fehlenden Vertrauen und der fehlenden Akzeptanz der dort genutzten zentralen Techniklösung liegt. Mit seinem datenschutzgerechten Weg ist in Deutschland eine Verbreitung gelungen, die eine wesentliche Voraussetzung zum Erreichen der Ziele der Corona-Warnapp ist.

Wenn Datenschützer*innen fordern, dass die Digitalisierung der Schulen datenschutzgerecht erfolgen muss, dient dies nicht der Verhinderung einer Digitalisierung der Schulen, sondern vielmehr einer nachhaltigen Entwicklung, die viel mehr schafft als eine Digitalisierung um jeden Preis: Hier geht es darum, sowohl den Schülerinnen und Schülern als auch den Lehrkräften einen geschützten Raum zu verschaffen, in dem sie sicher sein können, dass ihre Daten nicht missbraucht und irgendwann gegen sie verwendet werden. Und das ist ein wesentlicher Unterschied, der darauf abzielt, unsere Grundrechte und damit unsere freiheitliche Gesellschaft in eine digitalisierte Zukunft zu retten.

Nein, der Datenschutz ist kein Supergrundrecht, das über anderen Grundrechten steht, aber er ist ein Grundrecht. Und als Grundrecht steht er in einer ständig neu auszutarierenden Wechselwirkung mit den anderen Grundrechten. Genau deshalb wird er gerade in Zeiten der Pandemie dort, wo es nötig ist, immer wieder eingeschränkt - sei es bei der Kontaktdatenerhebung durch Betriebe oder beim Austausch von Daten zwischen Gesundheitsämtern und medizinischen Einrichtungen.

Die Debatte um die richtigen Maßnahmen gegen das Virus, gerade mit Blick auf den Datenschutz, muss wieder rationaler und sachlicher geführt werden. Bisher ist es in Deutschland gelungen, auch in der Krise die Grundrechte nicht über Bord zu werfen und eine ausgewogene Abwägung zu treffen, ob und in welchen Fällen es notwendig ist, ein Grundrecht zu Gunsten eines anderen einzuschränken. Dass die Entscheider es sich damit nicht leichtmachen, ist gut so, denn diese Anforderung stellt ein freiheitlicher Rechtsstaat, auch und gerade in Krisenzeiten. Dies sollten wir uns immer wieder bewusst machen.

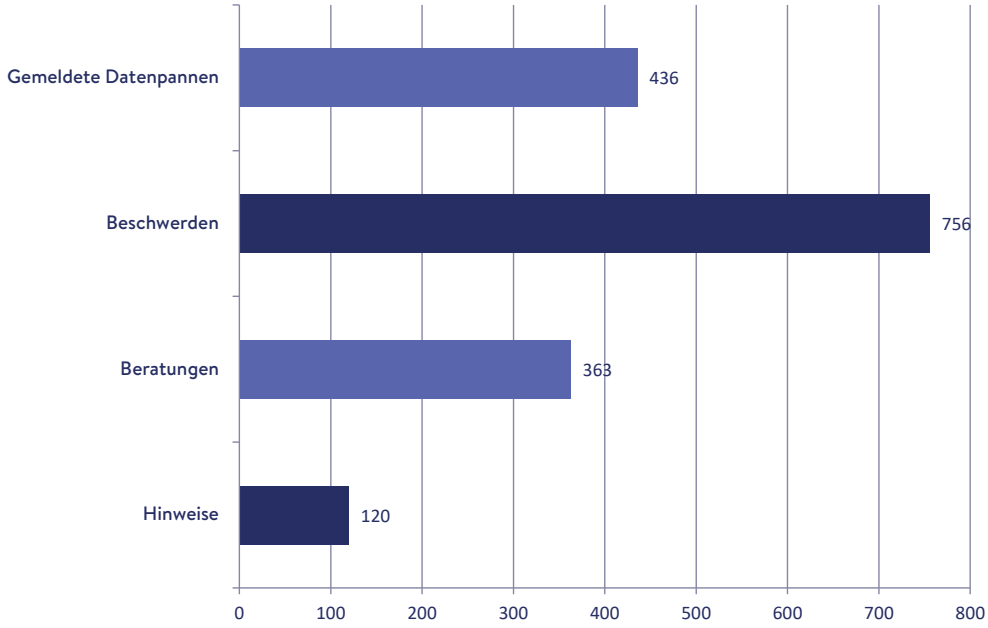
Ein angemessener Datenschutz darf dem Virus nicht zum Opfer fallen. Wir müssen den Datenschutz mit Vertrauen impfen und ihn vor haltlosen Attacken schützen. Anstatt immer wieder tretmühlenartig auf den Datenschutz zu schimpfen, sollten wir seine wichtige Bedeutung anerkennen: Der Datenschutz ist kein Verhinderer, sondern ein wichtiger Regulator und Steuerungsfaktor. Menschen lassen sich auf neue Technologien eher ein, wenn sie Vertrauen haben, dass ihre Rechte und Freiheiten gewahrt bleiben. Droht die Gefahr eines informationellen Kontrollverlusts, neigen Menschen dazu, sich ins Private zurückziehen oder Falschangaben machen.

Die Europäische Union hat das Potential eines starken Datenschutzes erkannt und mit einer geradezu unglaublichen Kraftanstrengung vor allem des Europäischen Parlaments ein einheitliches Datenschutzrecht für ganz Europa geschaffen. Damit hat sie ein kraftvolles Zeichen für die Bedeutung

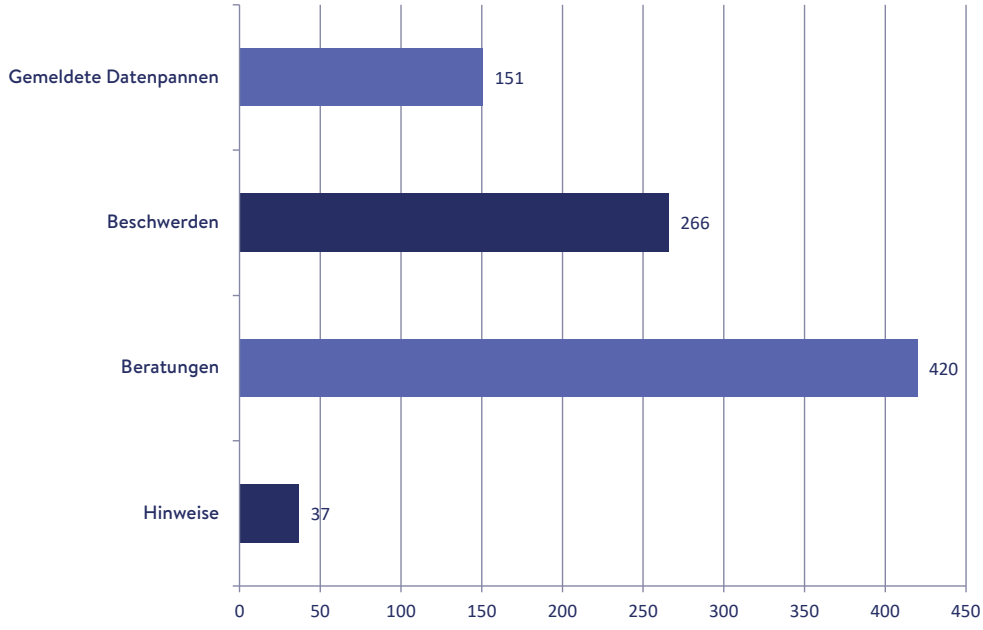
eines der grundlegenden europäischen Grundrechte gesetzt, an dem auch der Rest der Welt nicht mehr vorbeikommt. Denn sie hat erkannt, dass gerade das Recht auf Privatheit in Zeiten globaler Digitalisierung nur dann erhalten bleiben kann, wenn die europäischen Staaten sich zusammentun und als gemeinsamer Wirtschaftsraum auch ihre ethischen Überzeugungen verteidigen. Datenschutz ist Teil der europäischen Werte. Mit der Datenschutz-Grundverordnung (DS-GVO) wurde ein Maßstäbe setzendes Gesetz verabschiedet. In nicht wenigen Teilen der Welt wird es mittlerweile ganz oder in Teilen übernommen. Die DS-GVO hat Europa vorangebracht: Die EU bewährt sich hier als Bastion der Freiheit und Rechtsstaatlichkeit sowie als Schutzwall gegen Angriffe auf die Privatsphäre. Darauf sollten wir stolz sein!

I.
ZAHLEN UND FAKTEN

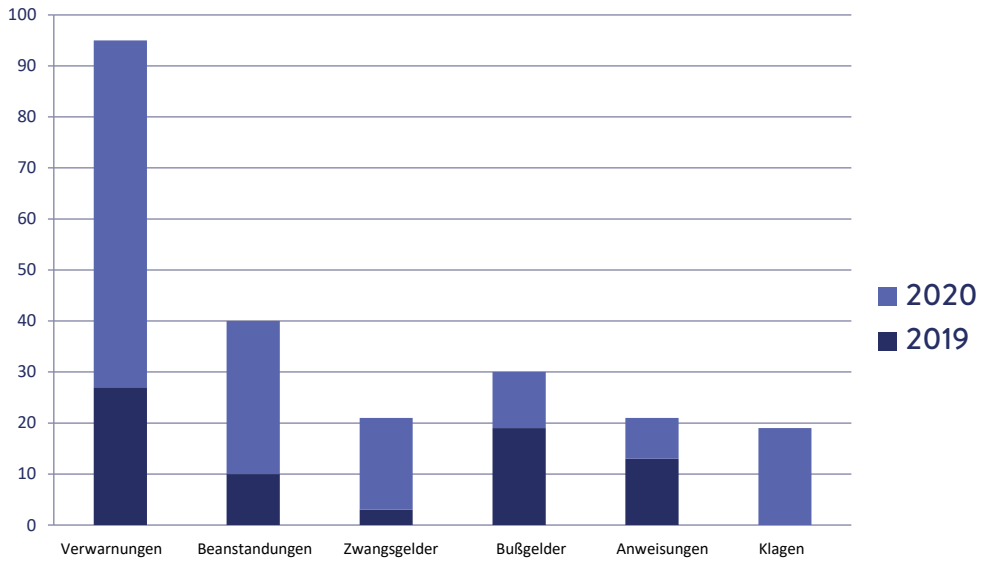
1. Geschäftsstatistik 2020: Privater Bereich



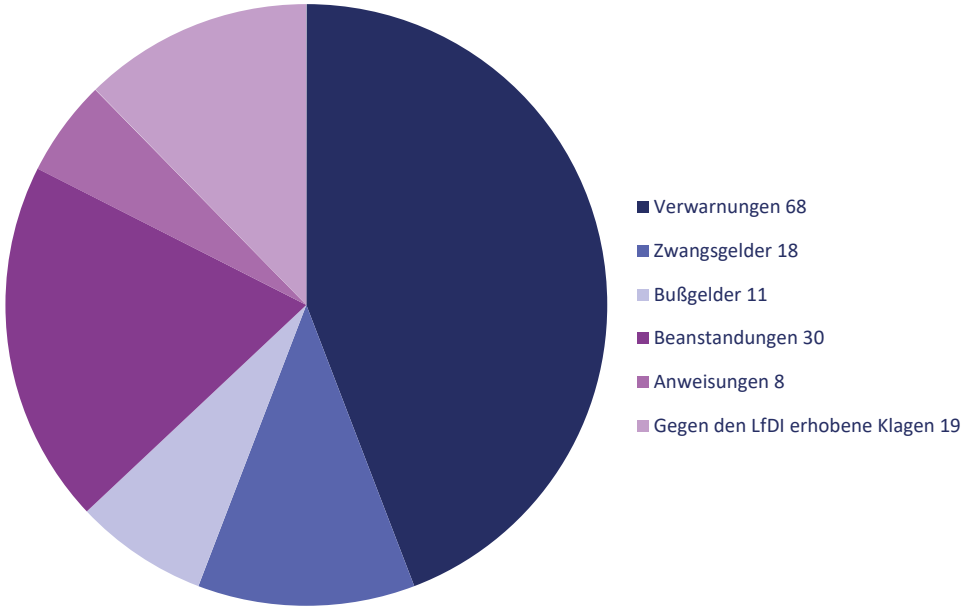
2. Geschäftsstatistik 2020: Öffentlicher Bereich



3. Ausgeübte Befugnisse 2019 und 2020



4. Ausgeübte Befugnisse 2020



II.
SACHGEBIETE

II. SACHGEBIETE

1. SICHERHEIT

Automatisierte Abfragen durch die Zentrale Bußgeldstelle im Fahreignungsregister

Im Rahmen von Ordnungswidrigkeitenverfahren der Zentralen Bußgeldstelle (ZBS) , die dem Polizeipräsidium Rheinpfalz in Ludwigshafen/Rhein angegliedert ist, wurde mit Versendung des Anhörbogens unter der Verwendung personenbezogener Daten eine automatisierte Abfrage im Fahreignungsregister (FAER) über eine Schnittstelle zum Kraftfahrt-Bundesamt getätigt, obwohl die betroffene Person nicht als Fahrzeugführer des Tatfahrzeugs feststand. Eine solche verfrühte Abfrage lässt sich auch nicht mit der Verpflichtung der Verfolgungsbehörde zu weitergehenden Ermittlungen begründen für den Fall, dass eine an den Fahrzeughalter versandte Anhörung nicht in Rücklauf gekommen ist. Die Anfrage ist nicht geeignet zum Ermittlungsziel, nämlich der Feststellung der Identität des Fahrzeugführers zum Tatzeitpunkt, beizutragen. Die Abfrage im Fahreignungsregister war nicht erforderlich und damit unzulässig.

Die Beanstandung des LfDI gegenüber dem Ministerium des Innern und für Sport Rheinland-Pfalz hat dazu geführt, dass der oben beschriebene automatisierte Abfrageprozess bei der ZBS - der insbesondere bei Personen durchgeführt worden ist, die zum Zeitpunkt der Abfrage nicht als Fahrer feststanden – nun manuell erst dann durch die Sachbearbeiter*in angestoßen wird, wenn die Fahrereigenschaft feststeht. Das Ergebnis der Abfrage wird automatisiert ebenfalls über die Schnittstelle vom Kraftfahrt-Bundesamt an die ZBS übersandt.

2. JUSTIZ

2.1 Erhebung von Besucherdaten in den Gerichten als Corona-Maßnahme

Auch Gerichte haben der Herausforderung der Corona-Pandemie zu begegnen. Sie müssen unter den Anforderungen des Infektionsschutzes für Besucherinnen und Besucher sowie für die Mitarbeitenden des Gerichts den Betrieb aufrechterhalten, hierzu zählt u.a. eine Kontaktnachverfolgung zu gewährleisten.

Nach der Beschwerde eines Rechtsanwalts an den LfDI hat das Justizministerium auf Veranlassung des LfDI eine Lösung entwickelt, um dies in datenschutzkonformer Weise umzusetzen. Den Gerichten wurde ein einheitliches Formular zur Verfügung gestellt, welches eine Kontaktnachverfolgung zum Infektions- und Gesundheitsschutz im Zusammenhang mit Covid- 19 gestattet. In diesem Formular haben die Besucher und Besucherinnen allein anzugeben, ob innerhalb der letzten 10 Tage Ihres Wissens nach ein persönlicher Kontakt mit einer mit Corona-infizierten Person bestand. Auf weitergehende Datenerhebungen wird verzichtet. In dem zuvor verwendeten Fragebogen, der Anlass zu der Beschwerde gegeben hatte, hatten alle Besucherinnen und Besucher u.a. Angaben zu allgemeinen Krankheitssymptomen wie z.B. Fieber, Husten, Kopfschmerzen machen müssen. Bei wahrheitsgemäßer Beantwortung des Fragebogens hätten so zahlreiche nicht infizierte Besucherinnen und Besucher befürchten müssen, erst nach Erläuterung ihres Gesundheitszustands oder gar nicht in das Gerichtsgebäude zu gelangen. Diese Erhebung von sensiblen Gesundheitsdaten durch die Gerichte war unverhältnismäßig und wurde nach Einschreiten des LfDI unverzüglich eingestellt.

2.2 Ersatzzustellung durch Gerichtsvollzieher nur in verschlossenem Umschlag

Im Berichtszeitraum ging eine Beschwerde über eine Gerichtsvollzieherin ein. Diese hatte einen Pfändungs- und Überweisungsbeschluss an den Arbeitgeber der Beschwerdeführerin zugestellt, indem dieser an einen Mitarbeiter, der in keiner Weise mit Personalangelegenheiten befasst gewesen ist, offen übergeben worden ist. Zwar ist eine Ersatzzustellung im Fall der Abwesenheit der Unternehmensleitung an jede beim Unternehmen beschäftigte Person möglich, allerdings sollte diese grundsätzlich in einem verschlossenen Umschlag erfolgen. Die Geschäftsanweisung für Gerichtsvollzieher regelt dies nicht eindeutig, da hierin die Möglichkeit einer offenen Übergabe an die bloße „Bereitschaft“ des jeweiligen Mitarbeiters zu Annahme anknüpft. Zwar ist die Geschäftsanweisung der Gerichtsvollzieher nicht geeignet, eine datenschutzrechtliche Befugnisnorm zu liefern, aber sie ist maßgeblich für das Handeln der Gerichtsvollzieher, sodass hier eine zweifelsfrei datenschutzkonforme Regelung getroffen werden sollte. Die Beschwerde hat den LfDI veranlasst, die Thematik gegenüber dem Justizministerium zur Sprache zu bringen. Dieses hat bestätigt, dass gegen eine Klarstellung dieser Regelung nichts einzuwenden ist und das für die Abstimmung der bundesweit einheitlichen Regelungen der Geschäftsordnung für Gerichtsvollzieher federführende Bundesland über das Klarstellungsbegehren informiert ist.

2.3 Veröffentlichungen von Insolvenzen durch Insolvenzverwalter

Eine Beschwerde machte den LfDI darauf aufmerksam, dass eine Insolvenzverwalterin regelmäßig die von ihr betreuten Insolvenzverfahren auf ihrer Internetpräsenz veröffentlicht. Der Zugang zu den personenbezogenen Daten der Insolvenzschuldner (Vor- und Nachname, Wohnanschrift und Insolvenzaktenzeichen) war uneingeschränkt möglich. Dies widersprach den Vorgaben der Insolvenzbekanntmachungsverordnung (InsoBekV). Nach § 2 Abs. 1 Nr. 3 InsoBekV dürfen Daten der Insolvenzschuldner spätestens nach Ablauf von 2 Wochen nach dem ersten Tag der Veröffentlichung nur noch abgerufen werden können, wenn die Abfrage den Sitz des Insolvenzgerichts und mindestens eine zusätzliche Angabe (Familiennamen, Firma, Sitz oder Wohnsitz des Schuldners, das Aktenzeichen des Insolvenzgerichts oder Registernummer und Sitz des Registergerichts) enthält. Diese Anforderung wurde von der Insolvenzverwalterin nicht erfüllt, weshalb sie eine Verwarnung des LfDI erhalten hat.

2.4 Datenverarbeitungen in Justizvollzugsanstalten

Die unterschiedlichen Datenverarbeitungen von Justizvollzugsanstalten sind immer wieder ein Thema des LfDI. In diesem Berichtszeitraum ging beispielsweise eine Beschwerde bzgl. der neuen Lichtbildausweise der Gefangenen einer JVA ein, die neuerdings die Gefangenenbuchnummer enthalten. Da der Lichtbildausweis beim „Umschluss“ offen an die Haftraumtür gesteckt wurde, konnten die Nummer nunmehr alle Mitinhaftierten lesen. Ein Datenschutzverstoß konnte in der Kennzeichnung der Lichtbildausweise mit der Gefangenenbuchnummer nicht gesehen werden. Allein die Vorgehensweise beim Umschluss war datenschutzrechtlich fragwürdig und wurde von der JVA dahingehend geändert, dass die Ausweise nunmehr mit der Rückseite nach vorne an die Haftraumtür gesteckt werden.

Eine andere Beschwerde betraf den zusätzlichen Buchstaben „S“ (für Strafhaft) hinter dem Namen an der Haftraumtür, derjenigen Gefangenen, die sich nicht in Untersuchungshaft befanden. Die Beschwerdeführerin, die als „Zivilhäftling“ inhaftiert war, wendete sich wegen dieser unrichtigen Einordnung ihrer Person als Strafhäftling an den LfDI. Eine Verarbeitung unrichtiger Daten verstößt gegen Art. 5 Abs. 1 lit. d DS-GVO. Die Befassung des LfDI mit dieser Angelegenheit bewirkte einen unverzüglichen Verzicht auf die unrichtige Zusatzinformation bei Gefangenen, die sich nicht in Untersuchungshaft befanden.

Durch eine weitere Beschwerde wurde die datenschutzwidrige Verwendung von Urinproben von Gefangenen im Rahmen einer europäischen Studie zum Phänomen neuer psychoaktiver Substanzen in Justizvollzugsanstalten offenbar. Die prinzipiell mögliche Verarbeitung von personenbezogenen Daten von Gefangenen im Zusammenhang mit wissenschaftlichen Forschungsprojekten, auch ohne deren Einwilligung, verstieß deswegen gegen das Datenschutzrecht, weil eine „Anonymisierung“ der Urinproben von Seiten der Justizvollzugsanstalt nicht vorgenommen worden ist, bevor eine Übersendung an das zuständige Labor erfolgt ist. Die Proben wurden zusammen mit der regulären Testung auf Drogenabstinenz an das Labor weitergegeben. Für das Labor wäre es damit ohne besonderen Aufwand möglich gewesen, die im Rahmen der Studie durchgeführte Urinanalyse den einzelnen Gefangenen zuzuordnen.

2.5 Das neue Landesjustizvollzugs datenschutzgesetz Rheinland-Pfalz (LJVollzDSG)

Der LfDI hatte bereits in seinem letzten Tätigkeitsbericht angeführt, eine Stellungnahme zu dem Musterentwurf abgegeben zu haben. Hieran schloss sich, nach Überarbeitung des Justizministeriums Rheinland-Pfalz zur Anpassung an das Landesrecht, eine weitere Stellungnahme an. Das LJVollzDSG ist nunmehr seit dem 09.06.2020 in Kraft. Die Empfehlungen des LfDI wurden größtenteils umgesetzt. So wurde beispielsweise die datenschutzrechtliche Verantwortlichkeit der Justizvollzugsbehörden im LJVollzDSG ausdrücklich festgehalten und sichergestellt, dass bei einer Verweigerung der Einwilligung in die Datenverarbeitung eine Aufklärung über die damit einhergehenden Folgen zu erfolgen hat. Die möglichen Datenverarbeitungen wurden unter dem Gesichtspunkt der Erforderlichkeit weitergehender eingeschränkt, als dies der ursprüngliche Entwurf des Justizministeriums vorgesehen hatte. Hervorzuheben ist auch, dass bzgl. der Regelung über die Benachrichtigung bei Datenverarbeitung ohne Kenntnis der betroffenen Person im Falle der Übermittlung an bestimmte öffentliche Stellen dem Vorschlag des LfDI gefolgt worden ist. Deren notwendige Zustimmung bzgl. der Benachrichtigung können diese nunmehr nur verweigern, sofern die Benachrichtigung die Erfüllung ihrer eigenen Aufgaben gefährden würde. Der ursprüngliche Entwurf des LJVollzDSG hatte dies noch nicht enthalten. Die grundsätzliche Kritik des LfDI an der Benennung der Einwilligung als Rechtsgrundlage bei Gefangenen hat demgegenüber keinen Anklang gefunden. Eine Legaldefinition der „unbedingten Erforderlichkeit“, welche oftmals eine wesentliche Tatbestandvoraussetzung bei den einzelnen Datenverarbeitungsgrundlagen darstellt, ist ebenfalls nicht erfolgt.

