Datenschutz + Digitalisierung = nachhaltige Entwicklung

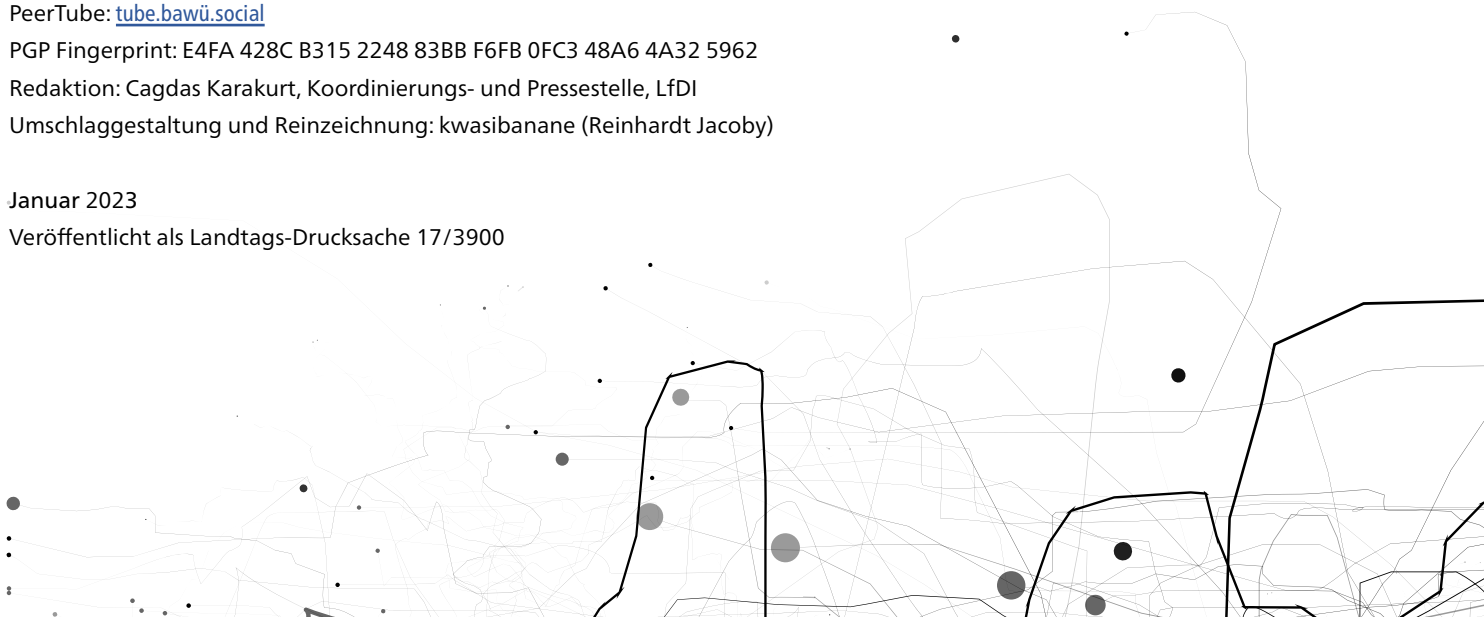
Unsere Freiheiten:
Daten nützen – Daten schützen

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Tätigkeitsbericht
Datenschutz 2022

Herausgegeben von
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit
Dr. Jan Ulrich Wacke, Leitender Beamter
Lautenschlagerstraße 20, 70173 Stuttgart
Telefon: 0711/615541-0
Telefax: 0711/615541-15
www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de
Mastodon: bawü.social/@lfdi
PeerTube: tube.bawü.social
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Redaktion: Cagdas Karakurt, Koordinierungs- und Pressestelle, LfDI
Umschlaggestaltung und Reinzeichnung: kwasibanane (Reinhardt Jacoby)

Januar 2023
Veröffentlicht als Landtags-Drucksache 17/3900



38. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2022

Inhalt

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Vorwort


© K. Schmid

Dr. Jan Ulrich Wacke

Mit dem Ende des Jahres 2022 endete auch die Amtszeit von Dr. Stefan Brink als Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg. Daher obliegt es mir als Leitendem Beamten der Dienststelle bis zur Ernennung einer neuen Amtsträgerin oder eines neuen Amtsträgers, die Rechte und Pflichten des Landesbeauftragten kommissarisch wahrzunehmen.