3. VIDEOÜBERWACHUNG

Der Einsatz von opto-elektronischen Geräten ist weiterhin weit verbreitet, zumal leistungsfähige Aufnahmegeräte regelmäßig auch über die Discounter angeboten werden. Im Vergleich zum Jahr 2019 hat sich 2020 eine deutliche Zunahme der Beschwerden aus dem nachbarschaftlichen Bereich ergeben (insgesamt 180 Fälle). Dies ist sicher der (teilweisen) Schließung vieler Geschäftsbereiche geschuldet, aber auch der gestiegenen Sensibilisierung durch den verstärkten Aufenthalt im häuslichen Umfeld.

Videoüberwachung wird gesellschaftlich wie politisch weiterhin kontrovers diskutiert. Während sie zum Teil als Allheilmittel für Eigentumsschutz und Kriminalitätsprävention gesehen wird, steigt aber auch die Zahl der Menschen, die einer Überwachungskamera mit einem gewissen Misstrauen begegnen. Das Meinungsbild reicht vom Gefühl einer schwerwiegenden Beeinträchtigung bis zu Gleichgültigkeit bzw. Unverständnis für datenschutzrechtliche Anforderungen. Dies zeigt sich auch darin, dass Entscheidungen der Aufsichtsbehörden mitunter weder von den Verantwortlichen und noch von den Beschwerdeführern akzeptiert werden.

In der Aufsichtspraxis binden nachbarschaftliche Verfahren einen Großteil der Ressourcen. Die im letzten Jahr deswegen verstärkt eingeforderte Mitwirkung der Beschwerdeführer hat Wirkung gezeigt. Ein Großteil der Beschwerden ist seitdem formal vollständig. Inhaltlich bleibt jedoch festzustellen, dass dieser Bereich durch Nachbarschaftsstreitigkeiten geprägt ist, bei denen der Datenschutz in Form von Videoüberwachungen nur Mittel zum Zweck ist. Nachdem das Verwaltungsgericht Mainz derzeit die Anordnung der Deinstallation von Kameras als nicht durch die DS-GVO gedeckt ansieht, wird hier verstärkt auf den Zivilrechtsweg verwiesen.

Die Fortführung gezielter anlassloser Ortsbegehungen auch für den Bereich der Videoüberwachung konnte aufgrund der Pandemielage im Jahr 2020 nicht wie beabsichtigt umgesetzt werden.

Im Rahmen der Einleitung und Durchsetzung von Bußgeldverfahren wurden die ersten Verfahren gerichtlich entschieden. Hierbei handelte es sich um Videoüberwachungen in Gewerbebetrieben. Das zuständige Amtsgericht bestätigte hier in allen Fällen, dass Datenschutzverstöße vorlagen, verneinte jedoch in vielen Fällen die Ahndungsbedürftigkeit.

Im öffentlichen Bereich ist das Beratungsaufkommen nach wie vor hoch. Oft wurde von den öffentlichen Stellen als Verantwortliche nicht wahrgenommen, dass eine Videoüberwachung kein vernachlässigbarer, sondern ein erheblicher Eingriff in die Grundrechte der Bürgerinnen und Bürger darstellt. Auch wird weiterhin die Einrichtung einer Videoüberwachung häufig vorschnell als einzige Lösung bestehender Probleme angesehen. Alternative mildere Mittel werden zu selten geprüft. Vor diesem Hintergrund ist es besonders erfreulich, dass im öffentlichen Bereich wegen Videoüberwachung lediglich eine Maßnahme gem. Art. 58 Abs. 2 Datenschutz-Grundverordnung ausgesprochen werden musste. Vielmehr konnten möglicherweise rechtswidrige Maßnahmen durch die Beratungstätigkeit im Vorfeld vermieden werden. Auffällig war insgesamt die Anzahl der Anfragen von Kommunen zur Überwachung der Müllentsorgung, die durch meine Behörde - soweit abschließend bearbeitet - als unzulässig bewertet wurden.

Pandemiebedingt war die Anzahl der Veranstaltungen, die durch Behörden, Polizei oder sonstige öffentlichen Stellen mit Videoüberwachung begleitet wurden, gering. Im Rah-

men der Vorbereitung einer bedeutenden Ausstellung in Mainz kam das Landesmuseum Rheinland-Pfalz auf den LfDI zu, um das Videokonzept im Außenbereich des Ausstellungsgebäudes zu prüfen.

Zudem machte die Einrichtung von Impfzentren in Rheinland-Pfalz in Abhängigkeit von Gebäudestrukturen und Zutrittsmöglichkeiten in bestimmten Bereichen eine Videoüberwachung erforderlich. Meine Behörde legte nach einer örtlichen Feststellung in einem Impfzentrum dazu Leitlinien fest, die sowohl die Persönlichkeitsrechte der zu impfenden Personen als auch das Sicherheitsinteresse der verantwortlichen Kommunen berücksichtigt.

Die Prüfung der Einhaltung dieser Leitlinien wird meine Behörde auch zukünftig im weiteren Betrieb der Impfzentren beschäftigen.

4. WIRTSCHAFT

4.1 Datenverarbeitung durch Private in Zeiten von Corona

Die Einschränkungen aufgrund der Corona-Pandemie hat Verantwortlichen in der Privatwirtschaft auch in datenschutzrechtlicher Hinsicht Einiges abverlangt.

Bei den stets geöffneten Anbietern von Gütern des täglichen Bedarfs, also Supermärkten, Drogerien und anderen Einzelhändlern, stand anfangs die Frage im Raum, ob dort die Körpertemperatur der Kunden z.B. mittels einer Wärmebildkamera gemessen werden durfte, bevor sie das Ladengeschäft betreten. Eine erhöhte Körpertemperatur hätte ein Indiz für eine Corona-Infektion sein können. Beim Überschreiten einer gewissen Temperatur könnte dem Kunden der Zutritt verwehrt werden bzw. er könnte zu weiteren Erklärungen über seinen Gesundheitszustand aufgefordert werden. Solche Maßnahmen sollten verhindern, dass Personen, die ein mögliches Covid-19-Symptom aufweisen, nämlich eine erhöhte Körpertemperatur, das Ladengeschäft betreten.

Bei der Feststellung der Körpertemperatur von Personen handelt es sich um die Erhebung von personenbezogenen Daten, und zwar von Gesundheitsdaten im Sinne von Art. 9 Abs. 1 DS-GVO. Bei der Auswertung dieser Daten mit dem Ziel, bestimmten Personen den Zugang zu verweigern, werden diese Gesundheitsdaten weiterverarbeitet. Die Verarbeitung solcher Gesundheitsdaten ist gem. Art. 9 Abs. 1 DS-GVO untersagt, außer in den in Art. 9 Abs. 2 DS-GVO genannten Ausnahmefällen.

Da die Voraussetzungen dieser Ausnahmen, z.B. eine informierte Einwilligung oder eine zweckgebundene rechtliche Regelung, hier nicht vorlagen, hat der LfDI von dieser Maßnahme abgeraten.

Als dann weitere Dienstleister, insbesondere Gaststätten, Hotels, Freizeiteinrichtungen etc., wieder öffnen durften, waren diese verpflichtet, die Kontaktdaten ihrer Gäste, Besucher und Kunden zu erheben. Zu diesen Kontaktdaten gehörten und gehören der vollständige Name, die Adresse und die Telefonnummer. Dies sollte in datenschutzgerechter Weise erfolgen, wie es die jeweilige Corona-Bekämpfungsverordnung in Rheinland-Pfalz formulierte. Wie dies datenschutzgerecht erfolgen kann, hat der LfDI zeitnah in seinen FAQ dargestellt: Hier kommt es insbesondere darauf an, dass Dritte keinen Einblick in die Daten erhalten, also das Auslegen einer offenen Liste ist unzulässig. Die Daten dürfen nur für eine mögliche Übermittlung an das anfragende Gesundheitsamt genutzt werden, ansonsten sind sie geschützt vor unberechtigten Zugriffen aufzubewahren und taggenau nach Ablauf von zunächst einem Monat, zwischenzeitlich von vier Wochen zu löschen.

Den LfDI erreichten zahlreiche Hinweise, dass oftmals offene Listen bei den Verantwortlichen auslagen. In diesen Fällen wurden die Verantwortlichen stets auf die datenschutzrechtlichen Anforderungen hingewiesen, die in der Regel auch unverzüglich umgesetzt wurden.

Viele Bürgerinnen und Bürger sahen sich durch die Pflicht zur Angabe ihrer Kontaktdaten in ihrem Recht auf informationelle Selbstbestimmung unverhältnismäßig eingeschränkt. Manche hatten Sorge, dass ihre Daten missbraucht werden könnten oder hielten die Angabe der reinen Telefonnummer für ausreichend. Der LfDI musste in diesen Fällen auf den Verordnungsgeber verweisen. Dieser hält es für erforderlich, alle genannten Daten für eine Kontaktnachverfolgung anzugeben, was aus datenschutzrechtlicher Sicht nicht zu widerlegen ist.

Die Datenverarbeitung in Form der Kontakterfassung findet ihre rechtliche Grundlage in Art. 6 Abs. 1 lit. c DS-GVO i.V.m. § 32 S. 1, 28

Abs. 1 Satz 1 und 2 IfSG und der aktuell geltenden Corona-Bekämpfungsverordnung.

Teilweise gingen Verantwortliche dazu über, die Ausweise ihrer Kunden und Gäste zu kontrollieren, da manche Fantasienamen angegeben hatten. Grundsätzlich ist es zulässig, den Ausweis zur Identifizierung auch im privaten Geschäftsverkehr vorzulegen bzw. ihn sich vorlegen zu lassen, eine Verpflichtung hierzu besteht jedoch nicht. Dies gilt auch dann noch, wenn die Corona-Bekämpfungsverordnung nunmehr eine sog. Plausibilitätsprüfung der angegebenen Kontaktdaten durch den Verantwortlichen vorsieht. Der Verantwortliche muss danach prüfen, ob die angegebenen Kontaktdaten vollständig sind und ggf. offenkundig falsche Angaben enthalten. Personen, die die Erhebung ihrer Kontaktdaten verweigern oder offenkundig falsche oder unvollständige Angaben machen, dürfen nicht bedient werden. Eine Pflicht, sich den Personalausweis vorlegen zu lassen bzw. diesen vorzulegen, ergibt sich hieraus nicht.

Manchmal wurde auch eine Unterschrift verlangt. Dies stellt die Erhebung eines zusätzlichen personenbezogenen Datums dar, wofür es in der Verordnung keine Rechtsgrundlage gibt. Von der Einholung der Unterschrift zu den Kontaktdaten ist daher von den Verantwortlichen abzusehen.

Mittlerweile gibt es einige Anbieter, die Lösungen für eine digitale Erfassung der Kontaktdaten auf den Markt bringen. Auch diese Entwicklungen wurden und werden vom LfDI datenschutzrechtlich begleitet.

Der Verordnungsgeber sieht mittlerweile auch ausdrücklich die Möglichkeit vor, dass die Kontaktdaten digital erfasst werden unter Einhaltung der Datenschutzbestimmungen. Der zur Erfassung verpflichtete Dienstleister bleibt, auch wenn er das Produkt eines Dritten nutzt, verantwortlich für die ordnungsgemäße Löschung der Daten. Die Nutzung der digitalen Erfassung ist freiwillig. Wenn der Kunde oder Gast dies nicht möchte, muss ihm eine papiergebundene Datenerfassung angeboten werden.

In manchen Bereichen, die nicht unter die Pflicht zur Kontakterfassung fallen, und auch im privaten Bereich werden teilweise ebenfalls Kontaktdaten erfasst. Grundsätzlich ist dies nicht unzulässig, wenn eine solche Erfassung aufgrund einer informierten und freiwilligen Einwilligung beruht.

In allen Fällen sind die betroffenen Personen stets von den Verantwortlichen transparent und verständlich zu informieren.

Dem LfDI wurden auch einige Fälle des Missbrauchs der Kontaktdaten bekannt. So wurden diese genutzt, um z.B. einen besonders sympathischen Gast privat zu kontaktieren, Werbung zu versenden oder gegen eine Bewertung in den sozialen Medien vorzugehen. In diesen Fällen hat der LfDI Verfahren gegen die Verantwortlichen eingeleitet und diese mit der Verhängung einer datenschutzrechtlichen Sanktion beendet.

Im Rahmen des Vereinssports kam es zu Abfragen von Gesundheitsdaten, bevor Mitglieder an den Übungsstunden teilnehmen durften. Es wurde nach Erkältungssymptomen, Kontakt zu Infizierten und Aufenthalten in Risikogebieten gefragt. Diese Abfragen wurden auf die Vorgaben der Corona-Bekämpfungsverordnung bzw. des Gesundheitsamtes gestützt. Man wollte sicher gehen, dass nur gesunde Personen an den Übungsstunden teilenehmen. Die Angabe solcher Informationen ist durch den Verordnungsgeber aber nicht vorgesehen. Daher bestand hier keine rechtliche Verpflichtung für den Verein, diese zu erheben. Solche Gesundheitsdaten hätten nur erhoben werden dürfen, wenn die betroffenen Personen hierin einge-

willigt haben. Eine Einwilligung wiederum ist nur wirksam, wenn sie informiert und freiwillig erfolgt. Der LfDI empfahl daher, von einer solchen Befragung abzusehen. Alternativ konnte in die Teilnahmebedingungen einen Passus aufgenommen werden, wonach nur solche Personen an den Übungsstunden teilnehmen dürfen, die keine Symptome aufweisen und auch kein anderes Kriterium erfüllen. Die Kenntnisnahme der Teilnahmebedingungen konnte sich der Verein dann bestätigen lassen.

Als der Verordnungsgeber die Pflicht zum Tragen eines Mund-Nasenschutzes, die sog. Maskenpflicht, einführte, warf dies neue datenschutzrechtliche Fragen auf. So besteht die Maskenpflicht z.B. nicht für Personen, denen das Tragen einer Bedeckung wegen einer Behinderung oder aus gesundheitlichen Gründen nicht möglich oder unzumutbar ist. Dies ist durch ärztliche Bescheinigung nachzuweisen. Fraglich war nun, welche Angaben die ärztliche Bescheinigung enthalten muss bzw. darf und ob auch Kopien einer solchen Bescheinigung angefertigt werden dürfen. Auch hierzu erreichten den LfDI zahlreiche Anfragen, in denen auch Zweifel geäußert wurden, ob private Stellen überhaupt diese Bescheinigungen einsehen dürfen.

Für betroffene Personen bedeutet dies, dass sie auf Verlangen die ärztliche Bescheinigung vorlegen müssen, aus der sich ihre Identitätsdaten ergeben müssen. Auch muss für den Verantwortlichen erkennbar sein, dass die Bescheinigung von einem Arzt ausgestellt ist. Weitere Angaben zur Diagnose muss das Attest zumindest beim Besuch von Einzelhändlern und Gewerbetreibenden nicht enthalten. Der LfDI empfahl daher, eine ärztliche Bescheinigung mitzuführen, die nur die genannten Angaben enthält, nicht aber die Diagnose.

Es ist nicht erforderlich, eine Kopie der Bescheinigung anzufertigen. Inwieweit Einzelhändler oder Gewerbetreibende den Zutritt zu ihren Räumlichkeiten ganz verweigern dürfen, wenn der Mund-Nasen-Schutz nicht getragen bzw. keine Befreiung nachgewiesen wird, ist letztlich keine datenschutzrechtliche Frage. Vielmehr müssen die Einrichtungen unter Berücksichtigung der ohne das Tragen eines Mund-Nasen-Schutzes resultierenden objektiven Gesundheitsgefährdung und der ihnen zustehenden Vertragsfreiheit zunächst selbst entscheiden, ob und inwieweit sie unter diesen Bedingungen ihre Leistungen anbieten.

4.2 Steuerberater als Verantwortliche

Viele Steuerberaterinnen und -berater führen für ihre Kunden auch die Lohn- und Gehaltsabrechnung durch. Aus datenschutzrechtlicher Sicht war es bisher fraglich, ob sie dann als Auftragsverarbeiter handeln oder ob ihnen die Aufgabe zur selbständigen Erledigung übertragen wird.

Nunmehr hat der Gesetzgeber im Steuerberatungsgesetz eine Klarstellung getroffen: In der Neufassung des § 11 Steuerberatungsgesetz (StBerG) vom Dezember 2019 wird festgestellt, dass Steuerberaterinnen und -berater bei der Erbringung von Leistungen nach dem Steuerberatungsgesetz stets als datenschutzrechtlich Verantwortliche anzusehen sind und eine Auftragsverarbeitung nicht mehr in Betracht kommt.

Demnach erfolgt eine Verarbeitung personenbezogener Daten durch Steuerberaterinnen und -berater unter Beachtung der für sie geltenden Berufspflichten weisungsfrei. Dies gilt auch dann, wenn sie im Rahmen ihrer gesetzlichen Pflichten geschäftsmäßig Hilfeleistung in Steuersachen erbringen und dabei personenbezogene Daten ihrer Mandanten verarbeiten.

Ausweislich der Gesetzesbegründung sind davon auch das Buchen laufender Geschäfts-

vorfälle, die laufende Lohnabrechnung und das Fertigen der Lohnsteuer-Anmeldungen umfasst. Auch diese werden als weisungsfreie Tätigkeiten angesehen, da auch sie die eigenverantwortliche Prüfung und Anwendung der gesetzlichen Bestimmungen umfassen.

Steuerberaterinnen und -berater sind demnach bei der Erbringung von Leistungen nach dem Steuerberatungsgesetz nun stets als datenschutzrechtlich Verantwortliche anzusehen. Mit dieser Klarstellung sind auch die Anfragen an den LfDI, wie die Tätigkeit im Bereich der Lohn- und Gehaltsabrechnung datenschutzrechtlich zu qualifizieren ist, deutlich zurückgegangen.

4.3 FSV Mainz 05: E-Mail Post vom Lieblingsverein nach Heimspiel

Nach dem Heimspiel gegen Borussia Mönchengladbach am 24. August 2019 wertete der 1. FSV Mainz 05 e.V. aus, welche verkauften Tickets zum Betreten des Stadions genutzt wurden. Basierend auf dieser Auswertung versandte der Verein an 10.103 Ticketkäufer E-Mails. Dabei erhielten die Ticketkäufer, deren Tickets nicht zum Betreten des Stadions genutzt wurden, einen anderen E-Mail-Inhalt als die Ticketkäufer, von denen man davon ausging, dass sie beim Spiel im Stadion anwesend waren, da ihr Ticket für den Zugang zum Stadion genutzt wurde. Wurde das Ticket zum Betreten des Stadions genutzt, enthielt die E-Mail einen Dank für die Unterstützung beim Spiel. Wurde das Ticket hingegen nicht benutzt, wurde das Bedauern darüber ausgedrückt, dass der Ticketkäufer beim Spiel nicht anwesend war. Weder für die Auswertung des Stadionzugangs noch für den Versand der E-Mail konnte der Verein Einwilligungen der betroffenen Personen vorlegen. Die Verarbeitung konnte auch nicht auf eine andere Rechtsgrundlage gestützt werden.

Der LfDI verwarnte den Verein aufgrund dieses Sachverhalts Anfang 2020, da er ohne die Einwilligung der betroffenen Personen das Betretungsverhalten von 10.103 Personen beim Heimspiel ausgewertet hat, um im Anschluss eine E-Mail mit gezielten Informationen – je nachdem ob die betroffene Person beim Spiel anwesend war oder nicht – an 10.103 Personen zu versenden.

Im Rahmen der Gespräche und dem Schriftverkehr mit dem Verein zum o.g. Sachverhalt, teilte der Verein mit, dass er zukünftig die Auswertung des Zutrittsverhaltens der Ticketinhaber beim Betreten des Stadions in einen Passus in seiner Allgemeinen Ticketbedingungen (ATGB) aufnehmen wolle. Der Verein ging davon aus, dass die Auswertung des Zutrittsverhaltens dann Vertragsbestandteil würde und es den Kunden frei stünde, diesen Vertrag mit ihm zu schließen, die Tickets anonym im Fanshop zu kaufen oder auf einen Stadionbesuch zu verzichten. Jeder Kunde habe außerdem weiterhin die Möglichkeit, dem Erhalt von Werbemails des Vereines zu widersprechen.

Der LfDI sprach daraufhin eine Warnung aus, dass die Auswertung des Zutrittsverhaltens der Ticketinhaber beim Betreten des Stadions zur werblichen Ansprache ohne die Einwilligung der betroffenen Personen gegen Art. 6 Abs. 1 DS-GVO verstößt. Allein die Aufnahme eines Abschnitts in die ATGB, dass eine Auswertung des Zutrittsverhaltens der Ticketinhaber beim Betreten des Stadions erfolgt, macht die Auswertung zwar unter Umständen zu einem Vertragsbestandteil, jedoch ist die Auswertung weiterhin keine Verarbeitung, die zur Erfüllung des Vertrags erforderlich ist, wie es Art. 6 Abs. 1 lit. b DS-GVO verlangt. Die Auswertung des Zutrittsverhaltens ist hingegen nur dann zur Erfüllung des Vertrages erforderlich, wenn das Betreten des Stadions durch den Ticketinhaber eine zwingende Bedingung für das Vertragsverhältnis oder für zukünftige Verträge wäre. Der Verein hatte dargelegt, dass es einzelne Vereine

gebe, die ihren Kunden Dauerkarten abnehmen oder sie für den Kauf für Tickets für zukünftige Spiele sperren, wenn sie die gekauften Tickets nicht zum Betreten des Stadions nutzten, sondern verfallen lassen. In diesen Fällen ist die Vertragsleistung auf Seiten des Vereins die Zutrittsberechtigung ins Stadion am Spieltag und die Vertragsleistung des Kunden, das Ticket zu bezahlen sowie am Tag des Spiels das Ticket zur Betretung des Stadions zu nutzen. Kommt der Ticketkäufer seinen Vertragspflichten nicht nach, können daran Konsequenzen wie die Aberkennung der Dauerkarten oder die Sperrung für zukünftige Ticketkäufe geknüpft werden. Um die Erfüllung dieser Vertragsleistungen des Ticketkäufers kontrollieren zu können, können die Vereine (ausschließlich) in diesem Fall dazu das Betretungsverhalten der Ticketkäufer kontrollieren. Der 1. FSV Mainz 05 e.V. teilte jedoch mit, dass die Gegenleistung des Ticketkäufers weiterhin nur eine monetäre sein soll. Weder soll der Kunde mit seinen Daten zahlen noch hat er eine Präsenzpflicht im Stadion am Spieltag, zu deren Kontrolle eine Auswertung des Betretungsverhaltens erforderlich wäre. Aufgrund der Corona Pandemie wurde der Besuch von Fans im Stadion kurz nach der Warnung des LfDI eingestellt. Das vom Verein geplante Vorhaben der Auswertung des Zutrittsverhaltes wurde aufgrund dessen nicht weiter betrieben.