Nach den Jahren 2020 und 2021, in denen unsere Behörde maßgeblich mit den der Bewältigung der Corona-Pandemie dienenden Maßnahmen und Grundrechtseingriffen befasst war, ließ die Dominanz dieses Themas im Laufe des Jahres 2022 infolge der rückläufigen pandemischen Entwicklung deutlich nach. Zwar hatten wir uns noch immer mit herausfordernden pandemiebedingten Sonderfragen wie etwa der Umsetzung der sogenannten einrichtungsbezogenen Impfpflicht auseinanderzusetzen. Gleichwohl nahmen auch Zahl und Intensität der Grundrechtseingriffe ab. Diese begrüßenswerte und konsequente Entwicklung begleiteten wir, unter anderem indem wir bei verschiedenen Verantwortlichen nachprüften, inwieweit sie nunmehr nicht mehr erforderliche zu Infektionsschutzzwecken erhobene Daten auch tatsächlich nicht mehr vorhalten, und indem wir auch mit der Landesregierung das Gespräch über die Notwendigkeit weiterer coronabedingter Regelungen suchten. Zum gegenwärtigen Zeitpunkt zeichnet sich ab, dass in Kürze beinahe alle derartigen Sonderregelungen aufgehoben werden könnten.

Durch den Rückgang der Belastungen durch die Pandemie konnten wir uns wieder vermehrt weiteren Themen intensiver zuwenden. Der durch die Pandemie erfolgte Digitalisierungsschub in der Gesellschaft ist nicht zu verkennen. Ebenso sahen wir ein verstärktes Interesse an der Gesundheitsforschung. Wir griffen beide Entwicklungen auf: In unserer Woche zur Künstlichen Intelligenz luden wir Fachleute aus Wissenschaft, Wirtschaft, Politik, Philosophie und Kultur in unsere Räume, um mit ihnen, unseren Besucher_innen und den Online beiwohnenden Interessierten die Chancen und Risiken dieser faszinierenden Technologie für unsere Freiheiten aus verschiedenen Perspektiven zu beleuchten. Wir unterstützten die Landesregierung bei verschiedenen Digitalisierungsprojekten und berieten Forschende und Start-ups, wie sie ihre jeweiligen Vorhaben datenschutzkonform umsetzen können.

Zugleich bauten wir unser Fortbildungsangebot über das BIDIB weiter aus, sprachen etwa mit vielen Interessierten darüber, wie es uns gelingen kann, auch in der digitalen Welt als Bürger_innen souverän zu handeln. Dank mehrerer Stellen, die der Landtag uns dankenswerter Weise bis Ende 2024 bewilligte, konnten wir zu dem wichtigen Thema des Datenschutzes an Schulen eine ganze Reihe sehr gut angenommener Fortbildungen für Schulleitungen, Lehrkräfte, Schulsekretariate, Eltern und Schülervertreter_innen anbieten und auch Schüler_innen für den Datenschutz sensibilisieren.

Wir engagierten uns weiterhin in der Zusammenarbeit der europäischen und deutschen Datenschutzbehörden, veranstalteten einen Datenschutzwettbewerb und präsentierten unsere Datenschutz-Icons, mit den Datenschutzhinweise übersichtlicher und damit bürgerfreundlicher werden können. Durch unsere Teilnahme an der Langen Nacht der Museen konnten wir viele jungen Menschen auf unsere Arbeit aufmerksam machen – und wir tauschten uns mit Datenschutzfachleuten auf der BvD-Herbstkonferenz in Stuttgart aus.

Dieses vielfältige Spektrum an Tätigkeiten konnten wir nur durch das großartige Engagement der Mitarbeiter_innen unseres Hauses bewältigen, denen ich sehr herzlich danke.

Der Abschied von Stefan Brink gebietet einen kurzen Rückblick: In den sechs Jahren seiner Amtszeit hat Stefan Brink viele Impulse gesetzt und zugleich einen kooperativen und Freiräume lassenden Führungsstil gepflegt. Er hat unsere Behörde in die Zeit der Geltung der europäischen Datenschutz-Grundverordnung überführt und enorm weiterentwickelt. Dafür gebührt ihm großer Dank. Wir haben uns in den Europäischen Kontext eingebunden und uns als Behörde weiter geöffnet. Wir nehmen an relevanten gesellschaftlichen Debatten über die informationelle Selbstbestimmung teil, sind eine lernende Organisation und geben unser Wissen weiter. Unsere Behörde ist heute ein Zentrum für die modernen Bürgerrechte Datenschutz und Informationsfreiheit, und das vom Landtag stark unterstützte, im Jahr 2020 gegründete Bildungszentrum BIDIB ist einzigartig in Deutschland erfreut sich großer Nachfrage.