4.4 Hacker-Angriff auf die Technischen Werke Ludwigshafen (TWL) offenbart konzernweite Datenschutzdefizite

Die TWL entdeckte nach eigenen Angaben am 20. April 2020, dass Kriminelle Daten aus internen Daten-Systemen der TWL gestohlen hatten. Trotz umgehend eingeleiteter Maßnahmen wurden die Daten von 150.000 Kunden sowie 1300 Beschäftigten gestohlen. Es handelt sich um Namen, Anschriften und zum Teil um Bankverbindungen. Die TWL unterrichteten umgehend das Dezernat der Kriminalpolizei, das Dezernat Cybercrime des Landeskriminalamtes Rheinland-Pfalz und das Bundesamt für Sicherheit in der Informationstechnik. Die TWL meldeten dem LfDI innerhalb der vorgesehenen Frist (72 Stunden) eine Verletzung des Schutzes personenbezogener Daten im Sinne des Artikel 33 Datenschutz-Grundverordnung.

Im Laufe der Ermittlungen stellte sich heraus, dass es den Kriminellen bereits Mitte Februar 2020 über einen infizierten E-Mail-Anhang gelungen war, Zugang zu dem IT-Netz der TWL zu erlangen. Die TWL konnten eine Verschlüsselung der Systeme sowie einen Zugriff auf die Prozessleittechnik des Unternehmens verhindern, sodass die Versorgung der Stadt Ludwigshafen zu keinem Zeitpunkt gefährdet war. Am 30. April 2020 nahm die Hackergruppe Kontakt zu den TWL auf und versuchte, Lösegeld im zweistelligen Millionenbereich zu erpressen. Gedroht wurde mit der Veröffentlichung der gestohlenen Daten. Der vom Datendiebstahl betroffene Personenkreis erhielt zudem ab dem 11. Mai 2020 E-Mails, in denen den TWL mangelnde Kooperation und Fehlverhalten vorgeworfen wurden. Als die TWL nicht auf die Forderung der Hackergruppe einging, veröffentlichen die Täter die Daten im sogenannten Darknet.

Der Angriff war auf das Fehlverhalten eines Mitarbeiters bei der Bearbeitung einer E-Mail zurückzuführen. Die Person öffnete entgegen bestehender, interner TWL-Vorgaben eine E-Mail mit Anhang, die eine Schadsoftware enthielt. Der LfDI nahm aufgrund dieses Vorfalls umfangreiche Ermittlungen auf. Im Rahmen dieser Ermittlungen wurde offenbart, dass der Angriff nur möglich war, da das Unternehmen allen Mitarbeitern das Öffnen von ausführenden Makros erlaubt hatte, unabhängig davon, ob diese Funktion für die tägliche Arbeit notwendig war. Des Weiteren wurde im Rahmen der Aufarbeitung des Vorfalls deutlich, wie es zu einer so hohen Zahl an betroffenen Personen kommen konnte: Aufgrund fehelender Löschung und Sperrung personenbezogener

Daten ehemaliger Kunden, war es den Angreiffern möglich, nicht nur auf die Daten der derzeitigen Kunden des Unternehmens, sondern auch auf die Daten von Kunden, die früher einen Vertrag mit dem Unternehmen hatten, zuzugreifen.

Während der Sachverhalt im Berichtszeitraum abschließend ermittelt werden konnte, sind die aufsichtsrechtlichen Maßnahmen und Sanktionen im Berichtszeitraum noch zu keinem Abschluss gekommen und werden den LfDI im Jahr 2021 weiter begleiten.

5. LEBEN DIGITAL

5.1 Die datenschutzrechtliche Verantwortlichkeit von Wohnungseigentümergemeinschaften (WEG) und Hausverwaltungen

An den LfDI werden sowohl seitens der Wohnungseigentümergemeinschaften (WEG) als auch von den Hausverwaltungen immer wieder Fragen im Hinblick auf die datenschutzrechtliche Verantwortlichkeit dieser Stellen gerichtet. Insbesondere aufgrund des Urteils des Amtsgerichts Mannheim (Urt. v. 11.09.2019 – 5 C 1733/19 WEG), durch welches erstmals von Seiten der Rechtsprechung Stellung zu dieser Frage genommen wurde, beschäftigte sich der LfDI im Jahr 2020 verstärkt mit Fragen der Verantwortlichkeit in der Immobilienwirtschaft. Im Rahmen von Tätigkeiten der WEG und Hausverwaltungen fallen viele verschiedene Datenverarbeitungsvorgänge an. So werden personenbezogene Daten etwa bei der bloßen Eigentümer- bzw. Mieterverwaltung, der Abrechnung von Nebenkosten, der Versendung von Informationsschreiben sowie der Schlichtung von Streitigkeiten oder auch bei der Einführung von Videoüberwachungsmaßnahmen verarbeitet. Da diese verschiedenen Verarbeitungsvorgänge mithin verschiedene Lebens- und Personenbereiche betreffen, stellt sich immer wieder die Frage, welche Stelle für welche Verarbeitungsvorgänge verantwortlich ist.

Gemäß Artikel 4 Nr. 7 DS-GVO ist Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Anhand dieser Kriterien wird deutlich, dass keine generelle Aussage hinsichtlich der Verantwortlichkeit getroffen werden kann. Je nach Vorgang ist es denkbar, dass entweder ausschließlich die WEG oder ausschließlich die Hausverwaltung oder ggf. auch beide gleichrangig für die Datenverarbeitung verantwortlich sind.

Im Rahmen der Verantwortlichkeit können demnach folgende Abgrenzungskriterien herangezogen werden:

1. Der Verwalter ist überwiegend alleinverantwortlich, soweit er seine originären Verwalteraufgaben (vgl. §§ 27, 28 Wohnungseigentumsgesetz) ausführt.

2. Führt der Verwalter einen Beschluss der Eigentümergemeinschaft aus (z.B. Entscheidung über eine Videoüberwachung im Haus), so ist es wahrscheinlich, dass die WEG datenschutzrechtlich verantwortlich ist und der Verwalter die Aufgaben nur auf Weisung der WEG ausführt und somit keine eigenen Entscheidungen über Zwecke und Mittel der Verarbeitung trifft. Wenn diese der Fall ist, liegt ggf. eine Auftragsverarbeitung i.S.v. Art 28 DS-GVO vor. Für die Frage, ob es sich gegebenenfalls um eine Auftragsverarbeitung handelt, sollte jedoch immer der konkrete Beschluss bzw. die Datenverarbeitung im Einzelfall geprüft werden.

3. Es ist nicht ausgeschlossen, dass es auch Fälle geben kann, in denen die WEG und der Verwalter als gemeinsame Verantwortliche i.S.v. Art. 26 DS-GVO agieren. Auch dies ist anhand des konkreten Einzelfalles zu beurteilen.

Die Abgrenzung der Verantwortlichkeit des Hausverwalters zur Verantwortlichkeit der WEG folgt dabei aus folgenden Überlegungen:

Die WEG schließt mit dem Verwalter einen Vertrag ab, der zum Gegenstand die Hausverwaltung hat. Im Rahmen dieser Dienstleistung verarbeitet der Hausverwalter die personenbezogenen Daten in eigener Verantwortung. Der

Verwalter ist also Verantwortlicher für die Datenverarbeitung innerhalb seines Geschäftsbetriebes. Würde die WEG darüber hinaus eigenständig personenbezogene Daten verarbeiten, wäre sie für diesen Bereich als Verantwortlicher zu sehen.

Dies hat auch zur Folge, dass der Verwalter als Verantwortlicher die Vorgaben der DS-GVO und des BDSG beachten muss, also z.B. betroffene Personen informieren (Art. 13, 14 DS-GVO), Auskunft erteilen (Art. 15 DS-GVO) und für seine eigenen Verfahren ein entsprechendes Verzeichnis erstellen muss (Art. 35 DS-GVO). Dazu muss er von der WEG nicht beauftragt werden.

Muss mit der Hausverwaltung zwingend ein Vertrag zur Auftragsverarbeitung nach Art. 28 DS-GVO geschlossen werden?

Von obiger Einordnung ist auch abhängig, ob möglicherweise eine Auftragsverarbeitung durch die Hausverwaltung vorliegt und ob in diesem Rahmen dann ein entsprechender Vertrag zur Auftragsverarbeitung zwischen der WEG und der Hausverwaltung erforderlich ist. Auch zur dieser Frage wurde der LfDI im Jahr 2020, nicht zuletzt wegen des o.g. Urteils des AG Mannheim, verstärkt konsultiert.

Der LfDI ist mit der Datenschutzkonferenz nicht der Auffassung, dass die Verwaltung für WEG grundsätzlich eine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO darstellt. Die Hausverwaltung verarbeitet personenbezogene Daten in eigener Verantwortung. Sie ist mithin Verantwortlicher im Sinne der DS-GVO. Die WEG hat mit der Hauserwaltung einen Vertrag abgeschlossen, der die Hausverwaltung zum Gegenstand hat. Ob diese Vereinbarung nur eine Bestellung unter Bezugnahme auf § 27 Wohnungseigentumsgesetz beinhaltet oder darüber hinaus noch weitere Inhalte hat (z.B. die Vergütung des Verwalters), ist aus Sicht des LfDI für die datenschutzrechtliche Beurteilung unerheblich.

Die Verwaltung will ihre Pflichten aus dem Verwaltervertrag ordnungsgemäß erfüllen. Dazu muss sie personenbezogene Daten verarbeiten. Diese Datenverarbeitung ist über Art. 6 Abs. 1 Satz 1 Buchstabe b (Vertragserfüllung) oder Buchstabe f (berechtigtes Interesse) DS-GVO legitimiert. Zu diesem Zweck verarbeitet sie personenbezogene Daten von Eigentümern und Mietern in eigener Verantwortung. Sie ist damit Verantwortlicher innerhalb der Datenverarbeitung ihres Geschäftsbereichs. Die Verwaltung entscheidet überwiegend autark, welche Daten sie zur Erfüllung ihrer Aufgabe verarbeitet und wie sie dies tut. Ein Auftragsverarbeitungsverhältnis liegt daher nicht vor.

In einem internen Arbeitskreis der Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) wurde das Urteil des AG Mannheims vom 11. September 2019 bereits im Herbst 2019 thematisiert und einhellig besprochen, dass dieses nichts an der bisherigen Rechtsauffassung der DSK ändert.

5.2 Energieversorger Pools

Dürfen Wirtschaftsauskunfteien eine Datenbank mit Vertragsdaten von Strom- und Gaskunden anlegen, um etwa festzustellen, wie oft Kunden ihren Anbieter wechseln?

Der Markt der Strom- und Gasanbieter ist vielseitig und hart umkämpft. Wer regelmäßig die Konditionen der verschiedenen Anbieter vergleicht, seinen Vertrag kündigt und gegebenenfalls zu einem Konkurrenten wechselt, kann mitunter Geld sparen. Kunden können

so etwa von günstigeren Preisen oder besonderen Angeboten für Neukunden profitieren. Die Anbieter auf der anderen Seite haben jedoch ein Interesse daran, möglichst dauerhaft treue Kunden zu gewinnen. Kunden, die ihren Vertrag schnell wieder kündigen und den Anbieter wechseln, sind für die meisten Anbieter dagegen weniger interessant. Aus diesem Grunde haben diese ein Interesse daran, möglichst schon vor Vertragsabschluss in Erfahrung zu bringen, wie häufig der jeweilige potentielle Kunde seinen Energieanbieter wechselt.

An dieser Stelle kommen Wirtschaftsauskunfteien ins Spiel. Bisher begegneten Kunden solchen Auskunfteien überwiegend etwa beim Onlinehandel oder der Kreditvergabe im Rahmen von Bonitätsauskünften. In der Mitte des Jahres entzündeten sich Diskussionen um mutmaßliche Pläne von Auskunfteien, die den Strom- und Gaswechsel von Bürgerinnen und Bürgern erschweren könnten. Hintergrund der Diskussionen waren Berichte des NDR sowie der Süddeutschen Zeitung, wonach zwei große deutsche Auskunfteien eine Datenbank geplant haben sollen, in denen Vertragsdaten von Strom- und Gaskunden branchenweit gespeichert werden sollen. Während bisher solche Daten verarbeitet werden können, die etwa aufgrund von Zahlungsausfällen gemeldet werden (sog. Negativdaten), war durch die Auskunfteien nun im Bereich der Energieversorger auch die Verarbeitung von sog. Positivdaten geplant. Im Gegensatz zu Negativdaten, welche einen unmittelbaren Rückschluss auf vertragswidriges Verhalten der Kundinnen und Kunden zulassen, sind Positivdaten solche Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben. Hiervon umfasst sein können insbesondere Informationen hinsichtlich der Begründung, ordnungsgemäßen Durchführung und Beendigung sowie etwa Daten zur Laufzeit und über die Anzahl der (bisher) geschlossenen Verträge. Diese Daten hätten dann möglicherweise von den Energieversorgern abgefragt werden können. Auf diese Weise hätten diese dann unter Umständen die Möglichkeit gehabt, das Wechselverhalten von Kunden bereits vor Vertragsschluss zu prüfen, um auf diese entsprechend zu reagieren. So wäre es denkbar gewesen, dass die Strom- und Gasanbieter häufig wechselnden Kunden andere Konditionen anbieten oder diese sogar gänzlich ablehnen.

Datenschutzrechtlich zulässig ist etwa die Speicherung und Beauskunftung solcher Daten nur dann, soweit hierfür eine entsprechende Rechtsgrundlage gemäß Art. 5 Abs. 1 lit. a i.V.m. Art. 6 Abs. 1 DS-GVO vorliegt. Neben einer ausdrücklichen Einwilligung durch den Kunden (Art. 6 Abs. 1 lit. a DS-GVO) ist hier insbesondere die Datenverarbeitung aufgrund eines berechtigten Interesses (Art. 6 Abs. 1 lit. f DS-GVO) relevant. Eine solche setzt allerdings voraus, dass im Rahmen einer Abwägung die Interessen insbesondere der Anbieter an der Datenverarbeitung höher zu bewerten sind, als die Interessen der betroffenen Kundinnen und Kunden an deren Schutz ihrer personenbezogenen Daten. Dass hier der Datenschutz der Kundinnen und Kunden hinter den Interessen der Energieversorger zurückstehen muss, ist aus Sicht des LfDI jedoch zweifelhaft. Typischerweise erfolgt die Tätigkeit von Wirtschaftsauskunfteien zur Absicherung von Zahlungsausfällen, also vertragswidrigem Verhalten. Vorliegend könnte eine solche Datenbank jedoch dazu genutzt werden, solche Kundinnen und Kunden auszufiltern, welche sich völlig vertragsgemäß verhalten, indem sie von den ihnen gesetzlich zustehenden Kündigungsrechten Gebrauch machen. In diesem Falle würden die Anbieter lediglich das gewöhnliche wirtschaftliche Risiko der Wettbewerbssituation am Markt zu Lasten des Datenschutzes auf die betroffenen Personen abwälzen. Andererseits besteht die Gefahr, dass bestimmte Kundinnen und Kunden benachteiligt werden. Dass dieses Risiko der Energieversorger gegenüber

dem Datenschutz der betroffenen Personen besonders schutzwürdig ist, war jedoch nicht erkennbar.

Der LfDI sieht solche Datenbanken kritisch, da die Energieversorger hiermit lediglich ihr eigenes marktübliches wirtschaftliches Risiko zu Lasten des Datenschutzes auf die Kundinnen und Kunden verlagern würden. Diese Auffassung vertreten auch andere Datenschutzaufsichtsbehörden. Es bestehen erhebliche Zweifel an der Verarbeitung von Positivdaten wie Angaben zur Vertragsdauer durch Wirtschaftsauskunfteien im Bereich der Energieversorgungsbranche auf der Grundlage des Art. 6 Abs. 1 S. 1 lit. f Datenschutz-Grundverordnung.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat in einem Beschluss vom 15. März 2021 festgehalten, dass entsprechende Pläne nach Maßgabe von Artikel 6 Absatz 1 Satz 1 lit. f) Datenschutz-Grundverordnung (DS-GVO) rechtswidrig wären.

5.3 Gemeinsame Verantwortlichkeit von Werbenden und Adresshändler

Der LfDI hat sich im Jahr 2020 mit der der Frage der Verantwortlichkeit von Unternehmen, die Adressen mieten oder Werbung im Lettershop-Verfahren versenden lassen, beschäftigt. Bei diesen Werbemaßnahmen verfügt das werbende Unternehmen nicht selbst über die personenbezogenen Daten der Werbeadressaten, sondern greift auf Datenbestände eines Adresshändlers oder Lettershops zurück. Ein Adresshändler selektiert Datensätze mit Anschriften von natürlichen Personen nach gewissen Kriterien. An Hand dieser Kriterien wählt das werbende Unternehmen die jeweiligen Datensätze aus und mietet oder kauft sie vom Adresshändler. Bei einem Lettershop übernimmt dieser den kompletten Versand der Werbung. Das werbende Unternehmen liefert lediglich die Werbebotschaft und die Kriterien, die bestimmen, an welche Personen die Werbung versandt werden soll. Mit dem weiteren Ablauf der Werbemaßnahme hat das werbende Unternehmen dann nichts mehr zu tun.

Der LfDI nimmt in den beschriebenen Konstellationen eine gemeinsame Verantwortlichkeit zwischen werbenden Unternehmen und Adresshändler/Lettershop an. Hintergrund dieser Frage sind Beschwerden von Bürgerinnen und Bürger, die unverlangt Werbung von rheinland-pfälzischen Unternehmen erhielten. Als Reaktion darauf machten die betroffenen Personen ihren Anspruch auf Auskunft gegen das Unternehmen geltend, von dem die Werbung stammte, vor allem wenn sie mit diesem Unternehmen zuvor noch keinen Kontakt hatten. Oftmals konnten diese Unternehmen keine Auskunft geben, da ein Adresshändler oder Lettershop die Werbung für das Unternehmen versendet hat und das Unternehmen selbst gar nicht über die Daten der Werbungsempfänger verfügte. In vielen Fällen gab der Verantwortliche den Auskunftsantrag weder an den Adresshändler (sog. Listeneigner) weiter noch teilte er den betroffenen Personen die Kontaktdaten des Adresshändlers mit. Die betroffenen Personen wurden zumeist auf die Angaben in der Werbung verwiesen, die meistens nur sehr schwer erkennbare Informationen zum Adresshändler enthielt.

Da die werbenden Unternehmen in dieser Konstellation selbst keine personenbezogenen Daten verarbeiten, war die Frage nach ihrer datenschutzrechtlichen Verantwortlichkeit zu beantworten. Verantwortlicher im Sinne der DS-GVO ist nicht nur, wer personenbezogene Daten tatsächlich verarbeitet, sondern auch wer die Zwecke und Mittel der Verarbeitung festlegt. Der Zweck der Werbung für einen bestimmten Personenkreis wird durch das werbende Unternehmen (sog. Listenmieter)

und seine Zielgruppenauswahl maßgeblich bestimmt. Für die Einordnung der Verantwortlichkeit ist außerdem zu berücksichtigen, dass der Listenmieter zwar selbst keinen Zugriff auf die für die Werbung verwendeten personenbezogenen Daten erhält, die Verwendung der Daten mit seiner Werbeaktion allerdings veranlasst, von dieser hauptsächlich profitiert und gegenüber den betroffenen Personen als Ansprechpartner und Widerspruchsadressat auftritt. Der Listeneigner hingegen hat vollen Zugriff auf die Daten. Er verarbeitet diese nicht als Auftragsverarbeiter, da er für die beauftragte Werbeaktion „eigene" Daten mehrfach verwendet und je nach Kunde (Listenmieter) die Daten zusammenstellt und selektiert.

Der LfDI betrachtet den Adresslisteneigener und das werbende Unternehmen in der beschriebenen Konstellation daher als gemeinsam für die Verarbeitung Verantwortliche nach Art. 26 DS-GVO. Sie haben einen Vertrag im Sinne des Art. 26 Abs. 2 DS-GVO zu schließen und die betroffenen Personen können ihre Rechte bei und gegenüber jedem einzelnen der Verantwortlichen geltend machen. Diese Sichtweise wird der Rollenverteilung zwischen Werbendem und Adresshändler gerecht und sichert die Gewährleistung der Rechte der betroffenen Personen. Diese Art der Rollenverteilung ist inzwischen weit verbreitet, von der Direktpostwerbung über die Online-Werbung bis hin zur modernen Wahlwerbung. Würde in all diesen Konstellationen der Werbende aus der Verantwortung entlassen, weil er selbst die Daten nie verarbeitet, würde der Datenschutz weitgehend entwertet. Die betroffenen Personen würden dann voraussichtlich immer häufiger auf schwer greifbare Dritte (mitunter im nicht EU-Ausland, die nicht das EU-Datenschutzniveau einhalten) verwiesen werden, obwohl der Veranlasser der Verarbeitung vor Ort greifbar wäre. Verantwortliche aus der EU könnten sich so ganz von den Anforderungen der DS-GVO befreien, indem sie Dienstleistungen außereuropäisch buchen.