Gemeinsam mit den Mitarbeiter_innen der Behörde wird auch eine gute Gestaltung der nunmehr zunächst anstehenden Übergangsphase gelingen, bis unser Haus wieder durch eine neue Person im Amt der oder des Landesbeauftragten vervollständigt ist.

Ich danke auch den Abgeordneten des Landtags für ihre Unterstützung und Förderung unserer Arbeit. Ebenfalls danken möchte ich der Landesregierung sowie der Landesverwaltung und den Kommunen für die konstruktive Zusammenarbeit im vergangenen Jahr.

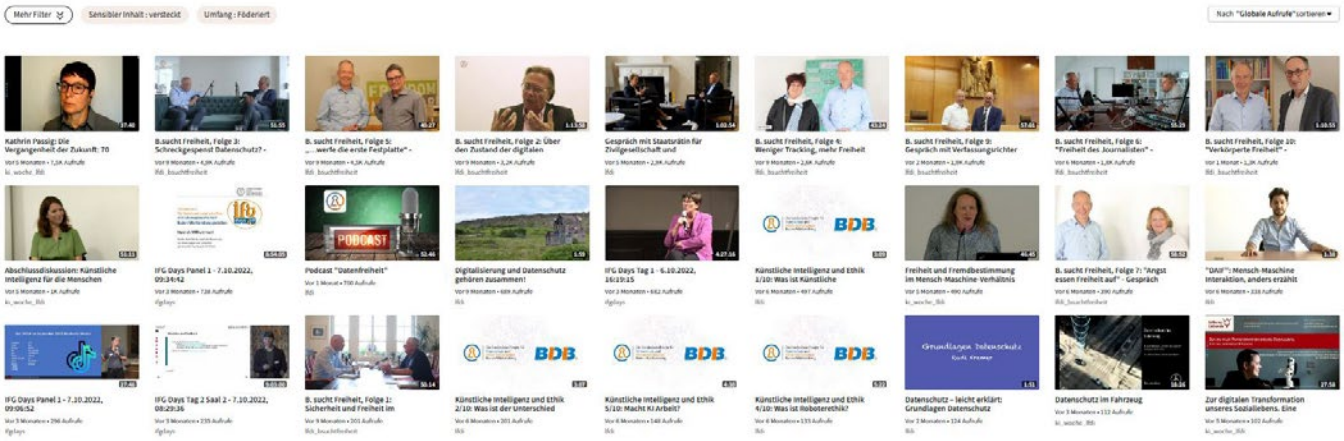
Ihr

Dr. Jan Ulrich Wacke

☛ Über 90 aktive Accounts von öffentlichen Stellen und Stellen mit Bezug zu öffentlichen Aufgaben sind mittlerweile auf der LfDI-Instanz Mastodon: bawü.social

Viele öffentliche Stellen aus Baden-Württemberg nutzen eine datenschutzfreundliche digitale Kommunikationsplattform. Auf der Mastodon Instanz des LfDI aktiv sind u.a.: das Staatsministerium, das Finanzministerium, das Sozialministerium, das Verkehrsministerium, das Wirtschaftsministerium, das Umweltmnisterium, das Kultusministerium, Der Beauftragte der Landesregierung Baden-Württemberg gegen Antisemitismus, Dr. Michael Blume, die Städte Freiburg, Friedrichshafen, Ulm, Stuttgart, Laupheim und Reutlingen, die Hochschule der Medien Stuttgart, die Universität Freiburg, der Fahrradbeauftragter der Universität Hohenheim, die Universität Tübingen – insgesamt sind etwa über 35 Hochschulaccounts auf der Instanz aktiv –, die Landeszentrale für politische Bildung, die Verbraucherzentrale Baden-Württemberg, das Fraunhofer ISI, die Städtischen Museen Freiburg, das Badische Landesmuseum, das Regierungspräsidium Freiburg, die Forstliche Versuchs- und die Forschungsanstalt Baden-Württemberg, der Naturpark Schwarzwald und viele weitere Einrichtungen, Städte und Gemeinden sowie Hochschulen.