Die Zweckfestlegung wird durch die Adresslisteneigener und die Werbenden gemeinsam in mehreren Schritten vorgenommen. Die Adresslisteneigner sammeln und pflegen beständig personenbezogener Daten mit dem Ziel, diese werbenden Unternehmen als Infrastruktur anzubieten, wobei die Daten nicht offenbart werden, aber genutzt werden können. Durch die vom werbenden Unternehmen vorgenommene Auswahl der Inhalte der Werbung und ihren Zuschnitt auf Zielgruppen wird der spezifische Verarbeitungszweck festgelegt. Die Auswahl von Zielgruppen durch den Werbenden entspricht der vom EuGH im Fanpage-Urteil für die Begründung der gemeinsamen Verantwortung angeführten „Parametrierung". Auf die Auswahl der Mittel hat das werbende Unternehmen zwar nur einen generellen Einfluss, nämlich die Auswahl, die Infrastruktur eines bestimmten Anbieters zu wählen. Der Adresslisteneigener hat den maßgeblichen Einfluss auf die Auswahl der Mittel der Verarbeitung. Dies ist für die Annahme einer gemeinsamen Verarbeitung aber nicht entscheidend.

6. BESCHÄFTIGTENDATENSCHUTZ

6.1 Erhebung privater Kontaktdaten von Beschäftigten während der Corona-Pandemie

Aufgrund einiger Anfragen und einer Beschwerde musste sich meine Behörde mit der Frage auseinandersetzen, ob und wenn ja in welchem Umfang der Arbeitgeber/Dienstherr private Kontaktdaten von Beschäftigten erheben darf.

Öffentliche Arbeitgeber dürfen nach § 20 Abs. 1 Landesdatenschutzgesetz (LDSG) personenbezogene Daten von Beschäftigten erheben, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Beschäftigungsverhältnisses oder zur Durchführung innerdienstlicher, planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder in einer Rechtsvorschrift, einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung (Kollektivvereinbarung) vorgesehen ist.

Erforderlichkeit in diesem Sinne bedeutet, dass die Aufgabe ohne die Kenntnis der personenbezogenen Daten nicht, nicht rechtzeitig, nur mit unverhältnismäßigem Aufwand oder nur mit sonstigen unverhältnismäßigen Nachteilen erfüllt werden kann. Dabei ist das Organisationsermessen des Arbeitgebers mit den Persönlichkeitsrechten der Beschäftigten in einen Ausgleich zu bringen.

Die Datenerhebungsbefugnis korrespondiert mit einer entsprechenden Mitwirkungsverpflichtung des Beschäftigten. Sofern der Arbeitgeber personenbezogene Daten des Beschäftigten erheben darf, ist der Beschäftigte auch verpflichtet, diese Daten mitzuteilen. Im umgekehrten Fall steht dem Beschäftigten ein Weigerungsrecht zu.

Die datenschutzrechtliche Beurteilung hängt davon ab, welche – der Privatsphäre zuzurechnenden – Daten zu welchem Zweck vom Arbeitgeber erhoben werden sollen.

Szenario 1:

Der Arbeitgeber verlangt die Mitteilung der privaten E-Mail-Adresse

Sofern in einer Ausnahmesituation wie der Corona-Pandemie auf die ansonsten zur Verfügung stehenden dienstlichen Kommunikationsmittel nicht zurückgegriffen werden kann, weil sich nahezu sämtliche Beschäftigte aufgrund der Gefahrensituation auf Weisung des Arbeitgebers im Homeoffice befinden, ist es zur Durchführung des Arbeitsverhältnisses erforderlich, eine private E-Mail-Adresse der Beschäftigten in Erfahrung zu bringen. Denn ansonsten ist die Kommunikation innerhalb der Behörde schlechterdings nicht möglich, was die Funktionsfähigkeit des gesamten Behördenapparats in erheblichem Maße beeinträchtigt. Der damit verbundene Eingriff in die Persönlichkeitsrechte der Beschäftigten ist als gering anzusehen, da sich diese für diesen Zweck eine eigene E-Mail-Adresse zulegen können, so dass zumindest eine provisorische Trennung zwischen dienstlich und privat hergestellt werden kann. Hinzu kommt, dass die Kommunikation per Mail keine ständige Verfügbarkeit impliziert, wie dies bei der Sicherstellung einer telefonischen Erreichbarkeit der Fall wäre.

Szenario 2:

Der Arbeitgeber verlangt, Anrufe auf die private Festnetznummer/Handynummer umzuleiten

Grundsätzlich sollten dienstliche Telefonate auch über dienstliche Endgeräte (Diensthandy)

erfolgen. Wenn aber aus Ressourcengründen nicht sämtliche Beschäftigte mit Diensthandys ausgestattet werden können, kommt auch die Nutzung des privaten Telefonanschlusses im Rahmen des Homeoffices in Betracht. In der Regel wird bei Abschluss eines Mobilfunk-Vertrags ohnehin auch eine (ggf. auch mehrere) virtuelle Festnetznummern bereitgestellt, sodass eine Trennung zwischen „dienstlich" und „privat" auch hier zumindest provisorisch möglich ist. Soweit ein separater Anschluss zur Verfügung steht, sollte dieser für die Umleitung genutzt werden. Mitarbeiter sollten sich ggfs. bei ihrem Provider danach erkundigen. Sollte die Einrichtung eines zusätzlichen Anschlusses mit Kosten verbunden sein, müssten diese grundsätzlich vom Arbeitgeber übernommen werden.

Denkbar wäre es, dass eine manuelle Weiterleitung anhand einer Liste beispielsweise durch eine Telefonzentrale erfolgt. Entsprechende Regelungen können in einer Dienstvereinbarung zur Tele- bzw. Heimarbeit getroffen werden. Sofern die Beschäftigten ihre private Telefonnummer dabei selbst in die Telefonanlage eingeben oder auf einer Liste für zentrale Auskünfte eintragen, liegt zwar eine Speicherung durch den Arbeitgeber vor; diese (vorübergehende) Speicherung ist nach § 20 Abs. 1 LDSG zur Sicherstellung des Dienstbetriebs, wozu auch eine telefonische Erreichbarkeit der Beschäftigten im Innen- und Außenverhältnis gehört, erforderlich und daher datenschutzrechtlich vertretbar. Dies gilt erst recht in den Fällen, in denen Beschäftigte ihre privaten Telefonnummern in öffentlich zugänglichen Verzeichnissen veröffentlicht haben (z. B. Telefonbuch). Hinzukommt, dass der Zugriff auf die Telefonnummern durch Kollegen oder Vorgesetzte in einem nur sehr eingeschränkten Maße möglich ist und die Daten zudem einer engen Zweckbindung (vgl. § 20 Abs. 7; § 7 LDSG) unterliegen. In technischer Hinsicht sollte darauf geachtet werden, dass bei der Telefonanlage des Arbeitgebers die Rufnummerunterdrückung bei der Weiterleitung zu aktivieren ist. Soweit bei Rückrufen nicht ohnehin nur die Nummer des dienstlichen Anschlusses angezeigt wird, kann für den privaten Anschluss die Rufnummerunterdrückung durch den Beschäftigten selbst aktiviert werden.

Szenario 3:

Der Arbeitgeber verlangt die Angabe der privaten Handynummer

Unstreitig liegt hierin der am weitest gehende Eingriff in die Persönlichkeitsrechte der Beschäftigten. Nach dem LAG Thüringen (Urt. v. 16.05.2018, Az: 6 Sa 442/17) ist die Erhebung/Erfassung der privaten Mobiltelefonnummer eines Arbeitnehmers gegen seinen Willen nur dann ausnahmsweise zulässig, wenn der Arbeitgeber ohne Kenntnis der Mobiltelefonnummer im Einzelfall eine legitime Aufgabe, für die der Arbeitnehmer eingestellt ist, nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und ihm eine andere Organisation der Aufgabenerfüllung nicht möglich oder nicht zumutbar ist.

In der zugrundeliegenden Entscheidung ging es um einen kommunalen Arbeitgeber, der sein Gesundheitsamt so umorganisierte, das die Rufbereitschaft für Mitarbeiter des Infektionsschutzes/Hygiene abgeschafft wurde und die Mitarbeiter zur Sicherstellung ihrer Erreichbarkeit ihre private Handynummer angeben sollten. Das LAG sah in diesem Verlangen einen äußerst schwerwiegenden Eingriff des Arbeitgebers, da der Beschäftigte sodann auch in seiner Freizeit jederzeit für den Arbeitgeber verfügbar sei. Als mildere Maßnahme wurde im vorliegenden Fall die Angabe der Festnetznummer nicht in Erwägung gezogen; das LAG stützte eine Entscheidung aber maßgeblich auf den Umstand, dass der Arbeitgeber durch die Umorganisation zeitliche Lücken in der Erreichbarkeit selbst geschaffen habe, die er nicht durch einen Eingriff in die Persönlichkeitsrechte der Beschäftigten auflösen könne.

Bezogen auf die gegenwärtige Situation wird man auch angesichts der o. g. LAG-Entscheidung die Erhebung der privaten Handynummern datenschutzrechtlich akzeptieren können, wenn

- Sich dies auf einzelne Behördenmitarbeiter mit einer gewissen Schlüsselfunktion beschränkt (z.B. Systemadministrator, Hausmeister)

- Der Arbeitgeber ohne Kenntnis der Mobiltelefonnummer im Einzelfall eine legitime Aufgabe, für die der Arbeitnehmer eingestellt ist, nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann und ihm eine andere Organisation der Aufgabenerfüllung nicht möglich oder nicht zumutbar ist und insb. die Erhebung der Festnetznummer als mildere Maßnahme nicht zielführend ist

- In einer Dienstanweisung/Dienstvereinbarung Regelungen zu den Anlässen einer telefonischen Kontaktaufnahme, zur Zweckbindung, Zugriffsberechtigung und zur Löschung festgeschrieben werden.

Gegenstand einer Beschwerde war die Aufforderung eines Dienstherrn an die Beschäftigten, anlässlich der Corona-Krise ihre privaten Erreichbarkeit in Form einer Mobilfunk- oder Festnetznummer sowie einer E-Mail-Adresse der Behördenleitung mitzuteilen. Der Beschwerdeführer war den vorangegangenen diesbezüglichen allgemeinen Ersuchen nicht nachgekommen weshalb er darauf hingewiesen wurde, dass die Behördenleitung sich für den Fall der fortgesetzten Weigerung weitere Schritte vorbehalte.

In diesem Zusammenhang hat der Beschwerdeführer vorgetragen, dass er an fünf Tagen in der Woche in den Räumlichkeiten des Dienstherrn im Dienst sei und eine Telearbeit nicht vorgesehen sei.

Im vorliegenden Fall ging es insbesondere um die Erfüllung der Fürsorgepflichten des Dienstherrn hinsichtlich des Gesundheitsschutzes der Bediensteten bei weitgehender Aufrechterhaltung der Funktionsfähigkeit der Verwaltung. Zutreffend ging der Dienstherr davon aus, dass die Erhebung privater Erreichbarkeitsdaten seiner Beschäftigten auch für diejenigen als erforderlich anzusehen ist, welche täglich vor Ort zum Dienst erscheinen. Dies aus dem Grund, da es sich bei dem neuartigen Coronavirus um ein sich schnell verbreitendes Virus handelt, welches ein hohes Ansteckungspotential und insbesondere für Personen mit relevanten Vorerkrankungen ein nicht unerhebliches Risiko birgt.

Aus diesem Grunde war es gerade zu Beginn der Pandemie, als die Kontaktnachverfolgung durch das Gesundheitsamt noch nicht etabliert war, erforderlich, nach Kenntniserlangung einer Ansteckung innerhalb des Personalkörpers unverzüglich, also ohne schuldhaftes Zögern, zu handeln und all diejenigen, welche mit der infizierten Person in der kürzeren Vergangenheit Kontakt hatten über diesen Umstand in anonymer Form zu informieren. Aufgrund der Eilbedürftigkeit kann dies kann auch Zeiträume betreffen, welche nicht innerhalb der täglichen Arbeitszeit der Beschäftigten liegen.

Aus diesem Grund war es vorliegend vertretbar, die Beschäftigten zur Mitteilung mindestens einer privaten Erreichbarkeitsangabe aufzufordern. Der Privatsphäre der Beschäftigten wurde dadurch größtmögliche Rechnung getragen, dass ihnen selbst überlassen wurde, welche Form der Erreichbarkeit sie ihrem Dienstherrn mitteilen wollten. So war es beispielweise den Beschäftigten möglich, sich eine vorübergehende (private) E-Mail-Adresse anzulegen, welche allein zu internen dienstlichen Zwecken verwendet wurde.

6.2 Erfassung der Körpertemperatur von Beschäftigten im Rahmen der Corona-Bekämpfung

Vielerorts beabsichtigten Arbeitgeber bereits zu Beginn der Pandemie, bei Beschäftigten Messungen der Körpertemperatur vorzunehmen oder Fragebögen auszugeben, in denen betroffene Personen mitteilen sollten, ob sie in den letzten Wochen eine Reise in Risikogebiete unternommen hätten und Erkältungsanzeichen verspürten.

Bei den durch diese Vorgehensweisen generierten personenbezogenen Daten handelt es sich um Gesundheitsdaten. Diese sind „besondere Kategorien personenbezogener Daten" im Sinne des Art. 9 Abs. 1 DS-GVO und damit besonders schutzwürdig. Aus diesem Grunde sind die Anforderungen, die an die Rechtmäßigkeit der Verarbeitung solcher Daten gestellt werden, erhöht.

Im Beschäftigtendatenschutz muss sich ein Datenverarbeitungsvorgang im nicht-öffentlichen Bereich zunächst an § 26 Abs. 1 S. 1 BDSG und im öffentlichen Bereich an § 20 Abs. 1 S. 1 LDSG messen lassen. Handelt es sich jedoch wie vorliegend um besondere Kategorien personenbezogener Daten, sind die diese Verarbeitung explizit gestattende Rechtsgrundlagen zu beachten.

Im nicht-öffentlichen Bereich ist dies Art. 9 Abs. 2 lit. b DS-GVO i. V. m. § 26 Abs. 3 BDSG. Danach ist die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses unter anderem zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Im öffentlichen Bereich trifft § 20 Abs. 3 LDSG eine ähnliche landesrechtliche Regelung unter zusätzlicher Erwähnung der Erfüllung rechtlicher Pflichten aus dem Beamtenrecht, der Gesundheitsvorsorge und der Arbeitsmedizin.

In beiden Fällen sind solche rechtlichen Pflichten im konkreten Zusammenhang zuvörderst die Fürsorgepflicht des Arbeitgebers oder des Dienstherrn. Von der Erforderlichkeit einer Datenverarbeitung – in diesem Fall in Form der Erhebung – kann dann gesprochen werden, wenn die personenbezogenen Daten für die Aufgabenerfüllung der verantwortlichen Stelle unabdingbar sind. Dies ist wiederum der Fall, wenn die Aufgabe ohne die Kenntnis der Information nicht, nicht rechtzeitig, nur mit unverhältnismäßigem Aufwand oder nur mit sonstigen unverhältnismäßigen Nachteilen erfüllt werden kann.

In den Fällen, in denen der Arbeitgeber das Betreten der Räumlichkeiten des Unternehmens oder der Behörde durch die Beschäftigten davon abhängig machen wollte, dass diese zunächst ihre Körpertemperatur erfassen lassen, war von einer Erforderlichkeit nicht auszugehen.

Festzuhalten war, dass die reine Tatsache einer erhöhten Körpertemperatur noch nicht automatisch den Schluss auf das Vorliegen einer Corona-Erkrankung zuließ. Umgekehrt musste sich eine bereits bestehende Corona-Erkrankung nicht zwangsläufig durch eine erhöhte Körpertemperatur zu erkennen geben. Daher war bereits an der Geeignetheit der Körpertemperaturmessung zu zweifeln.

Dem Arbeitgeber oder Dienstherrn standen trotz der unklaren Lage bereits zu Beginn der Pandemie zahlreiche Möglichkeiten zur Verfügung, seiner Fürsorgepflicht nachzukommen, beispielsweise das Anbieten von Heimarbeit, sodass ein Betreten des Gebäudes durch Be-

schäftigte entbehrlich wurde. War die Präsenz der Beschäftigten am Arbeitsplatz erforderlich, war es vorzugswürdig, Hygienekonzepte zu erarbeiten und darauf hinzuweisen, dass bei Verspüren von grippalen Symptomen ein Arzt aufzusuchen sei, um den Gesundheitszustand abklären zu lassen.

Weiterhin konnte und kann der Besuch beim Amts- oder Betriebsarzt angeordnet werden, sofern begründete Zweifel an der Dienstfähigkeit bestehen. Davon konnte beispielsweise ausgegangen werden, wenn bekannt ist, dass sich der Beschäftigte zuvor in einer als gefährdetes Gebiet eingestuften Region aufgehalten hatte und somit Ansteckungsrisiken ausgesetzt war.

Eine detaillierte Befragung aller Beschäftigten in Form eines Fragebogens war und ist hierfür allerdings nicht erforderlich. Vorzugswürdig ist es, auf die seinerzeit als Gebiet mit erhöhter Ansteckungsgefahr qualifizierten Länder hinzuweisen und sodann die Beschäftigten aufzufordern mitzuteilen, falls sie sich kürzlich in einem dieser Gebiete aufgehalten haben. Die Angabe des konkreten Ziels oder die Dauer des Aufenthalts ist insoweit entbehrlich.

Sollte ein Beschäftigter nach einem Arztbesuch die Rückmeldung bekommen, dass sie oder er sich mit dem Corona-Virus infiziert hat, greifen die gewöhnlichen Regeln bei Erkrankung, nämlich die Vorlage einer Arbeitsunfähigkeitsbescheinigung. Auch wenn die Aufgabe der Kontaktnachverfolgung dem Gesundheitsamt zugewiesen ist, kann es jedoch zur Vermeidung wahrscheinlich eintretender Verzögerungen oder bei Kenntnis darüber, dass sich unter den Beschäftigten Personen befinden, welche einer Risikogruppe angehören, erforderlich sein, herauszufinden, mit welchen Personen der Beschäftigte innerhalb des Unternehmens oder der Behörde Kontakt hatte. Am datensparsamsten ist es dabei, den betroffenen Beschäftigten selbst um die Vorlage einer Liste von Kolleginnen und Kollegen zu bitten und diese gezielt anzusprechen und auf den Risikokontakt hinzuweisen, ohne die betreffende Person dabei namentlich zu benennen. Eine unternehmens- oder behördenweite namentliche Benennung der oder des erkrankten Beschäftigten erübrigt sich so.

Zuletzt muss in jedem Fall eine Abwägung vorgenommen und beurteilt werden, ob Grund zur Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. In Anbetracht der Tatsache, dass die Coronavirus-Erkrankung mittlerweile als Pandemie eingestuft wurde, dürften Interessen des Gemeinwohls die Datenverarbeitung im Einzelfall überwiegen. Allerdings kommen auch im Pandemiefall stets die Grundsätze der Datenverarbeitung vollumfänglich zu Geltung, was auch bedeutet, dass im Sinne des Prinzips der Datensparsamkeit nur so viele Daten wie nötig erhoben werden dürfen und diese im Sinne der Speicherbegrenzung nur so lange gespeichert werden, wie sie zur Aufgabenerfüllung erforderlich sind. Ein denkbarer Zeitpunkt ist das Ende etwaiger Quarantänemaßnahmen.

Das Einholen einer Einwilligungserklärung der Beschäftigten zur Legitimierung von Datenverarbeitungsvorgängen, die weiter gehen, als die oben genannten, ist nicht zulässig, da die dafür erforderliche Freiwilligkeit, also das Vorhandensein einer echten Wahlmöglichkeit, fehlt. Der Beschäftigte befindet sich in einem wirtschaftlichen Abhängigkeitsverhältnis zum Arbeitgeber oder Dienstherrn. Wird die Erlaubnis, Arbeitsleistung zu erbringen, davon abhängig gemacht, dass weitergehende personenbezogene (Gesundheits-)Daten preisgegeben werden, muss sie oder er befürchten, dass dies zu finanziellen Nachteilen in Form von unbezahlter Freistellung vom Dienst führen kann.

6.3 Abfrage des Impfstatus von Beschäftigten

Seitdem die Möglichkeit, sich gegen das neuartige Corona-Virus impfen zu lassen, immer mehr Personen eröffnet ist, treten vermehrt Dienstherren und Arbeitgeber an meine Behörde heran, um in Erfahrung zu bringen, ob sie zulässigerweise den Impfstatus der bei ihnen Beschäftigten erfragen dürfen.

Bei der Abfrage des Impfstatus von Beschäftigten durch den Arbeitgeber oder den Dienstherrn handelt es sich um eine Erhebung besonderer Kategorien personenbezogener Beschäftigtendaten in Form von Gesundheitsdaten. Dies kann zulässigerweise nur dann erfolgen, wenn hierfür ein gesetzlicher Erlaubnistatbestand existiert.

Ein solcher Erlaubnistatbestand ist in § 23a Infektionsschutzgesetz (IfSG) zu sehen. Danach darf der Arbeitgeber, soweit es zur Erfüllung von Verpflichtungen aus § 23 Abs. 3 IfSG in Bezug auf übertragbare Krankheiten erforderlich ist, personenbezogene Daten eines Beschäftigten über dessen Impf- und Serostatus verarbeiten, um über die Begründung eines Beschäftigungsverhältnisses oder über die Art und Weise einer Beschäftigung zu entscheiden. § 23 Abs. 3 IfSG bezieht sich jedoch nur auf die Leitungen der dort aufgeführten medizinischen Einrichtungen, wie beispielsweise Krankenhäuser oder Pflegeeinrichtungen, weshalb die Erlaubnis zur Impfstatuserhebung nur für die in diesen Einrichtungen Beschäftigten herangezogen werden kann.

Für alle übrigen Beschäftigten richtet sich die Zulässigkeit dieser Vorgehensweise nach Art. 9 Abs. 2 lit. b Datenschutz-Grundverordnung (DS-GVO) i. v. m. § 26 Abs. 3 Bundesdatenschutzgesetz (BDSG) beziehungsweise im öffentlichen Bereich nach § 20 Abs. Abs. 3 Landesdatenschutzgesetz (LDSG). Danach ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DS-GVO für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht (oder dem Beamtenrecht), dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Die landesrechtliche Regelung ergänzt diese Aufzählung noch um die Erfüllung der Pflichten der Gesundheitsvorsorge oder der Arbeitsmedizin.

Von einer Erforderlichkeit kann nur dann ausgegangen werden, wenn die personenbezogenen Daten für die Aufgabenerfüllung der verantwortlichen Stelle unabdingbar sind. Dies ist wiederum der Fall, wenn die Aufgabe ohne die Kenntnis der Information nicht, nicht rechtzeitig, nur mit unverhältnismäßigem Aufwand oder nur mit sonstigen unverhältnismäßigen Nachteilen erfüllt werden kann.

Um im vorliegenden Fall eine Erforderlichkeit bejahen zu können, dürfte der Arbeitgeber bzw. Dienstherr also ohne die Information über den Impfstatus schlechterdings nicht in der Lage sein, seinen Betrieb zu organisieren oder seinen Verpflichtungen als Arbeitsgeber nachzukommen. Zur Beurteilung, ob dies der Fall ist, sind die Wertungen der im Zusammenhang mit der Corona-Pandemie erlassenen Regelungen auf Bundes- und Landesebene heranzuziehen.

Dabei ist zunächst festzuhalten, dass weder in der derzeit geltenden 21. Corona-Bekämpfungsverordnung Rheinland-Pfalz (21. CoBeLVO) noch in der SARS-CoV2-Arbeitsschutzverordnung (Corona-ArbSchV) des Bundes Impfungen als Teil des Hygienekonzepts vorgesehen sind. Auch ist festzuhalten, dass die aktuelle Rechtslage mit Blick auf den Eingriff in die Grundrechte der einzelnen Person

aktuell keine Impfpflicht zum Schutze vor der COVID-19-Erkrankung vorsieht. Während dies für die oben genannten Personengruppen, deren Impfstatus zulässigerweise abgefragt werden darf, dazu führen könnte, dass gewisse berufsbezogene Tätigkeiten aufgrund dieser Tatsache nicht mehr durchgeführt werden können, erwachsen Beschäftigten in übrigen Berufszweigen hier keine Einschränkungen.

Dies wird bereits daran deutlich, dass die gängigen Hygieneregelungen, wie das Tragen einer medizinischen Maske und das Abstandhalten, nach wie vor und trotz möglicherweise vorhandenem Impfschutz einzuhalten sind. So regelt auch § 3 Corona-ArbSchV ausdrücklich, dass der Arbeitgeber auf der Grundlage einer Gefährdungsbeurteilung und unter Berücksichtigung der SARS-CoV-2-Arbeitsschutzregel in einem Hygienekonzept die erforderlichen Maßnahmen zum betrieblichen Infektionsschutz festzulegen und umzusetzen hat. Dies kann sich allerdings nur auf die ohnehin gesetzlich angeordneten Regelungen erstrecken. Würde der Arbeitgeber die Abfrage des Impfstatus – und sei es auch nur durch freiwillige Angabe der Beschäftigten – als Teil des Hygienekonzepts vorsehen, könnte dies aufgrund des dadurch für die Beschäftigten entstehenden sozialen Drucks und die Angst vor Repressalien dazu führen, dass ein indirekter Impfzwang entsteht. Aus diesem Grunde kann auch eine Einwilligung von Beschäftigten nicht als Grundlage für eine solche Datenerhebung herangezogen werden, da sie aufgrund der angesichts des wirtschaftlichen Abhängigkeitsverhältnisses mangelnden echten Wahlmöglichkeit der Beschäftigten nicht freiwillig zustande kommen kann.

Der Gesamtschau der gesetzlichen Regelungen ist zu entnehmen, dass der Gesetzgeber der Ansicht ist, dass sich ein ausreichendes Hygienemanagement und eine zuverlässige Betriebsplanung auch ohne die Kenntnis des Impfstatus von Beschäftigten bewerkstelligen lässt und der Arbeitgeber so seinen Fürsorge- und Schutzpflichten aus § 613 BGB hinreichend nachkommen kann. Ob und inwieweit die Fürsorgepflicht des Arbeitgebers Schutzpflichten zur Gestaltung der Arbeitsorganisation beinhaltet, kann nur vor dem Hintergrund der Wertungen des Gesetzgebers konkretisiert werden. Die Abfrage des Impfstatus von Beschäftigten außerhalb der in § 23 Abs. 3 IfSG genannten Bereiche ist daher grundsätzlich unzulässig.

Ausnahmen können dort gelten, wo aufgrund der geltenden Corona-Vorschriften der Zugang zu gewissen Einrichtungen nur unter Vorlage eines negativen Testergebnisses gewährt wird. Dies ist derzeit im schulischen Bereich der Fall. Ausweislich § 28b Abs. 3 IfSG ist die Teilnahme am Präsenzunterricht nur zulässig für Schülerinnen und Schüler sowie für Lehrkräfte, die zweimal in der Woche mittels eines anerkannten Tests auf eine Infektion mit dem Coronavirus SARS-CoV-2 getestet werden.

Gemäß der auf Grundlage des § 28c IfSG erlassenen Schutzmaßnahmen-Ausnahmeverordnung besteht nunmehr die Möglichkeit, im Falle des Nachweises eines vollständigen Impfschutzes von der verpflichtenden Teilnahme an der Testung befreit zu werden. In diesem Zusammenhang bestehen hinsichtlich der Abfrage des Impfstatus durch den Dienstherrn keine datenschutzrechtlichen Bedenken, da die Mitteilung durch die Beschäftigten in diesem Falle aufgrund der bestehenden Wahlmöglichkeit, ob sie statt der Offenbarung ihres Impfstatus weiterhin an verpflichtenden Testungen teilnehmen möchten, freiwillig erfolgt.

Sollten sich die Beschäftigten für die Mitteilung des Impfstatus entschließen, ist zu beachten, dass lediglich ein Vermerk über die Inaugenscheinnahme des Impfnachweises und den bestehenden Impfschutz in die Personalakte aufzunehmen ist und keinesfalls eine Kopie des Impfpasses.

Für andere Berufszweige gilt in Bezug auf Corona-Schnelltests, dass Arbeitgeber und Dienstherrn gemäß § 5 Abs. 1 Corona-ArbSchV zur Minderung des betrieblichen SARS-CoV-2-Infektionsrisikos Beschäftigten, soweit diese nicht ausschließlich in ihrer Wohnung arbeiten, mindestens zweimal pro Kalenderwoche einen Test in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 anzubieten haben. Eine Verpflichtung für Beschäftigte, dieses Angebot anzunehmen oder zur Teilnahme an Schnelltest vor Betreten der Tätigkeitsstätte ist derzeit nicht vorgesehen, sondern lediglich empfohlen. Daher gilt hier in Anlehnung an das oben Gesagte, dass eine Erhebung von Testergebnissen durch den Arbeitgeber oder Dienstherrn unzulässig ist.

Darüber hinaus gibt es auch keine Rechtsgrundlage, die es Kunden eines Unternehmens erlaubt, von Mitarbeitern dieses Unternehmens ein negatives Testzertifikat oder Mitteilungen über den Impfstatus zu verlangen, solange es sich nicht um Dienstleister im Sinne des § 23 Abs. 3 IfSG handelt. Seinen (vor)vertraglichen Verpflichtungen gegenüber Kunden, Besuchern oder schutzbedürftigen Beschäftigten muss der Dienstherr/Arbeitgeber ohnehin im Wege der oben genannten Hygienemaßnahmen nachkommen, und bezüglich einer möglicherweise bestehenden Einwilligung gilt das oben Gesagte. Eine Übermittlung von Daten aus Testzertifikaten von Beschäftigten an Kunden kann somit weder durch eine Rechtsgrundlage, noch aufgrund einer Einwilligung der Beschäftigten legitimiert werden und ist somit generell unzulässig.

7. MEDIEN

7.1 Cookies, Plugins und vieles mehr: Tracking im Internet

Die Überprüfung der Datenschutzkonformität von Webseiten im Hinblick auf den Einsatz von Cookies und anderen Trackingmechanismen stellt weiterhin einen Schwerpunkt des Medienatenschutzes beim LfDI dar. Die aufsichtsbehördlichen Aktivitäten des LfDI in diesem Bereich wurden im Berichtszeitraum sowohl durch eingehende Beschwerden und Hinweise initiiert als auch proaktiv. Im Jahr 2020 haben sich in diesem Bereich außerdem insbesondere durch eine Entscheidung des Bundesgerichtshofs sowohl rechtlich als auch tatsächlich neue Entwicklungen ergeben.

Zur Rechtslage: Orientierungshilfe der DSK und Entscheidungen des EuGH und des BGH zu „Planet49“

Das Speichern von Cookies auf dem Endgerät eines Nutzers oder einer Nutzerin und das Auslesen gespeicherter Cookies ist gemäß Art. 5 Abs. 3 Satz 1 der Richtlinie 2002/58 EU (ePrivacy-Richtlinie) nur mit ausdrücklicher Einwilligung der Nutzer und Nutzerinnen zulässig. Dies hatte der Europäische Gerichtshof (EuGH) im Urteil vom 1.10.2019 zur Rechtssache C-673/17 „Planet49“ klargestellt. Eine Ausnahme gilt gemäß Art. 5 Abs. 3 Satz 2 nur für solche Cookies, die für die Bereitstellung der Webseite oder der App, die der Nutzer oder die Nutzerin aufrufen möchte, unbedingt erforderlich sind.

Art. 5 Abs. 3 der ePrivacy-Richtlinie ist in Deutschland nicht richtig umgesetzt worden. § 15 Abs. 3 Telemediengesetz (TMG) enthält dem Wortlaut nach gerade keine Pflicht zur ausdrücklichen Einwilligung für Cookies, die nicht für die Bereitstellung der Webseite oder App erforderlich sind. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ging auch davon aus, dass § 15 Abs. 3 TMG nicht richtlinienkonform ausgelegt werden kann, da eine Auslegung anhand von Art. 5 Abs. 3 der ePrivacy-Richtlinie dem Wortlaut von § 15 Abs. 3 TMG vollkommen widerspricht. Daher sah die DSK § 15 Abs. 3 TMG für unanwendbar und stattdessen ausschließlich die DS-GVO für anwendbar an. Die DSK hatte bereits im März 2019 eine Orientierungshilfe für Anbieter von Telemedien veröffentlicht, die erklärt, in welchen Fällen eine Einwilligung notwendig ist und wie sie wirksam eingeholt werden kann.

Die Orientierungshilfe unterscheidet zwischen technisch notwendigen Cookies und anderen Cookies. Technisch notwendige Cookies können zum Beispiel Cookies sein, die dafür sorgen, dass bei einem Online-Shop der Warenkorb dem Nutzer oder der Nutzerin zugeordnet bleibt. Auch kann mit Hilfe von Cookies etwa die Spracheinstellung eines Nutzers oder einer Nutzerin oder die Einwilligung in den Einsatz anderer Cookies festgehalten werden. Technisch notwendige Cookies können von öffentlichen Stellen gemäß Art. 6 Abs. 1 lit. e und für nicht öffentliche Stellen gemäß Art. 6 lit. f DS-GVO verarbeitet werden. Hierfür müssen die Nutzer und Nutzerinnen nicht um ihre ausdrückliche Erlaubnis gefragt werden.

Für den Einsatz von Cookies, die zur Bereitstellung einer Webseite oder App nicht unbedingt erforderlich sind, wäre nach Art. 5 Abs. 3 der ePrivacy-Richtlinie generell eine Einwilligung notwendig. Im Rahmen der Anwendung von Art. 6 Abs. 1 lit. f DS-GVO gemäß der o.g. Orientierungshilfe ist dies zumindest dann der Fall, wenn die Cookies einem Dritten den Zugriff auf die Cookie-Informationen erlauben, der eigene Zwecke mit der Verarbeitung der Daten verfolgt.

Dies ist zum Beispiel für das weit verbreitete Werkzeug „Google Analytics“ der Fall. Google Analytics und vergleichbare Dienste, die ein webseitenübergreifendes Tracking der Nutzer und Nutzerinnen ermöglichen, dürfen auf Webseiten und in Apps generell nur mit deren Einwilligung aktiviert werden. Anders kann das Ergebnis nach der Orientierungshilfe der DSK zum Beispiel dann ausfallen, wenn der Dritte die Nutzerdaten als Auftragsverarbeiter des Webseitenbetreibers nur für dessen Zwecke verarbeitet und diese Zwecke nicht gegen die Rechte und Freiheiten der Nutzer und Nutzerinnen verstoßen.

Mit Urteil vom 28.5.2020 hat nun der Bundesgerichtshof (BGH) anhand des o.g. Urteils des EuGH im Fall Planet49 letztinstanzlich entschieden. Der BGH hat sich dafür entschieden, § 15 Abs. 3 TMG richtlinienkonform auszulegen und das Einwilligungserfordernis in Art. 5 Abs. 3 ePrivacy-RL hineinzulesen. Damit kam der BGH auf einem anderen Weg zum selben Ergebnis wie die DSK: Für Cookies, die nicht zur Bereitstellung der Webseite oder App erforderlich sind, ist in jedem Fall eine aktive Einwilligung der Webseitenbesucher und -besucherinnen erforderlich. Der BGH ist an dieser Stelle sogar strenger als die Aufsichtsbehörden, die bisher nicht vollständig ausgeschlossen hatten, dass in bestimmten Fällen auch andere als technisch notwendige Cookies nach Art. 6 Abs. 1 lit. f DSGVO verarbeitet werden könnten. § 15 Abs. 3 TMG ist außerdem auf private und öffentliche Stellen gleichermaßen anwendbar.

Entwicklung auf Webseiten

Viele Webseitenbetreiber in Rheinland-Pfalz haben in Reaktion auf das Urteil des BGH und die Prüftätigkeiten des LfDI ihre Webseiten überarbeitet. Teilweise wurden eingebundene Dienste, für die eine Einwilligung der Nutzer und Nutzerinnen notwendig wäre, deinstalliert. Auf den meisten Webseiten wurden aber neue interaktive Banner installiert, die Einwilligungen der Webseitennutzer und -nutzerinnen einholen sollen.

Viele dieser Banner erfüllen jedoch die Anforderungen an eine wirksame Einwilligung nicht. Die Prüftätigkeit des LfDI verlagerte sich daher auf die Frage, ob mit dem Banner einer konkreten Webseite wirksame Einwilligungen von den Webseitennutzern und -nutzerinnen eingeholt werden können. Viele Webseitenbetreiber gestalten ihre Banner gezielt derart, dass zwar eine Möglichkeit besteht, Cookies und andere Trackingmechanismen abzulehnen, diese Möglichkeit jedoch viel schwieriger aufzufinden oder durchzuführen ist als das Akzeptieren des Trackings.

Dies hat auch dazu geführt, dass beim LfDI zahlreiche Beschwerden eingingen, die darauf hinwiesen, Internetseiten seien „nun“ nur noch mit Tracking nutzbar. Der LfDI beriet diese Bürgerinnen und Bürger dahingehend, dass zuvor regelmäßig Tracking ohne ihr Einverständnis und ohne ihr Wissen stattgefunden habe und sie nun die Möglichkeit zur Entscheidung hätten, dass aber die Einwilligungsbanner häufig unfair gestaltet seien. Gegen eindeutig unrechtmäßige Einwilligungsbanner geht der LfDI bereits vor soweit er darauf aufmerksam gemacht wird. In solchen Fällen können mit den Bannern keine wirksamen Einwilligungen eingeholt werden. Außerdem erarbeitet der LfDI gemeinsam mit anderen deutschen Datenschutzaufsichtsbehörden einheitliche Maßstäbe dafür, welche Gestaltungsformen von Einwilligungsbannern für Nutzer und Nutzerinnen verständlich und bedienbar sind und daher zu einer wirksamen Einwilligung führen können und welche nicht. Diese Maßstäbe werden in der Zukunft auch durchgesetzt werden. Es ist hierbei zu erwarten, dass zahlreiche Webseitenbetreiber ihre Einwilligungsbanner erneut anpassen müssen.

Schließlich ist stets zu überprüfen, ob die Entscheidungen, die die Nutzer und Nutzerinnen mittels Einwilligungsbanner treffen auch tatsächlich technisch umgesetzt werden. Auch

diesbezüglich überprüft der LfDI konkrete Webseiten weiterhin hauptsächlich aufgrund von Beschwerden oder Hinweisen.

Webseitenprüfung bei Zeitungsverlagen

Gemeinsam mit elf weiteren Landesdatenschutzbehörden führt der LfDI seit 2020 eine proaktive Überprüfung der Webseiten von Presseverlagen im Hinblick auf die oben dargestellte Rechtslage zu Cookies und Tracking durch. Hierbei wurden standardisierte Fragebögen entwickelt, die im Sommer 2020 an jeweils ausgewählte Presseverlage in den einzelnen Bundesländern gesandt wurden. Die Fragebögen wurden in Rheinland-Pfalz von allen ausgewählten Verlagen beantwortet. Die Auswertung der Antworten läuft derzeit noch. Überdies erarbeiten die in der Prüfung gemeinsam aktiven Aufsichtsbehörden einheitliche Kriterien für die Bewertung der Antworten und der Implementierung auf den Webseiten. Ausgangspunkt dieser Kriterien sind die bereits vorhandenen Materialen, die auf Ebene des Europäischen Datenschutzausschusses abgestimmt wurden, sowie die Orientierungshilfe der DSK.

7.2 Liken, twittern, streamen: Öffentliche Stellen auf Facebook, Twitter, YouTube und anderen Social Media-Plattformen

Soziale Netzwerke wie Facebook, Twitter, Instagram oder YouTube sind zu einem wesentlichen Bestandteil im beruflichen und privaten Informations- und Kommunikationsverhalten vieler Nutzerinnen und Nutzer geworden. Für öffentliche Stellen bilden sie relevante Kommunikationskanäle. Durch das Betreiben von Auftritten in Sozialen Netzwerken tragen öffentliche Stellen aber auch dazu bei, dass personenbezogene Daten der Nutzerinnen und Nutzer ihrer Angebote an die jeweiligen Plattformbetreiber gelangen, die sie häufig (auch) zu eigenen, von der Nutzung unabhängigen Zwecken weiter verarbeiten.

Seit dem Aufkommen von Social Media-Angeboten haben sich aus Sicht des Datenschutzes grundlegende Fragen gestellt. Dies hat z.B. mit deren Konzeption als Plattformlösung zu tun, mit deren Geschäftsmodell, das auf einer kommerziellen Verwertung von Nutzungsdaten basiert, aber auch mit der Tatsache, dass die technischen Anbieter/Betreiber der Plattformen ihren Sitz zumeist außerhalb der Europäischen Union haben, wo ein vergleichbares Datenschutzniveau häufig nicht gegeben ist. So war lange Zeit umstritten, welche Verantwortung z.B. öffentliche Stellen haben, die auf der Facebook-Plattform eine sogenannte Fanpage betreiben und dadurch den Anlass für die Verarbeitung entsprechender Nutzungsdaten setzen.

Diesen Streit hat der Europäische Gerichtshof (EuGH) in seiner Entscheidung vom 5. Juni 2018 zum Betrieb von Facebook-Fanpages entschieden und festgestellt, dass nicht nur Facebook selbst, sondern auch der jeweilige Betreiber einer Fanpage datenschutzrechtlich verantwortlich ist, soweit durch den Besuch der Fanpage personenbezogene Daten der Fanpage-Besucher verarbeitet werden. Öffentliche Stellen, die eine Facebook-Fanpage betreiben, sind daher selbst als datenschutzrechtlich (Mit-)Verantwortliche zu sehen. Die Fanpage-Betreiber benötigen deshalb eine Rechtsgrundlage für die Verarbeitung der Nutzungsdaten und müssen auch alle weiteren Pflichten als Verantwortliche erfüllen.

Mit Urteil vom 11. September 2019 stellte das Bundesverwaltungsgericht (BVerwG) ergänzend klar, dass die Datenschutzaufsichtsbehörden gegen die Betreiber von Facebook-Fanpages selbst vorgehen können, wenn bei dem Betrieb von Facebook-Fanpages Datenschutzverstöße begangen werden.

Diese zwei Entscheidungen hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI) zum Anlass genommen, den Handlungsrahmen für die Nutzung von „Social Media“ durch öffentliche Stellen aus dem Jahr 2016 zu überarbeiten und Anfang März 2020 an die neuen Gegebenheiten anzupassen. Dieser steht allen Verantwortlichen auf der Internetseite des LfDI zur Verfügung (**https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Handlungsrahmen_Soziale_Medien_20200306.pdf**).

Voraussetzungen und Handlungsvorgaben für die rechtskonforme Anwendung von Social Media-Angeboten

Aus Sicht des LfDI haben öffentliche Stellen beim Betrieb von Social Media-Angeboten folgende Punkte zu berücksichtigen:

Rechtsgrundlage für den Betrieb eines Social Media-Angebots

Jeder Verantwortliche benötigt für die Verarbeitungstätigkeiten, die seiner Verantwortung unterliegen, eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO. Dies gilt auch in den Fällen, in denen er die Verarbeitungstätigkeiten nicht unmittelbar selbst durchführt, sondern durch andere gemeinsam mit ihm Verantwortliche durchführen lässt.

Abschluss einer Vereinbarung über die gemeinsame Verantwortlichkeit

Öffentliche Stellen müssen für einen datenschutzgerechten Betrieb von Social Media-Angeboten eine Vereinbarung zur gemeinsamen Verantwortlichkeit mit dem Plattformbetreiber des Sozialen Netzwerkes schließen, die den Anforderungen von Art. 26 DS-GVO entspricht.

Informationspflichten nachkommen

Wie bei allen Datenverarbeitungsvorgängen trifft die Pflicht zur Information nach Art. 13 bzw. 14 DS-GVO auch öffentliche Stellen im Hinblick auf ihre Social Media-Angebote, sodass entsprechende Datenschutzinformationen in Form einer Datenschutzerklärung im Social Media-Angebot vorzuhalten sind.

Konzept für das Social Media-Angebot

In einem Konzept für das Social Media-Angebot muss der Verantwortliche darlegen, welche fundierten Erwägungen die Entscheidung für das gewählte Social Media-Angebot begründen. Dabei muss erkennbar sein, warum ein Verzicht zu einer ernsthaften Beeinträchtigung der Aufgabenerfüllung führen würde.

Impressumspflicht

Das Social Media-Angebot muss Angaben gemäß § 5 Telemediengesetz enthalten, welche die jeweilige Stelle als Anbieter erkennen lassen. Diese Angaben müssen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sein.

Keine konkreten Verwaltungsleistungen

Für die Bereitstellung und den Bezug von konkreten Verwaltungsleistungen ist auf Social Media-Dienste zu verzichten, wenn dabei sensible Bereiche oder besondere personenbezogene Daten (Art. 9 Abs. 1 DS-GVO) betroffen sind.

Alternativer Weg zur Informationsbeschaffung

Die bloße Kenntnisnahme von Informationen der öffentlichen Stelle darf nicht von einer vorherigen Registrierung auf einer Social Media-Plattform abhängig sein. Außer auf dem Social Media-Angebot müssen die bereitgestellten Informationen daher immer auch auf einem alternativen Weg verfügbar sein (z.B. Webseite der Verwaltung).

Alternative Kommunikationsmöglichkeiten

Die Nutzung interaktiver Funktionen (z.B. Kommentieren, Teilen, Bewerten) geht über ein reines Informationsangebot hinaus und steht weitgehend in der Verantwortung der Nutzerinnen und Nutzer. Soweit die Funktionen darauf ausgerichtet sind, in einen intensivierten Dialog mit der öffentlichen Stelle zu treten, ist immer auch eine alternative Kommunikationsmöglichkeit außerhalb der Social Media-Plattform anzubieten (z.B. E-Mail).