☛ Besuchen Sie uns auf PeerTube: tube.bawü.social



© LfDI BW

Kommunen, Städte und Landratsämter sind laufend mit den Bürger_innen vor Ort in Kontakt. Auf der lokalen Ebene leisten die kommunalen Beschäftigten unmittelbar Dienst für die Bürgerschaft. Dabei werden auch viele personenbezogene Informationen aufgenommen, eingetragen, zusammengeführt und an andere Stellen übermittelt. Das bedeutet: Fast in jedem kommunalen Arbeitsschritt muss auch an den Datenschutz gedacht werden. Dass der Schutz der personenbezogenen Daten nicht bürokratisch-kompliziert sein muss, sondern am besten leicht und gut integriert funktioniert, haben sechs öffentliche Stellen im Rahmen unseres ersten Kommunalen Datenschutzwettbewerbs mit ihren vorbildlichen Ideen gezeigt – und wurden von einer Fachjury mit Vertreter_innen der kommunalen Spitzenverbände unter dem Vorsitz des LfDI ausgezeichnet: die Großen Kreisstädte Böblingen und Laupheim, die Landratsämter Calw, Konstanz, Neckar-Odenwald-Kreis und die Stadt Knittlingen. Auf dem Bild v.l.n.r. Jurymitglieder_innen und Preisträger_innen: Städtetag-BW Dezernent Norbert Brugger; LfDI Stefan Brink; Gemeindetags-Dezernentin Heidi Schmid; A. Kohl vom Landratsamt Konstanz; T. Gernoth-Laber vom Landratsamt Necker-Odenwald-Kreis; S. Ege von der Stadt Böblingen; Bürgermeister der Stadt Knittlingen Alexander Kozel; P. Retzbach vom Landratsamt Calw.

1. Datenschutz + Digitalisierung = nachhaltiger Fortschritt

Digitalisierung hat schon heute unsere Lebensweise grundlegend verändert. Wer mit Blick darauf die letzten Jahrzehnte einmal Revue passieren lässt, wird gewahr, wie stark die Digitalisierung als eine der maßgeblichen Entwicklungslinien uns alle beeinflusst hat und noch weiter prägt. Die Selbstverständlichkeit, mit der heute über das Internet Informationen eingeholt, Meinungen ausgetauscht und Vertragsbeziehungen eingegangen werden und mit der uns digitale Geräte wie das Smartphone alltäglich begleiten, sind in der Rückbetrachtung nur besonders augenfällige Beispiele. Dabei hat die Corona-Krise, die unserer Behörde mit Blick auf die zu ihrer Bewältigung vorgenommen Grundrechtseinschränkungen in den Jahren 2020 und 2021 stark in Anspruch genommen hat (s. auch Kapitel 2), der Digitalisierung erst kürzlich nochmals einen enormen Schub verliehen.

Die Entwicklung in der Digitalisierung ist noch lange nicht abgeschlossen und wird vermutlich nie zu einem Stillstand kommen. Digitalisierung vereinfacht das Leben, beschleunigt Abläufe, vermehrt unser Wissen und unsere Welterkenntnis, schafft damit neue wirtschaftliche Werte, sie kann Benachteiligte unterstützen und ermöglicht weltweite Kommunikation – sie erweitert unserer Handlungsmöglichkeiten und damit unsere Freiheiten.

Digitalisierung kann aber auch Risiken und Nebenwirkungen für unsere Freiheiten bergen. Die zunehmenden technischen Möglichkeiten können – je nach Zielrichtung ihres Einsatzes – zu immer weiteren Methoden der Überwachung führen. Auch wenn Digitalisierung nicht primär zu solchen Zielen eingesetzt wird, können die dabei anfallenden Daten – soweit sie auf Personen bezogen werden können – zu überschießenden Kontrolltendenzen und Profilbildung führen, die uns in der Ausübung unserer Grundrechte und Freiheiten massiv beeinträchtigen können. Die Gefahr des Missbrauchs besteht dabei nicht nur durch die jeweiligen Verantwortlichen selbst, sondern auch durch Angriffe Dritter. Solche potentiellen negativen Auswirkungen können umso gravierender sein, je weniger transparent Umfang, Zwecke, Zugriffsmöglichkeiten und Verantwortlichkeiten im Rahmen der Digitalisierung sind und je weniger Möglichkeiten die betroffenen Personen haben, über souveräne Entscheidungen Einfluss auf die Verarbeitung der sie betreffenden Daten auszuüben.

Zum angemessenen Umgang mit diesen Risiken und Nebenwirkungen sind die Regelungen des Datenschutzes, wie sie insbesondere in der seit 2018 geltenden der Datenschutz-Grundverordnung (DS-GVO) europaweit einheitlich niedergelegt sind, der richtungsweisende, technikoffene Maßstab. Datenschutz erweist sich mithin gerade bei zunehmender Digitalisierung als immer wichtiger werdender Garant unseres freiheitlichen demokratischen Zusammenseins auch in der digitalen Welt.