Rechenschaftspflicht und technisch-organisatorischer Datenschutz

Öffentliche Stellen, die Social Media-Angebote betreiben, müssen alle Pflichten eines Verantwortlichen nach der Datenschutz-Grundverordnung erfüllen.

Was droht bei einem datenschutzwidrigen Betrieb von Social Media-Angeboten?

Werden die im Handlungsrahmen aufgeführten Vorgaben zum datenschutzgerechten Betrieb eines Social Media-Angebots nicht befolgt, kann der LfDI nach Art. 58 Abs. 2 lit. f DS-GVO in Ausübung seines pflichtgemäßen Ermessens die Außerbetriebnahme des Angebots anordnen. Dies bestätigt das BVerwG in seinem o.g. Urteil. Zusätzlich kann eine Beanstandung oder Verwarnung erfolgen.

Daneben können betroffene Personen gegenüber dem Betreiber einer Fanpage nach Art. 82 DS-GVO Schadensersatz fordern. Nach Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen. Ist mehr als ein Verantwortlicher an derselben Verarbeitung beteiligt und sind sie für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist (vgl. Art. 82 Abs. 4 DS-GVO). Dies bedeutet, dass betroffene Personen im Rahmen von zivilgerichtlichen Verfahren Schadensersatz von den Betreibern von Fanpages verlangen können, wenn die betroffene Person einen materiellen oder immateriellen Schaden darlegen kann. Die betroffenen Personen können hinsichtlich einer Kompensation nicht an die Betreiber der Sozialen Netzwerke verwiesen werden.

8. GESUNDHEIT

8.1 Die Digitalisierung des Gesundheitswesens geht weiter

Das Gesundheitswesen in Deutschland befindet sich weiterhin in einem fundamentalen Umbruch. Die Digitalisierung hat mit der Corona-Pandemie zusätzlich zu den zahlreichen gesetzgeberischen Aktivitäten auf Bundesebene deutlich an Fahrt aufgenommen. Denn schneller als erwartet zogen Videosprechstunden und telemedizinische Verfahren in den Versorgungsalltag ein. Seit Anfang 2021 ist nun auch die elektronische Patientenakte zumindest in eingeschränkter Form Realität geworden.

Aus der Perspektive des Datenschutzes ist die Entwicklung hin zu einer digitalen Gesundheitsversorgung natürlich folgerichtig und zeitgemäß; der effektive Schutz der Patientendaten und die in diesem Zusammenhang zu gewährleistende Sicherheit der digitalen Anwendungen müssen dabei jedoch ein zentrales Anliegen sein. Erforderlich sind weiterhin die frühzeitige Berücksichtigung datenschutzrechtlicher Belange bei der Gesetzgebung und die Umsetzung der Vorgaben zu Datenschutz und Datensicherheit in der Versorgungspraxis. Hilfreich ist dabei das Verständnis, dass die grundlegenden Prinzipien des Datenschutzes im Wesentlichen den Anforderungen an eine erfolgreiche Heilbehandlung entsprechen, unabhängig davon, ob man sich im digitalisierten oder papiergebunden Gesundheitswesen bewegt: Informationelle Selbstbestimmung und Patientenautonomie, Vertraulichkeit und Schweigepflicht, Datensicherheit und Medizinsicherheit, Transparenz und Aufklärung sowie die bestehenden Rechte der Betroffenen bzw. Patientinnen und Patienten sind zwei Seiten des gleichen Anliegens. In der zunehmenden Komplexität des digitalen Praxisalltags kann dies nur gelingen, wenn durch interdisziplinäre Zusammenarbeit im Gesundheitswesen rechtskonforme und praktikable Lösungen sowohl gesetzgeberisch als auch bei der Umsetzung gefunden und Handlungshilfen bereitgestellt werden.

Im Berichtszeitraum kam es wieder zu wichtigen Weichenstellungen auf dem Weg zu einer digitalisierten Gesundheitsversorgung. Die Aufbereitung sämtlicher datenschutzrelevanter Inhalte würde den Rahmen dieses Berichts sprengen. Deshalb werden nur einzelne aus Sicht des Datenschutzes besonders relevante Entwicklungen herausgestellt.

Digitale Gesundheitsanwendungen

Im Zuge der voranschreitenden Digitalisierung des deutschen Gesundheitswesens hatte die Bundesregierung in dem sogenannten Digitalen Versorgungs-Gesetz (DVG) bereits 2019 die rechtlichen Grundlagen für eine Regelversorgung der gesetzlich Versicherten mit digitalen Gesundheitsanwendungen – kurz DiGA – gelegt. In der im Jahr 2020 in Kraft gesetzten Digitalen-Gesundheitsanwendungen-Verordnung (DiGAV) wurden die Einzelheiten des Verfahrens, insbesondere der Erstattungsfähigkeit einzelner Anwendungen, festgelegt.

Aus Sicht des Datenschutzes war zunächst zu begrüßen, dass nur solche DiGAs von der Gesetzlichen Krankenversicherung erstattet werden dürfen, die den Anforderungen an den Datenschutz entsprechen und Datensicherheit nach dem Stand der Technik gewährleisten (§§ 33a Abs. 1, 139e Abs. 2 Satz 2 Nr. 2 SGB V). Sofern dies der Fall ist, nimmt das mit der Ausführung des Gesetzes beauftragte Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) die einzelne DiGA in ein Verzeichnis auf. Nur darin enthaltene DiGAs sind erstattungsfähig. Allerdings sieht das im Jahr 2020 in der DiGAV festgelegte Verfahren zur Aufnahme in das vom BfArM geführte Verzeichnis keine verlässliche und objektive Prüfung der gesetzlichen Anforderungen nach § 139e Abs. 2 Satz 2 Nr.

2 SGB V vor. Vielmehr soll es ausreichen, dass die Hersteller im Rahmen einer Selbsterklärung das Vorliegen bestimmter von dem Verordnungsgeber benannten Voraussetzungen bestätigen. Ist dies der Fall, wird die Herstellererklärung als Nachweis der gesetzlichen Anforderungen fingiert und eine Aufnahme der DiGA in das Verzeichnis nach § 139e SGB V erfolgt.

Hiergegen hatten die Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren schon frühzeitig Bedenken erhoben, leider ohne Erfolg. Die Bedenken erwiesen sich leider als berechtigt, nachdem bei einer der ersten im Oktober 2020 in das Verzeichnis aufgenommenen DiGA bereits Sicherheitslücken festgestellt worden waren. Ob die Bundesregierung künftig die von den Datenschutzbehörden geforderte Vorlage verlässlicher Nachweise für die Datenschutzkonformität von DiGAs verlangt, bevor diese in das Verzeichnis aufgenommen werden können, muss leider bezweifelt werden. Während der Nachweis bzgl. der Anforderungen an die IT-Sicherheit der Anwendungen nach den aktuellen gesetzgeberischen Planungen mittelfristig nur noch durch vom BSI ausgestellte Zertifikate erfolgen soll, sieht der aktuelle Gesetzentwurf für die Einhaltung datenschutzrechtlicher Anforderungen die Vorlage vergleichbarer verlässlicher Belege leider nicht vor. Dies ist nicht akzeptabel und konterkariert die in § 139e Abs. 2 Satz 2 Nr. 2 SGB V enthaltene klare gesetzliche Vorgabe, wonach die in das Verzeichnis aufzunehmenden DiGAs datenschutzkonform sein müssen und dies nachzuweisen ist. Letztendlich widerspricht der Gesetzgeber damit seinem eigenen Bekenntnis, dass die Wahrung des Datenschutzes in einem digitalisierten Gesundheitswesen höchste Priorität habe.

Elektronische Patientenakte (ePA)

Die ePA ist eine freiwillige, unentgeltliche und versichertengeführte Anwendung der Telematikinfrastruktur in der Gesetzlichen Krankenversicherung. Sie gilt als zentraler Baustein in der Digitalisierung des deutschen Gesundheitswesens. Ihr Leistungsumfang ergibt sich aus § 341 SGB V. Mit der ePA sollen Versicherte bei ihrer einrichtungs-, fach- und sektorenübergreifenden Gesundheitsversorgung unterstützt werden und einen transparenten Überblick über ihre in diesem Zusammenhang verarbeiteten Gesundheitsdaten erhalten. Zu diesem Zweck können die in § 341 Abs. 2 SGB V genannten Daten in die ePA eingestellt werden. Die Versicherten können auf diesem Wege ihre jeweiligen Behandlerinnen und Behandler im erforderlichen Umfang über ihren Gesundheitszustand und andere Behandlungen informieren, indem zum Beispiel Befunde für alle zugänglich in die ePA geladen werden. Nach dem im Jahr 2020 in Kraft getretenen Patientendaten-Schutzgesetz (PDSG) mussten die Krankenkassen ihren Versicherten bereits zum Jahresbeginn 2021 die ePA als App bereitstellen.

Datenschutzrechtlich standen insbesondere die zunächst nach dem PDSG nur sehr eingeschränkte Möglichkeit der Versicherten zur Steuerung der Zugriffsrechte auf die ePA sowie die nicht vollständige Gewährleistung der Betroffenenrechte für Nutzer ohne eigenes mobiles Endgerät im Fokus der Kritik. So besteht für Patientinnen und Patienten im Jahr 2021 zwar bereits die Möglichkeit der Nutzung der ePA, sie können jedoch die Zugriffsrechte der jeweiligen Behandler noch nicht gezielt steuern. Dies bedeutet, dass im Jahr 2021 entweder alle in die ePA eingestellten Dokumente von den zugriffsberechtigten Behandlerinnen und Behandler eingesehen werden können oder ein Zugriff komplett verwehrt werden muss. Erst ab dem Jahr 2022 soll es möglich sein, dass Patientinnen und Patienten gezielt entscheiden können, welche Zugriffsrechte der jeweiligen Behandlerin bzw. dem jeweiligen Behandler zugewiesen werden. Diese durch den Gesetzgeber nur verzögert ermöglichte differenzierte Zugriffsrechtesteuerung auf die ePA ist daten-

schutzrechtlich bedenklich und wurde im Gesetzgebungsverfahren von den Datenschutzaufsichtsbehörden stark kritisiert.

Gleiches gilt für die im Ergebnis nur indirekt Nutzern ohne eigenes Endgerät eingeräumte Möglichkeit, ihre Betroffenenrechte wie z.B. das Recht auf Auskunft wahrzunehmen. Diese können zwar auch eine ePA nutzen, dürfen aber erst ab dem Jahr 2022 einen Vertreter benennen, über dessen Endgerät sie dann ihre Rechte ausüben sollen. Eine eigene Wahrnehmungsmöglichkeit von Betroffenenrechten z.B. über Terminals bei den Krankenkassen wird ihnen dauerhaft versagt. Auch dies verstößt im Ergebnis elementar gegen die Vorgaben der Datenschutz-Grundverordnung und ist nicht hinnehmbar.

Trotz dieser massiven Bedenken und einer Entschließung der DSK aus dem September 2020, in der diese datenschutzrechtliche Verbesserungen angemahnt hatte, wurde der Entwurf des PDSG nicht mehr geändert und trat im Oktober 2020 in Kraft. Der LfDI hat sich im Zuge der aufgezeigten datenschutzrechtlichen Defizite unmittelbar an die seiner Zuständigkeit unterliegenden Krankenkassen gewandt und mit ihnen vereinbart, im Falle diesbezüglich eingehender Beschwerden von Versicherten einvernehmliche und datenschutzgerechte Lösungen zu erzielen. Von aufsichtsrechtlichen Maßnahmen sah er dagegen angesichts der strikten technischen Spezifikationen der Gematik, die den Krankenkassen eine Abweichung von den im PDSG enthaltenen Vorgaben faktisch unmöglich machten, ab.

Zentrale sichere Kommunikationsdienste

Mittlerweile steht im Fokus der Digitalisierung des Gesundheitswesens auch eine zeitgemäße und sichere Kommunikation zwischen den Beteiligten. Telefax und der Austausch von WhatsApp-Nachrichten im Behandlungskontext sollen nach den Vorstellungen der Bundesregierung bald der Vergangenheit angehören. Der im Herbst 2020 zunächst vorgelegte Referentenentwurf des Digitalen Versorgung und Pflege-Modernisierungs-Gesetzes (DVPMG) sowie der daraus im Februar 2021 entstandene Regierungsentwurf sehen endlich die Etablierung von sicheren Übermittlungsverfahren, die auch einen Sofortnachrichtendienst umfassen, zu einem sog. zentralen sicheren Kommunikationsdienst in der Gesundheitsversorgung vor. Nach den im Entwurf enthaltenen Vorstellungen soll die Gematik spätestens bis zum Jahr 2023 schrittweise neben den bereits bestehenden Festlegungen zur elektronischen Übermittlung von medizinischen Dokumenten auch solche für einen Sofortnachrichtendienst sowie zu Videokonferenzsystemen treffen. Die über die Telematikinfrastruktur laufenden und von der Gematik zuzulassenden Dienste der sicheren Übermittlungsverfahren sollen insbesondere der Kommunikation der Leistungserbringer untereinander, zwischen Leistungserbringern und Versicherten sowie zwischen Leistungserbringern und den Krankenkassen dienen.

Die Intention der Bundesregierung ist richtig und überfällig, Rahmenbedingungen für eine zeitgemäße und sichere Kommunikation zwischen den Beteiligten im digitalen Gesundheitswesen festzulegen. Hierzu gehört natürlich auch die Berücksichtigung datenschutzrechtlicher Anforderungen. Im Zusammenhang mit der Nutzung von sog. Messengerdiensten in Krankenhäusern hatte die DSK bereits im Jahr 2020 ein Whitepaper vorgelegt, das die Belange des Datenschutzes konkretisierte. Diese sollten bei den von der Gematik nach dem Gesetzentwurf zu treffenden Festlegungen aufgegriffen werden. Es bleibt jedoch abzuwarten, welche Änderungen der Gesetzentwurf im weiteren Gesetzgebungsverfahren noch erfahren wird und ob es tatsächlich zu einem datenschutzgerechten sicheren zentralen Kommunikationsdienst im Gesundheitswesen kommt.

Informationen zur Digitalisierung des Gesundheitswesens auf der Internetseite der Initiative „Mit Sicherheit gut behandelt“

Die auch über die Landesgrenzen von Rheinland-Pfalz hinaus beispielgebende Kooperation des LfDI mit der rheinland-pfälzischen Kassenärztlichen Vereinigung, der Landespsychotherapeutenkammer und der Landesärztekammer, die Initiative „Mit Sicherheit gut behandelt“, hat im Berichtszeitraum ihre Unterstützungsangebote ausgebaut und auf ihrer Internetseite u.a. einen Themenblock zur Digitalisierung des Gesundheitswesens neu eingerichtet. Die Informationsangebote sollen dazu beitragen, die Praxisinhaberinnen und Praxisinhaber auf die datenschutzrechtlichen Bezüge des Digitalisierungsprozesses aufmerksam zu machen und neben allgemeinen Informationen auch die daraus resultierenden praxisbezogenen Auswirkungen darzustellen. Ziel ist es, die Akzeptanz für den Datenschutz bei der Digitalisierung des Gesundheitsbereichs bei den Praxisinhaberinnen und Praxisinhabern zu erhöhen. Denn diese sind es schließlich, die auch in einer digitalisierten Gesundheitsversorgung neben anderen Akteuren weiterhin für die Einhaltung des Datenschutzes rechtlich verantwortlich sein werden. Umso mehr ist es erforderlich, ihnen frühzeitig geeignete Informationsmöglichkeiten anzubieten und sie auf die künftigen vielschichtigen Fragestellungen vorzubereiten. Aus Sicht der Kooperationspartner bietet die Initiative damit ihren Mitgliedern eine erste Hilfestellung bei der Bewältigung des gegenwärtigen Transformationsprozesses.

8.2 Unterrichtung von Schulen über negative Corona-Testergebnisse bei Schülern oder Lehrern durch die Gesundheitsämter

Nach in einzelnen Schulen aufgetretenen Infektionsfällen wurden auf Veranlassung der jeweils zuständigen Gesundheitsämter mehrfach komplette Lehrerkollegien und Schulklassen auf das Vorliegen einer Corona-Infektion getestet. In den Fällen, in denen keine Infektion festgestellt werden konnte, kam es im November 2020 wiederholt zu einer unmittelbaren Übermittlung der Testergebnisse durch die Gesundheitsämter an die jeweiligen Schulleitungen. Eine unmittelbare Unterrichtung der getesteten Personen über das Ergebnis ihrer Testung erfolgte nicht. Hiergegen erhoben betroffene Lehrer und Schüler beim LfDI Beschwerde.

Im Ergebnis verstieß die Weitergabe der negativen Testergebnisse durch die Gesundheitsämter an die Schulleitungen gegen die Vorgaben des Datenschutzes. Denn soweit Gesundheitsämter gegenüber Schulleitungen personenbezogene Angaben zum Ergebnis von Infektionstests von Lehrern und Schülern machen, stellt dies datenschutzrechtlich eine Übermittlung besonderer Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DS-GVO dar. Die Übermittlung dieser Daten ist nach den Vorgaben des Art. 5 Abs. 1 lit. a, Art. 6 Abs. 1 und Art. 9 Abs. 2 DS-GVO nur zulässig, wenn eine Rechtsgrundlage die Datenverarbeitung erlaubt oder der einzelne Betroffene darin eingewilligt hat. Dies war in den an den LfDI herangetragenen Sachverhalten jedoch nicht der Fall.

Nach den Vorgaben des Art. 6 Abs. 1 lit. e, Abs. 3 DS-GVO in Verbindung mit § 11 Abs. 3 des ÖGdG ist die Übermittlung personenbezogener Daten durch ein Gesundheitsamt zulässig, wenn eine der in § 11 Abs. 3 ÖGdG enthaltenen Anforderungen erfüllt ist. Mangels einer von den Betroffenen erteilten Einwilligung in die Datenübermittlung kam es für deren Zu-

lässigkeit auf das Vorliegen einer gesetzlichen Übermittlungsbefugnis an. Diese lag jedoch nicht vor. Insbesondere war die Weitergabe der negativen Testergebnisse an die Schulleitungen nicht zur rechtmäßigen Aufgabenerfüllung der Gesundheitsämter oder zur Gefahrenabwehr im Sinne von § 11 Abs. 3 Nr. 1 i.V.m. Abs. 2 Nr. 3 ÖGdG erforderlich. Denn mit den negativen Testergebnissen bestand für die Schule im Rahmen des Schulbetriebs trotz einer möglichen Anwesenheit der Getesteten objektiv keine konkrete Gesundheitsgefährdung. Zwar war zuzugeben, dass für die weitere Planung des Schulbetriebs regelmäßig detaillierte Informationen über bestehende oder nicht bestehende Infektionsfälle und die damit zusammenhängende Verfügbarkeit von Lehrern und Schülern durchaus von hohem Interesse sein können. Allerdings ist eine darauf bezogene Datenübermittlung durch das Gesundheitsamt an die Schule bei negativen Testergebnissen und damit tatsächlich nicht vorhandenen Infektionsfällen nach den gesetzlichen Vorgaben ohne Einwilligung der Betroffenen nicht zulässig.

Die Rechtslage führt im Ergebnis nicht zu einer unzumutbaren Einschränkung der Organisation des Schulbetriebs. Denn im Falle einer festgestellten Infektion wären die Schulen ohnehin auf der Grundlage infektionsschutzrechtlicher Vorgaben durch das zuständige Gesundheitsamt zu unterrichten gewesen. Soweit bei durchgeführten Testungen dagegen keine Infektionen festgestellt wurden, besteht weder eine konkrete Gefährdungslage noch ein daraus resultierender Bedarf für eine unmittelbare Kommunikation zwischen Gesundheitsamt und Schule über die Testergebnisse. Darüber hinaus müssen der Schulleitung ohnehin die für die Organisation des Schulbetriebs erforderlichen Informationen zur Verfügbarkeit des Lehrpersonals auf der Grundlage arbeitsvertraglicher bzw. dienstrechtlicher Mitwirkungspflichten von den einzelnen Lehrern mitgeteilt werden. Alternativ dazu wäre im Falle eines rascheren Informationsbedarfs der Schule die Einholung von Einwilligungen der betroffenen Lehrer in die unmittelbare Mitteilung der Testergebnisse durch das Gesundheitsamt an die Schule im Vorfeld der Testungen denkbar gewesen.

Die dem LfDI durch Beschwerden bekannt gewordenen Datenübermittlungen wurden gem. § 17 Abs. 1 LDSG jeweils formell beanstandet. Die betroffenen Kreisverwaltungen haben das datenschutzwidrige Vorgehen umgehend eingestellt.

8.3 Zulässigkeit der Weitergabe der Identität infizierter Personen durch Gesundheitsämter

Mit der Corona-Pandemie stellten sich viele Fragen zur Zulässigkeit der Weitergabe von Daten infizierter Personen durch die Gesundheitsämter. Insbesondere wurde darüber diskutiert, ob eine Bereitstellung von Listen infizierter Personen oder zumindest von Örtlichkeiten, in denen sich infizierte Personen aufhalten, zum Schutz von Einsatz- und Rettungskräften den Polizei- und Ordnungsbehörden oder den Integrierten Leitstellen bereit gestellt werden dürfen.

Soweit die durch die Gesundheitsämter weitergegebenen Informationen keinen Personenbezug enthalten, ist dies datenschutzrechtlich unproblematisch. Eine allgemeine Unterrichtung über die Höhe aufgetretener Infektionsfälle in räumlich abgegrenzten Gebieten wie z.B. Stadtbezirken oder einzelnen Ortsteilen begegnet daher regelmäßig keinen Bedenken. Denn ohne Personenbezug unterliegt die Verarbeitung derartiger Informationen nicht dem Datenschutz. Anders verhält es sich dagegen, wenn Angaben über einzelne Infizierte oder sogar eine Auflistung von Personen, bei denen eine Infektion festgestellt wurde, durch die Gesundheitsbehörden bereitgestellt werden

sollen. Für die Zulässigkeit einer derartigen Informationsweitergabe sind die fachrechtlichen Vorgaben maßgeblich:

Um die nach dem Infektionsschutzgesetz vorgesehenen Schutzmaßnahmen treffen zu können sind die Gesundheitsämter befugt, die hierzu zuständigen Behörden – in Rheinland-Pfalz die Kreisordnungsbehörden – über festgestellte erkrankte Personen zu unterrichten. Überdies sind die Gesundheitsämter nach den Bestimmungen des § 11 Abs. 3 Nr. 1, Abs. 2 Nr. 3 ÖGdG befugt, personenbezogen Daten an Dritte wie etwa Polizei- und Ordnungsbehörden oder Integrierte Leitstellen zu übermitteln. Die Voraussetzungen hierfür sind, dass die Weitergabe im Einzelfall zur Abwehr von gegenwärtigen Gefahren für das Leben oder die Gesundheit einer dritten Person erforderlich ist und dass die genannten Rechtsgüter das Geheimhaltungsinteresse der betroffenen Person erheblich überwiegen. Hiernach wäre es zum Schutz von Einsatzkräften zulässig, diese auf eine konkrete Anfrage hin über das Vorliegen einer übertragbaren Krankheit bei einem Betroffenen zu informieren, wenn ein Einsatz mit Personenkontakt wie etwa der Vollzug eines Haftbefehls, eine Durchsuchung oder ein Rettungseinsatz unmittelbar bevorsteht und zu befürchten ist, dass aufgrund konkreter Umstände ein erhöhtes Ansteckungsrisiko der Einsatzkräfte bestehen könnte.

Demgegenüber wäre eine einzelfallunabhängige generelle Bereitstellung von Listen infizierter Personen durch die Gesundheitsämter datenschutzrechtlich unzulässig. Aufgrund der bestehenden rechtlichen Vorgaben haben die Gesundheitsämter nach der derzeitigen Rechtslage deshalb auch keine Befugnis, auf kommunaler Ebene angeregte virtuelle Informations-Plattformen fortlaufend mit Daten zu füllen. Diese Einschränkung ist auch aus Sicht des Datenschutzes nicht zu beanstanden, da entsprechende Listen aufgrund ihrer fehlenden Validität und Aktualität im Einzelfall gerade nicht geeignet wären, verlässlich ggf. bestehende Infektionsrisiken auszuschließen. Denn unabhängig von den gemeldeten Infektionsfällen können jederzeit Personen infiziert sein, ohne dass sie es selbst bereits wissen. Insofern hätten Einsatz- und Einsatzkräfte auch bei vorhandenen Auflistungen immer alle Vorkehrungen zu treffen, um eine Infizierung zu vermeiden. Angesichts des darüber hinaus potentiell stigmatisierenden Charakters derartiger Auflistungen stellt die Rechtslage letztlich einen angemessenen Ausgleich zwischen den Bedürfnissen der Einsatz- und Rettungskräfte und dem informationellen Selbstbestimmungsrecht der infizierten Personen dar.

Die Landesregierung teilte im Zusammenhang mit der Behandlung eines darauf bezogenen Landtagsantrags (Drucksache 17/14310) diese Rechtsauffassung ausdrücklich.

8.4 Datenschutz und Corona-Schutzimpfungen

Im Dezember 2020 kam es auch in Rheinland-Pfalz zum Aufbau einer organisatorischen und technischen Infrastruktur für die Durchführung von Corona-Schutzimpfungen. Neben der Errichtung von Impfzentren und mobilen Impfteams gehörten insbesondere die Organisation der Impfanmeldung sowie die Durchführung der Impfung einschließlich der Impfdokumentation zu den Aufgaben der Landesregierung bzw. des fachlich zuständigen Ministeriums für Soziales, Arbeit, Gesundheit und Demografie (MSAGD). Dass dabei auch das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger gewahrt werden musste, war selbstverständlich.

Aufgrund dessen wurde beim Aufbau der Infrastruktur für die Impfungen die Expertise des LfDI genutzt, um den Schutz der Daten im Zusammenhang mit den freiwilligen Impfungen

sicherzustellen. Die seitens des LfDI gemachten Anregungen, insbesondere hinsichtlich der Transparenz der Datenverarbeitung, wurden alle aufgegriffen. Die konstruktive Zusammenarbeit zwischen MSAGD, der Impfdokumentation Rheinland-Pfalz und dem LfDI setzte sich auch mit dem Beginn der Impfungen im Jahr 2021 fort. Auf der Internetseite des LfDI wurden wesentliche Fragen hinsichtlich des Datenschutzes bei der Durchführung der Corona-Schutzimpfungen aufgegriffen und beantwortet.

9. SOZIALES

9.1 Bereitstellung von Unterlagen durch eine Sozialbehörde im Zusammenhang mit einer Kindeswohlgefährdung

Dass datenschutzrechtliche Regelungen der Bereitstellung personenbezogener Dokumente nicht im Wege stehen müssen, sondern im Gegenteil die Aufgabenerfüllung einzelner Stellen konkret unterstützen, wurde einer Sozialbehörde im Zusammenhang mit der Anfrage eines Jugendamts bewusst. Aufgrund der Anzeige einer drohenden Kindeswohlgefährdung nahm das örtlich zuständige Jugendamt eine Einschätzung des bestehenden Gefährdungsrisikos im Sinne von § 8a Abs. 1 Satz 1 SGB VIII vor. In diesem Zusammenhang wandte sich das Jugendamt an das Sozialamt der Kreisverwaltung und bat unter Hinweis auf die drohende Kindeswohlgefährdung und das von ihm abzuschätzende Gefährdungsrisiko um die Bereitstellung von bei dem Amt vorgehaltenen Unterlagen hinsichtlich der Kindesmutter. Dabei wurden ausdrücklich beim Sozialamt vorhandene Diagnosen, Arztberichte und Unterlagen im Zusammenhang mit der Beantragung von Leistungen der Eingliederungshilfe angefordert. Im Ergebnis verweigerte das Sozialamt die Übermittlung der seitens des Jugendamtes erbetenen Angaben bzw. Dokumente, solange keine Schweigepflichtentbindungserklärung der Betroffenen vorgelegt werde. Zugleich vertrat das Sozialamt gegenüber dem Jugendamt die Auffassung, dass eine Pflicht zur Bereitstellung der angeforderten personenbezogenen Informationen nicht bestehe, sofern die Datenerhebung telefonisch erfolge. Erst nachdem das Jugendamt eine von der Betroffenen unterzeichnete Schweigepflichtentbindungserklärung vorgelegt hatte, stellte das Sozialamt am 17.02.2020 die angeforderten Unterlagen zur Verfügung.

Mit der Weigerung, die seitens des Jugendamtes angeforderten Unterlagen ohne Vorlage einer Schweigepflichtentbindungserklärung zu übermitteln, verstieß das Sozialamt gegen Art. 5 Abs. 1 lit. a DS-GVO i.V.m. Art. 6 Abs. 1 lit. e DS-GVO, §§ 4 Abs. 4; 69 Abs. 1 Nr. 1 SGB X; 8a Abs. 1 Satz 1, Abs. 5 Satz 1 und 62 Abs. 3 Nr. 2 lit. d SGB VIII. Nach den gesetzlichen Vorgaben des Sozialdatenschutzes sind den örtlich zuständigen Jugendhilfeträgern im Zusammenhang mit der von ihnen nach § 8a Abs. 1 Satz 1 SGB VIII vorzunehmenden Einschätzung des Gefährdungsrisikos von den sonstigen Sozialleistungsträgern die hierzu angeforderten erforderlichen personenbezogenen Angaben im Wege der Amtshilfe bereit zu stellen (§§ 4 Abs. 4; 69 Abs. 1 Nr. 1 SGB X; 8a Abs. 1 Satz 1, Abs. 5 Satz 1 und 62 Abs. 3 Nr. 2 lit. d SGB VIII). Der Vorlage einer Einwilligungs- oder Schweigepflichtentbindungserklärung bedarf es in diesen Fällen nicht. Da nach § 67d Abs. 1 Satz 2 SGB X die die Daten anfordernde Stelle die Verantwortung für die Richtigkeit der Angaben in dem Ersuchen trägt, hat die übermittelnde Stelle zudem nicht zu prüfen, ob im konkreten Fall eine Kindeswohlgefährdung droht und die angeforderten Daten zur Einschätzung des Gefährdungsrisikos erforderlich sind.

Es entspricht deshalb nicht dem Anliegen des Datenschutzes, trotz derartiger rechtlicher Regelungen dem berechtigten Ersuchen des Jugendamtes entgegenzutreten und die erbetenen Unterlagen nicht bereitzustellen. Der Datenschutzverstoß wurde gegenüber der Kreisverwaltung nach § 17 Abs. 1 LDSG formell beanstandet.

9.2 Übermittlung von unrichtigen personenbezogenen Daten durch das Jugendamt

In der Presse wurde darüber berichtet, dass ein Jugendamt im Rahmen eines familiengerichtlichen Verfahrens wegen „Namensidentität“ und unsachgemäßer Prüfung eine Person als Vater benannt hatte, die zu keinem Zeitpunkt in Kontakt mit der Kindsmutter gestanden habe. Diese Person beschwerte sich über das Vorgehen des Jugendamts beim LfDI, dem diese „Datenpanne“ von Seiten des Jugendamts auch nicht gemeldet worden war.

Die Beschwerde führte zu einer förmlichen Beanstandung des Jugendamts wegen Verstoßes gegen Art. 5 Abs. 1 lit. a und d i.V.m. Abs. 2 und Art. 6 Abs. 1 lit. c bzw. e, Abs. 3 sowie Art. 33 DS-GVO. Die Übermittlung von personenbezogenen Daten bedarf als eine Form der Datenverarbeitung einer Rechtsgrundlage. Dies gilt selbstverständlich auch, sofern diese auf Anforderung einer Behörde oder eines Gerichtes erfolgt. Eine Rechtsgrundlage ist allein einschlägig, wenn der Verantwortliche berechtigterweise von der Richtigkeit der zu übermittelnden personenbezogenen Daten ausgehen durfte. Das Jugendamt hatte hier ohne die notwendige Überprüfung der vorliegenden Unterlagen den Beschwerdeführer als Vater des Kindes gegenüber dem Amtsgericht genannt. Darüber hinaus hatte das Jugendamt die erforderliche „Datenpannenmeldung“ an den LfDI unterlassen, obgleich für den Beschwerdeführer gravierende Konsequenzen aus der fehlerhaften Datenübermittlung resultierten. Eine Einschätzung hinsichtlich des Risikos für den Beschwerdeführer, die bei Nichtvornahme der Meldung nachzuweisen ist, wurde nicht vorgenommen.

10. KOMMUNALES

10.1 Netzwerktreffen mit den behördlichen Datenschutzbeauftragten

Die 2007 initiierte und jährlich weitergeführte Reihe von Informationsveranstaltungen insbesondere für die Datenschutzbeauftragten der Kommunen sollte im März 2020 mit der Kreisverwaltung Bad Dürkheim als Gastgeberin mit gut 50 Teilnehmerinnen und Teilnehmern fortgesetzt werden.

Leider musste diese Veranstaltung kurzfristig im unmittelbaren Vorfeld des ersten Lockdown abgesagt werden. Da diese Treffen einen maßgeblichen Anteil daran haben, dass seitens der Aufsichtsbehörde gute Kontakte zu den behördlichen Datenschutzbeauftragten bestehen, wird der Austausch zu gegebener Zeit mit alternativen Angeboten wie Video- oder Hybrid-Konferenzen fortgeführt.

10.2 Durchführung örtlicher Kontroll- und Beratungsbesuche

Im Herbst 2019 wurde mit einer umfangreichen Prüfphase von insgesamt 12 Kommunalverwaltungen auf der Grundlage von § 16 Abs. 1 und § 17 Abs. 3 LDSG i.V.m. den Art. 57 und 58 DS-GVO begonnen.

Nach dem Besuch der vierten Kommunalverwaltung musste auch diese Maßnahme pandemiebedingt eingestellt werden, zumal gerade die persönlichen Gespräche mit der jeweiligen Behördenleitung und den Beschäftigten aus verschiedenen Fachbereichen für die Mitarbeiter des LfDI hilfreich waren.

Klar geworden ist aber bereits anhand dieser Besuche, dass es für die nachhaltige Implementierung eines Datenschutz-Management nicht ausreichen wird, dem Datenschutzbeauftragen ein festes Zeitkontingent (27. Tätigkeitsbericht 2018, III.-11.) zur Verfügung zu stellen und dies im Stellenplan zu dokumentieren. So ergibt sich für Datenschutzbeauftragte, die nicht mit 100 % eines Vollzeit-Äquivalents ausgestattet sind, das Problem, dass der Arbeitsanfall im außerdem wahrzunehmenden Aufgabenbereich gleichbleibend planbar und dauerhaft kalkulierbar sein muss, weil ansonsten z.B. bei der Mitarbeit in Projekten, der Haushaltsaufstellung, o.ä. die Gefahr besteht, dass sich der für die Arbeit des Datenschutzbeauftragten vorgesehene Zeitanteil maßgeblich verringert.

Weiterhin ist schon frühzeitig im Zusammenhang mit den Kontroll- und Beratungsbesuchen die Frage aufgetaucht, ob der LfDI als Aufsichtsbehörde überhaupt die Befugnis hätte, die

- Benennung eines Datenschutzbeauftragten
- Dokumentation des Datenschutz-Management
- Erstellung eines Verzeichnisses nach Art. 30 DS-GVO oder die
- Durchführung einer Datenschutz-Folge abschätzung zu einer Verarbeitungstätig keitbzw. einem Verarbeitungsvorgan gemäß Art. 58 Abs. 2 DS-VO anzu weisen.

Dies ist der DS-GVO nicht eindeutig zu entnehmen und noch zu klären.

Die Besuche werden fortgesetzt, sobald es pandemiebedingt wieder möglich ist und die Personalsituation es erlaubt, um mit den weiter zum IST-Zustand zu gewinnenden Erkenntnissen aus der Sicht des Datenschutzes weiterführende Maßnahmen formulieren zu können.

10.3 Personenbezogene Veröffentlichung von Sitzungsniederschriften und sonstiger Dokumente aus der Gremienarbeit

Trotz ausführlichen Erläuterungen im 26. Datenschutzbericht 2016/2017, IV-9.1.4, sind gerade die an dieser Stelle geschilderten Beispiele aus der Praxis weiterhin Gegenstand von begründeten Beschwerden und Hinweisen der Bürgerinnen und Bürger.

Für die Veröffentlichung von Dokumenten aus der Gremienarbeit mit personenbezogenen Daten u.a. im Internet, die letztlich eine Offenlegung und somit eine Datenverarbeitung gem. Art. 4 Nr. 2 DS-GVO darstellt, gibt es grundsätzlich keine Verarbeitungsgrundlage gem. Art. 6 Abs. 1 DS-GVO. Die Aufgabenerfüllung der Kommune erfordert keine beliebige Datenweitergabe, denn das Kommunalverfassungsrecht sieht regelmäßig nur eine lokal begrenzte Öffentlichkeit vor. Zudem müssen gemäß Art. 5 Abs. 1 lit. c DS-GVO personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

§ 41 Abs. 5 Gemeindeordnung (GemO; § 34 Abs. 5 Landkreisordnung, LKO) sieht weiter vor, dass die Verwaltung die Einwohnerinnen und Einwohner über die Ergebnisse der Ratssitzungen in geeigneter Form unterrichten soll. Dies kann aber nur innerhalb dem von § 35 Abs. 1 GemO (§ 28 Abs. 1 LKO) vorgegebenen Rahmen erfolgen. Zur Erfüllung dieser Aufgabe durch die Kommune ist es aber nicht erforderlich, personenbezogene Daten zu verarbeiten. Mit anderen Worten, ein Text, mit dem die Pflicht zur Veröffentlichung aus § 41 Abs. 5 GemO erfüllt werden soll, muss grundsätzlich so formuliert sein, dass keine personenbezogenen Daten aufgeführt werden.

Deshalb müssen vor der Veröffentlichung von Sitzungsvorlagen sowie Niederschriften über das Bürgerinformationssystem oder die Online-Ausgabe des Amtsblattes im Internet ggf. alle personenbezogenen Daten aus den Dokumenten entfernt werden. Ansonsten wäre von einem Verstoß gegen Art. 5 Abs. 1 lit. a, lit. c, Art. 6 Abs. 1 DS-GVO bzw. § 3 LDSG auszugehen, der mit einer Beanstandung (§ 17 Abs. 1 LDSG) sanktioniert werden könnte.

In diesem Kontext wurden mehrere Beanstandungen ausgesprochen – für Kommunal-verwaltungen besteht hier offenbar noch Nachbesserungsbedarf. Damit steht in Zusammenhang, dass die Kommunalverwaltungen mit ihrem Rats- und Bürgerinformationssystem regelmäßig ein wahlperiodenübergreifendes Sitzungsarchiv inklusive einer Möglichkeit zur Recherche zur Verfügung stellen. Es befähigt die Mandatsträgerinnen und die Mandatsträger sowie auch die Bürgerinnen und Bürger, sich über frühere Entscheidungen der Gremien zu erneut anstehenden Sachthemen zu informieren und vorzubereiten.

Soweit darin abgelegte weitere Dokumente evtl. personenbezogene Daten enthalten, stellt sich aber die Frage, wie mit ihnen umzugehen ist – Schwärzung oder ersatzlose Herausnahme aus dem über das Internet zugänglichen Angebot. Eine dauerhafte Bereitstellung von Dokumenten könnte gegebenenfalls auf eine geschlossene Nutzergruppe für die Mandatsträgerinnen und Mandatsträger beschränkt werden.

11. BILDUNG

11.1 Coronabekämpfung in der Schule – ein Thema für den Datenschutz

In den Schulen stellten sich mit Beginn der Corona-Pandemie und den daraus folgenden Schulschließungen ab dem 17. März 2020 Herausforderungen an Infrastruktur und Organisation. Dies führte zu zahlreichen Fragen hinsichtlich der Verarbeitung von Daten bei den nun digitalisierten Lernwegen sowie anfallender medizinischer Daten, beispielsweise bei der Maskenbefreiung.

Videokonferenzsysteme

Der Umstieg von Präsenzunterricht auf Homeschooling stellte schlagartig große Anforderungen an die digitale Infrastruktur Im Bildungssektor, insbesondere was die Durchführung von Videokonferenzen anbelangte. Das Bildungsministerium (BM) und der LfDI waren daher während der Osterferien im engen Austausch, welche Videokonferenzplattform binnen kürzester Zeit entsprechend ausgebaut und hochskaliert werden könne, bei gleichzeitig datenschutzkonformem Betrieb. Der LfDI beriet das BM hinsichtlich einer Lösung mit dem US-amerikanischen Anbieter Cisco Webex in Verbindung mit der Deutschen Telekom als Infrastrukturbetreiber. Gleichzeitig sprach der LfDI eine Duldung aus, dass Schulen während der Coronapandemie vorübergehend auch die marktüblichen Produkte von außereuropäischen Anbietern für die Durchführung des Online-Unterrichts unter bestimmten Auflagen nutzen konnten.

Während durch das BM parallel der Ausbau einer eigenen Videoplattform des Landes auf Basis der Open-Source-Software „BigBlueButton“ auf Servern der Johannes Gutenberg-Universität Mainz vorangetrieben wurde, stellte sich mit dem EuGH-Urteil („Schrems II“) vom Juli 2020 die Frage der grundsätzlichen Zulässigkeit amerikanischer Dienste im Schulbereich. In der Folge erreichten den LfDI zahlreiche Beschwerden von Eltern wie auch Lehrkräften, die ganz konkret gegen die Nutzung amerikanischer Produkte richteten. Der LfDI wurde daraufhin gegenüber solchen Schulen tätig, die beispielsweise amerikanische Dienste als verpflichtendes Lehrmittel nach §1 Abs. 6 i. V. m. § 67 Abs.1 SchulG (siehe TB 2019, Tz.12.5) eingeführt hatten, ohne die Möglichkeit alternativer Kommunikationswege anzubieten (**https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/grosse-herausforderung-fuer-schulen-auch-bei-videokonferenzsystemen-muss-datenschutz-sichergestellt-s/**). Bei sämtlichen Beschwerden konnten jedoch datenschutzverträgliche Lösungen gefunden werden.

Atteste zur Maskenbefreiung

Mit der Rückkehr in den Präsenzunterricht nach den Sommerferien führten die Schulen eine Pflicht zum Tragen von Mund-Nase-Bedeckungen (MNB) ein. Zur Befreiung von der Maskenpflicht aus medizinischen Gründen verlangten die Schulen nach einer Vorgabe der Aufsichts- und Dienstleitungsdirektion (ADD) nun entsprechende „qualifizierte“ Atteste von den Betroffenen, aus denen auch die Diagnose hervorgehen musste. Dies führte zu insgesamt weit über 80 Beschwerden von betroffenen Eltern und Lehrkräften beim LfDI. Dieser stellte fest, dass hierfür zum damaligen Zeitpunkt keine rechtliche Grundlage bestand, aus der sich das Vorlegen qualifizierter Atteste herleiten ließe. Er sprach eine Warnung gegenüber der ADD aus und forderte die Schaffung einer entsprechenden Rechtsgrundlage (https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/bei-attesten-zur-befreiung-von-der-maskenpflicht-muessen-persoenlichkeitsrechte-gewahrt-bleiben-date/). Die Landesregierung folgte den Empfehlungen des LfDI und

nahm in § 12 Abs. 2 der Corona Bekämpfungsverordnung eine Bestimmung zu Attesten für den Schulbereich auf. Darin wurden Umfang der Datenanforderung bei ärztlichen Attesten und das Verbot der Anfertigung von Kopien ausdrücklich geregelt (**https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/dynamische-entwicklung-bei-attesten-fuer-maskenpflichtbefreiung-kugelmann-handlungssicherheit-fuer/**).

Zuvor hatten rheinland-pfälzische Gerichte die grundsätzliche Befugnis zur Anforderung qualifizierter Atteste bestätigt.

Corona-Schnelltests vor dem Unterricht

Mit einer Änderung des Infektionsschutzgesetzes ist eine Testpflicht für Schulen während der Pandemie eingeführt worden. Das Ministeriums für Bildung hatte die Eltern in einem Rundschreiben vom 22. April 2021 davon unterrichtet, dass die Testungen im Klassenverband stattfinden sollen, den Eltern aber die Möglichkeit eingeräumt wird, aktuelle Schnelltests von anerkannten Testzentren oder von Ärztinnen und Ärzten vorlegen zu können. Dies wurde datenschutzrechtlich in einigen Beschwerden thematisiert, da Eltern befürchteten, dass ihr Kind im Fall eines positiven Tests stigmatisiert werden könnte.

In gerichtlichen Entscheidungen wurde jedoch diese Praxis bei den Corona-Schnelltests in Schulen auch unter Datenschutzgesichtspunkten für zulässig befunden:

https://www.justiz.sachsen.de//ovgentschweb/document.phtml?id=6198

https://justiz.hamburg.de/contentblob/15012534/7607331bde5cce6a3840fce06b76f458/data/5-e-1754-21-beschluss-vom-9-4-21.pdf

Dem war auch aus Sicht des LfDI zuzustimmen, zumal das BM der Schulgemeinschaft die Möglichkeit eröffnet hatte, selbst festlegen zu können, dass die Tests zu Hause unter Aufsicht der Eltern durchgeführt werden.

11.2 Schüler-Workshops in der Pandemie

Die Datenschutz-Schülerworkshops des LfDI konnten unter Pandemiebedingungen und Schulschließungen zunächst nur in reduzierter und veränderter Form angeboten werden. Wurden bis März 2020 noch 113 Veranstaltungen regulär durchgeführt, mussten in der Folge viele Termine zunächst ausgesetzt werden. Mit der Wiedereröffnung der Grundschulen vor den Sommerferien konnten hier einige Workshops noch in entsprechend geteilten Klassen in Präsenz nachgeholt werden. Auch hier wurden bereits Anpassungen vorgenommen: So fanden aktivierende Module, die ansonsten im Klassenraum durchgeführt wurden, im Freien statt und entsprechende Partnerrechercheарbeit am Computer wurde zu Einzelrecherche am Tablet gewandelt, um entsprechende Abstände waren zu können. Zwischen den Sommerferien und den erneuten Schulschließungen im Dezember wurden wieder Workshops an Schulen aller Schulformen durchgeführt und erste Workshops als Online-Veranstaltungen im landeseigenen Videokonferenzsystem der Schulen umgesetzt.

Parallel hat der LfDI mit der Entwicklung von Online-Methoden begonnen, um die Workshops auch zukünftig – unabhängig von der Pandemiesituation – sowohl Online, wie auch in Präsenz umsetzen zu können. Insgesamt konnten von den für das Jahr 2020 beantragten 495 Workshops immerhin 291 durchgeführt werden.

Nicht unerwähnt sollte bleiben, dass das Schülerwirkshop-Projekt im September sein 10-Jähriges Bestehen feierte, wozu eine kurze Chronologie aufbereitet und ein Ausblick auf den Fortbestand und die Weiterentwicklungen gegeben wurde (**https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/10-jahre-datenschutz-schuelerworkshops-kugelmann-jedes-kind-und-jeder-jugendliche-sollte-ueber-ein/**). Die eigentlich vorgesehene Jubiläumsveranstaltung mit den Honorarkräften musste aber leider abgesagt werden.

12. MELDEWESEN

12.1 Verfahren bei der Veröffentlichung von Alters- und Ehejubiläen

Gemäß den Bestimmungen der Datenschutz-Grundverordnung (DS-GVO) ist eine Verarbeitung von personenbezogenen Daten rechtmäßig, wenn mindestens eine der in Art. 6 lit. a) bis f) genannten Voraussetzungen vorliegt. Nach Art. 6 Abs. 1 lit e) i.V.m. Abs. 3 DS-GVO ist dies der Fall, wenn die Verarbeitung, zu der auch die Veröffentlichung in einem Amtsblatt gehört, zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist und eine gesetzliche Ermächtigungsgrundlage dies erlaubt.

Für die Veröffentlichungen von Alters- und Ehejubiläen ist § 50 Abs. 2 Bundesmeldegesetz (BMG) einschlägig.

Verlangen hiernach Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde Auskunft erteilen über Familienname, Vornamen, Doktorgrad, Anschrift sowie Datum und Art des Jubiläums.

Altersjubiläen in diesem Sinne sind der 70. Geburtstag, jeder fünfte weitere Geburtstag und ab dem 100. Geburtstag jeder folgende Geburtstag; Ehejubiläen sind das 50. und jedes folgende Ehejubiläum. Leider gibt es noch immer Kommunen, die entgegen dieser Vorgaben auch „unrunde“ Geburtstage veröffentlichen. Der LfDI belässt es hier in aller Regel bei einem freundlichen Hinweis, dem sodann auch entsprochen wird.

Obwohl die Datenschutz-Grundverordnung für die Einwilligung eine aktiv bestätigende Handlung fordert, wird im Bereich des Meldewesens in Fällen der vorliegenden Art nach wie vor auf den Rechtssatz „Schweigen bedeutet Zustimmung“ abgestellt.

Betroffenen Person steht nach § 50 Abs. 5 BMG lediglich ein Widerspruchsrecht zu. Hierauf ist bei der Anmeldung nach § 17 Absatz 1 BMG sowie einmal jährlich durch ortsübliche Bekanntmachung hinzuweisen.

Unabhängig hiervon empfiehlt der LfDI Kommunen:

- Keine Veröffentlichung von Jubiläen im Internet
- Genereller Verzicht auf Veröffentlichung der Anschrift zur Vermeidung krimineller Tätigkeiten
- Datenschutzfreundlichere Variante prüfen: z.B. Veröffentlichung der genannten Jubiläen nach vorheriger Rücksprache, also mit ausdrücklicher Einwilligung der Betroffenen

12.2 Weitergabe von Meldedaten an Ortsbürgermeister

Immer wieder erreichen den LfDI Anfragen, ob Meldedaten an die ehrenamtlichen Ortsbürgermeister/innen herausgegeben werden dürfen.

Bei der datenschutzrechtlichen Beurteilung ist zunächst zu unterscheiden, ob die Daten einmalig oder regelmäßig übermittelt werden sollen.

Liegt eine einmalige, anlassbezogene Übermittlung vor, so kann § 34 Abs. 1 Bundesmeldegesetz (BMG) herangezogen werden. Dies ist dann der Fall, wenn die Datenübermittlung ausschließlich auf Abruf und in unregelmäßigen Abständen erfolgt. Regelmäßige Daten-

übermittlungen, für die wiederum § 36 BMG und die Bestimmungen in der Meldedatenlandesverordnung (MDLVO) gelten, sind dann gegeben, wenn Datenübermittlungen ohne Ersuchen in allgemein bestimmten Fällen regelmäßig wiederkehrend durchgeführt werden.

Nach § 34 BMG dürfen Meldebehörden öffentlichen Stellen im Einzelfall die in dieser Vorschrift genannten Meldedaten übermitteln. Zu den öffentlichen Stellen gehören auch die Ortsgemeinden, vertreten durch die ehrenamtlichen Ortsbürgermeisterinnen und Ortsbürgermeister (§ 2 Absatz 1 Satz 1 Nr. 4 LDSG).

Soweit es zur Erfüllung einer in der Zuständigkeit des Empfängers liegenden öffentlichen Aufgabe erforderlich ist, dürfen also bestimmte personenbezogene Daten aus dem Melderegister u.a. in Form des Namens, der Anschrift und des Geburtsdatums weiter gegeben werden. Schutzwürdige Interessen nach § 8 BMG dürfen dabei allerdings nicht beeinträchtigt werden. Dies wäre etwa dann der Fall, wenn Daten von Personen betroffen wären, für die eine Auskunftssperre eingetragen ist oder die der Übermittlung von Meldedaten für Jubiläumszwecke widersprochen haben.

Aus datenschutzrechtlicher Sicht ist jedenfalls nicht zu beanstanden, wenn den Ortsbürgermeisterinnen und Ortsbürgermeistern Meldedaten zur Verfügung gestellt werden, damit beispielsweise Seniorennachmittage organisiert werden können. Voraussetzung ist jedoch, dass es keine regelmäßigen Übermittlungen sind.

Für regelmäßige Datenübermittlungen im Sinne des § 36 BMG ist eine gesonderte Rechtsgrundlage notwendig. Diese findet sich in § 10 MDLVO wieder.

In § 10 Abs. 1 MDLVO ist eine abschließende Regelung zur regelmäßigen Übermittlung von Alters- und Ehejubiläumsdaten an die Ortsgemeinden getroffen. Nach § 10 Abs. 3 MDLVO können die Meldeämter regelmäßig auch Daten im Rahmen von Zuzügen (Anmeldungen) an die Ortsgemeinden zu übermitteln. Abmeldungen bzw. Wegzüge sind von dieser Vorschrift allerdings nicht erfasst.

Zusammenfassend ist also festzustellen, dass es datenschutzrechtlich zulässig ist, die in § 34 Abs. 1 BMG genannten Meldedaten auf Anfrage zu übermitteln, wenn dies zur Erfüllung von Aufgaben der Ortsgemeinden notwendig ist. Regelmäßige Listen für den Empfang von Neubürgern können ebenfalls unter den genannten Bedingungen an die Ortsgemeinden herausgegeben werden.

Unabhängig von der Zulässigkeit der erläuterten Datenübermittlungen ist allerdings stets zu überlegen, ob im Sinne der Datensparsamkeit und Datenminimierung nicht auch eine alternative, datenschutzfreundlichere Lösung in Frage käme. Dies ist der Fall, wenn die örtliche Meldebehörde für die Ortsgemeinde von dieser gefertigten Schreiben versendet, z.B. die Einladung zum Seniorennachmittag oder die Begrüßung von Neubürgern im Rahmen einer turnusmäßig stattfindenden Veranstaltung. Hierbei werden nämlich keine Meldedaten an die Ortsgemeinde übermittelt, so dass sich dieses Verfahren (sog. „Datenmittlung“) als vorzugswürdig darstellt.

13. VERWALTUNG DIGITAL

13.1 Einsatz von per Funk auslesbaren Wasserzählern

Bereits im 26. Datenschutzbericht 2016/2017 (IV-14.2) wurde eine datenschutzrechtliche Bewertung für die Nutzung von Funkwasserzählern durch kommunale Wasserversorger auf der Grundlage des damals bekannten Sachverhalts ausgeführt.

Bei den Wasserzählern der neuen Generation ist der Inhalt des gesendeten Datagrammes werkseitig fest definiert ist und bei der Auslese lediglich zu Abrechnungszwecken grundsätzlich nicht auf Zählernummer und –stand beschränkt. Sie verarbeiten mehr Daten, z.B. zur Feststellung von Leckagen oder zur Wahrung der Wasserhygiene, als ihre mechanischen Vorgänger und die damit verbundenen Möglichkeiten sind vielfältiger. Deshalb werden die rechtlichen Aspekte der Datenverarbeitung bei dem Einsatz dieser Wasserzähler insgesamt mit der „Gemeinsamen Erklärung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz (LfDI), des Landesverbands der Energie- und Wasserwirtschaft Hessen/Rheinland-Pfalz e.V. (LDEW) des Verbandes kommunaler Unternehmen e.V. – Landesgruppe Rheinland-Pfalz (VKU), der kommunalen Spitzenverbände Rheinland-Pfalz (Gemeinde- und Städtebund, Städtetag, Landkreistag) mit dem Fachbeirat Eigenbetriebe und kommunale Unternehmen im GStB“ ausführlich dargestellt. Die gemeinsame Erklärung ist im Internet-Angebot des LfDI unter **https://www.datenschutz.rlp.de/de/themenfelder-themen/themen-a-z/** bei den Stichworten „Kommunales“ sowie „Verwaltung digital“ abrufbar.

Als Vorlage diente die Erklärung des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) gemeinsam mit verschiedenen Verbänden. Es wurden lediglich Anpassungen an das Landesrecht RP vorgenommen.

13.2 Einsatz von videogestützter Kommunikationstechnik

Nach der Änderung kommunalrechtlicher Vorschriften, wonach im Falle von Naturkatastrophen oder anderer außergewöhnlicher Notsituationen Beschlüsse von kommunalen Gremien im Umlaufverfahren oder mittels Video- oder Telefonkonferenzen gefasst werden dürfen, und nach dem EuGH-Urteil in der Rechtssache Schrems II vom 16. Juli 2020 haben sich die Anfragen aus dem kommunalen Bereich im Hinblick auf den datenschutzkonformen Einsatz solcher Technik zu dem oben genannten Zweck gemehrt.

Diese hat der LfDI zum Anlass genommen, um gegenüber den Datenschutzbeauftragen der Kommunen klarzustellen, dass schon vor dieser EuGH-Entscheidung der Standpunkt vertreten wurde, dass es grundsätzlich vorzugswürdig ist, wenn Videokonferenzsysteme genutzt werden, die „on premises“ - also auf eigener Infrastruktur - betrieben werden können.

Bei Online-Diensten (Software-as-a-Service, SaaS) sollten Lösungen, bei denen alle Datenverarbeitungen innerhalb der EU stattfinden, und Lösungen von einem deutschen bzw. europäischen Anbieter berücksichtigt werden, bei denen die Behörden als Verantwortliche nicht die Einhaltung der Vorgaben aus Kapitel V der DS-GVO – Übermittlung personen-bezogener Daten an Drittländer – sicherstellen müssen.

Auf der Basis derzeit vorliegender Informationen kommen im kommunalen Bereich häufig Systeme zum Einsatz, die grundsätzlich datenschutzkonform betrieben werden können.

Hinsichtlich eines beabsichtigten Einsatzes von Online-Diensten US-amerikanischer Anbieter werden die Kommunalverwaltungen immer darauf hingewiesen, dass selbst wenn die Verwaltung mit einem solchen Anbieter vereinbaren können sollte, dass alle Datenverarbeitungen (weitgehend) innerhalb der EU stattfinden, die Verwaltung belegen können muss, dass der ausgewählte Dienstleister mit Transferproblematik kurz- und mittelfristig unersetzlich ist durch einen zumutbaren Dienstleister ohne Transferproblematik.

13.3 Parkraumbewirtschaftung am ICE-Bahnhof

Mehrere Pendler hatten sich über die Datenverarbeitung mit der zu diesem Zweck installierten schrankenlosen Anlage beschwert. Sie erfasst bei der Einfahrt auf die bewirtschaftete Parkplatzfläche automatisch das Kfz-Kennzeichen und verknüpft dieses mit einem Zeitstempel.

Für den Bezahlvorgang muss das Kennzeichen am Kassenautomat eingegeben werden. Auf dem Display des Kassenautomaten wird dann die Aufnahme zur Kennzeichenerfassung bei der Einfahrt, der Zeitstempel zur Einfahrt, die aktuelle Uhrzeit und der Rechnungsbetrag angezeigt.

Von den Beschwerdeführern wurde problematisiert, dass jeder ein beliebiges Kennzeichen eines parkenden Fahrzeuges eingeben kann und ebenfalls die oben genannten Daten zu dem fremden Fahrzeuges angezeigt erhält.

Die Verbandsgemeindeverwaltung hat u.a. vorgetragen, dass die oben genannten Daten zu einem beliebigen Fahrzeug nach dem Bezahlvorgang bzw. dem Verlassen des bewirtschafteten Parkraumes für Dritte nicht mehr abrufbar sind. Weiterhin ist ein Fahrer bzw. eine Fahrerin auf der Aufnahme zur Kennzeichenerfassung nicht erkennbar. Schließlich hat bei der Entscheidung für eine Bewirtschaftung mit Kennzeichenerfassung die Wirtschaftlichkeit im Vordergrund gestanden, damit das Parken für Pendler so kostengünstig wie möglich gestaltet werden kann.

Für das Parken auf öffentlichen Wegen und Plätzen können die Gemeinden Gebühren erheben (§ 6a Abs. 6 S. 1 Straßenverkehrsgesetz, StVG; Gebührenordnung der Kommune). Auch wenn im Vergleich zu der Parkraumbewirtschaftung mit Parkscheinautomaten mit dem hier eingesetzten Parkabfertigungssystem durch die problematisierte Aufrufbarkeit von Kennzeichen über das Display am Kassenautomat eine höhere Intensität des Eingriffes einhergeht, fällt die Abwägung zu Gunsten der Interessen der Verwaltung, aber auch gleichzeitig aller Pendler im Hinblick auf ein kostengünstige Parkmöglichkeit aus. D.h. der Eingriff in das Persönlichkeitsrecht des einzelnen Pendlers bleibt aus datenschutzrechtlicher Sicht akzeptabel. Diesem Ergebnis liegt eine Abwägung der sich gegenüberstehenden schutzwürdigen Interessen der Nutzer des Parkraumes als betroffene Personen einerseits und den anzuerkennenden Zwecken der Verwaltung als Verantwortliche der Festsetzung von Benutzungsgebühren andererseits zugrunde. Folgende Gesichtspunkte und Überlegungen haben eine Rolle gespielt:

- Der Informationsgehalt der Daten. Es werden Merkmale verarbeitet, über die eine Person nicht direkt identifizierbar ist. Ein Rückschluss auf eine Person ist nur über Zusatzwissen möglich.

- Die rechtlich zulässigen Identifizierungsmöglichkeiten und das Identifizierungsinteresse der den Parkplatz nutzenden Pendler und somit das Interesse an dem Erwerb von Zusatzwissen zur Identifizierung einer Person sind gering.

- Es genügt eine grundsätzliche Datensparsamkeit, ohne dass die Verbandsgemeindeverwaltung als Verantwortliche die Verarbeitungsweise wählen muss, die absolut mit der geringsten Menge an personenbeziehbaren Daten auskommt.

- Das mitstreitende Interesse der Verwaltung, das Parken für Pendler so kostengünstig wie möglich zu gestalten.

- Es besteht eine Ausweichmöglichkeit, d.h. es können weitere im Umfeld des ICE-Bahnhofes zur Verfügung stehende Parkplätze in Anspruch genommen werden.

Als Ergebnis ist daher festzuhalten, dass ein Datenschutzverstoß nicht vorliegt. Die für die Erhebung von Gebühren notwendige Verarbeitung von Kennzeichen, Zeitstempel zur Einfahrt und die aktuelle Uhrzeit auch über das Display eines Kassenautomaten ist zulässig.

14. RECHTSDURCHSETZUNG

Das Jahr 2020 war durch Einschränkungen aufgrund der Corona-Pandemie geprägt. So wurden insbesondere mündliche Verhandlungen in Gerichtsverfahren durch das Gericht verschoben. Dennoch machte der LfDI auch in diesem Jahr weitreichend von seinen Befugnissen Gebrauch.

Verantwortliche und Auftragsverarbeiter sind grundsätzlich verpflichtet, auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen zu arbeiten. Informationsersuchen sind unabdingbar, um die Sachverhalte zu ermitteln und dem Anliegen der Beschwerdeführer gerecht zu werden. Da jedoch nicht alle Verantwortlichen sofort ihren Mitwirkungspflichten nachkamen, wurde in 61 Fällen ein Zwangsgeld von durchschnittlich 500,00 € angedroht. In 18 Fällen mussten die Zwangsgelder auch festgesetzt werden. In 8 Fällen wurde gegenüber Verantwortlichen eine Anweisung erlassen und in 68 Fällen eine Verwarnung ausgesprochen. Ein besonderes Augenmerk wurde hier auf die datenschutzkonforme Beauskunftung nach Art. 15 DS-GVO gelegt. Im öffentlichen Sektor kam es in 30 Fällen zu einer Beanstandung. Meistens ging es dabei um eine unberechtigte Weitergabe personenbezogener Daten.

Im Jahr 2020 wurden 11 Bußgelder erlassen. Dabei reichten die Vorwürfe vom unzureichenden Schutz von Patienten- bzw. Mandantendaten über die Videoüberwachung Beschäftigter bis hin zu unberechtigten Datenbankabrufen durch Beamte oder dem unzulässigen Einsatz von Dashcams. Auch an der bundesweiten Vereinheitlichung der Bußgeldverfahren wurde weitergearbeitet. Dieser Bereich wird auf nationaler wie auch auf europäischer Ebene weiter intensiv diskutiert und weiterentwickelt.

Mit dem zunehmenden Erlass von Abhilfebefugnissen gegenüber den Verantwortlichen und der großen Zahl der Beschwerdeverfahren ging es einher, dass zahlreiche Sachverhalte zum Gegenstand von Gerichtsverfahrens wurden. Im Jahr 2020 wurde gegen den LfDI in 19 Fällen Klage erhoben. Gerade diejenigen Verfahren, in denen ein Beschwerdeführer sich gegen die Beendigung seines Verfahrens wendete (da ein Datenschutzverstoß nicht festgestellt werden konnte), hat der LfDI für sich entschieden. Hier ist auf die Entscheidung des OVG Koblenz vom 26. Oktober 2020 (Az. 10 A 10613/20.OVG) zu verweisen. Das Gericht hat den gerichtlichen Prüfungsumfang in Bezug auf die Beschwerdeentscheidungen der Aufsichtsbehörde (Art. 57 Abs. 1 Buchst. f DS-GVO) dahingehend konkretisiert, dass die Aufsichtsbehörde gemäß Art. 77 DS-GVO verpflichtet ist, sich nach Art. 57 Abs. 1 Buchst. f DS-GVO mit der Beschwerde zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten. Eine weitergehende gerichtliche Überprüfung, ob die Beschwerdeentscheidung der Aufsichtsbehörde auch inhaltlich zutreffend ist, sehen die Regelungen der Datenschutz-Grundverordnung nicht vor. Ein Anspruch auf eine konkrete Maßnahme (z.B. den Erlass eines Bußgeldbescheides) besteht ebenfalls nicht

ABKÜRZUNGSVERZEICHNIS

Aufsichts- und Dienstleistungsdirektion	ADD
Amtsgericht	AG
Bundesdatenschutzgesetz	BDSG
Bundesinstitut für Arzneimittel und Medizinprodukte	BfArM
Bundesgerichtshof	BGH
Bundesmeldegesetz	BMG
Corona-Bekämpfungsverordnung Rheinland-Pfalz	CoBeLVO
Digitale-Gesundheitsanwendungen-Verordnung	DiGAV
Datenschutzkonferenz	DSK
Datenschutz-Grundverordnung	DS-GVO
Digitale-Versorgung-Gesetz	DVG
Digitale-Versorgungs- und Pflege-Modernisierungs-Gesetz	DVPMG
Elektronische Patientenakte	ePA
Europäische Union	EU
Fahreignungsregister	FAER
Gemeindeordnung	GemO
Der Hessische Beauftragte für Datenschutz und Informationsfreiheit	HBDI
Infektionsschutzgesetz	IfSG
Verordnung zu öffentlichen Bekanntmachungen in Insolvenzverfahren im Internet	InsoBekV

Justizvollzugsanstalt	JVA
Landesverband der Energie- und Wasserwirtschaft Hessen/Rheinland-Pfalz e V.	LDEW
Landesdatenschutzgesetz Rheinland-Pfalz	LDSG
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz	LfDI
Landkreisordnung	LKO
Landesjustizvollzugsdatenschutzgesetz	LJVollzDSG
Ministerium für Soziales, Arbeit, Gesundheit und Demografie Rheinland-Pfalz	MSDAG
Norddeutscher Rundfunk	NDR
Software as a Service	SaaS
Sozialgesetzbuch	SGB
Steuerberatungsgesetz	StBerG
Telemediengesetz	TMG
Technische Werke Ludwigshafen am Rhein AG	TWL
Verband kommunaler Unternehmen e.V.	VKU
Wohnungseigentümergemeinschaft	WEG
Zentrale Bußgeldstelle	ZBS

Hintere Bleiche 34 | 55116 Mainz
Postfach 3040 | 55020 Mainz

Telefon +49 (0) 6131 8920 - 0
Telefax +49 (0) 6131 8920 - 299

poststelle@datenschutz.rlp.de