Dabei setzt das Datenschutzrecht die informationelle Selbstbestimmung nicht absolut, sondern sieht sie von vornherein im Kontext zu anderen Grundwerten der freiheitlichen Gesellschaftsordnung.

So formuliert etwa der Erwägungsgrund 4 zur DS-GVO:

„Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden."

Mit anderen Worten wahrt Datenschutz als modernes Bürgerrecht notwendige Freiräume, die Regelungen der DS-GVO erlauben indes auch, personenbezogene Daten zu verarbeiten, wo es zur Verfolgung legitimer Zwecke angemessen und erforderlich oder wo es vom Betroffenen individuell erwünscht ist.

Das bedeutet aber auch, dass es für eine für eine richtige datenschutzrechtliche Einschätzung entscheidend ist, sich mit den Chancen der Digitalen Entwicklung auseinanderzusetzen und die Ziele der sie Entwickelnden und derjenigen, die neue digitale Mittel einsetzen wollen, zu erkennen, nach-

zuvollziehen und zu würdigen. Erst dann sind die Risiken zu erkennen und einzuschätzen, angemessene Lösungen zu ihrer Vermeidbarkeit oder Minimierung zu suchen und etwaige verbleibende Risiken in ihrem Verhältnis gegen die verfolgten Ziele des Einsatzes abzuwägen.

Dieser umfassende Vorgang hat zur Folge, dass wir als Datenschützer_innen mit allen Akteur_innen ins Gespräch kommen müssen und wollen: Wir müssen den Kontakt mit den verantwortlichen Stellen halten, um die Ziele der von ihnen gewünschten Verarbeitung zu verstehen und zu erörtern, welche Handlungsalternativen es gibt. Dabei geht es auch darum, die Praktikabilität solcher Alternativen und zusätzlicher Schutzmaßnahmen auszuloten. Datenschutz ist aber idealer Weise nicht erst bei der Entscheidung über digitale Tools zu berücksichtigen, sondern – um ungünstige Vorfeldfestlegungen zu vermeiden, deren spätere Beseitigung ungleich schwerer wird – schon frühzeitig bei der Entwicklung und Forschung. Deswegen haben wir auch im vergangen Jahr explizit den Austausch (siehe Kapitel 1.2, 1.3.,1.4, 1.5) mit Verantwortlichen, Entwickelnden und Forschenden gesucht – z. B. bei Kommunen hospitiert und eine Woche zu künstlicher Intelligenz veranstaltet.

Der Austausch muss aber auch in andere Richtungen erfolgen (siehe Kapitel 1.1): Er muss vor allem auch die betroffenen Bürger_innen einbeziehen, und hier war und ist es uns ein Anliegen, mit ihnen intensiv ins Gespräch zu kommen, z. B. über moderne, datenschutzkonforme soziale Medien – auf Mastodon folgen uns mittlerweile über 6.000 Accounts (siehe Kapitel 10) – und unseren zahlreichen offenen Veranstaltungen, mit denen wir sie wo möglich – wie etwa im Rahmen der Langen Nacht der Museen (siehe Kapitel 6) – auch in unsere Räume einladen. Durch die vielen Fortbildungen, die wir über unser Bildungszentrum (siehe Kapitel 5) anbieten, wollen wir nicht nur die Kenntnis datenschutzrechtlicher Anforderungen bei den Verantwortlichen verbessern, sondern auch die Bürger_innen über vorgenommene Datenverarbeitungen und auf ihre Rechte und Entscheidungsmöglichkeiten informieren, um so ihre Souveränität in der Ausübung ihrer Freiheit zu stärken.

Darüber hinaus wollen wir aber auch den Blick auf die gesellschaftliche Wirkung der Digitalisierung und die Bedeutung der Grundrechte richten. Eine derartige Reflektion kann nicht ohne Berücksichtigung kultureller Impulse und ethischer Fragen erfolgen. Datenschutz ist und bleibt aus unserer Sicht auch eine Kulturaufgabe (siehe Kapitel 7). Denn wir sind davon überzeugt, dass nur Datenschutz und Digitalisierung gemeinsam eine nachhaltige Entwicklung bewirken können.

Praktische Unterstützung für Bürger_innen und verantwortliche Stellen

Einige Beispiele sollen stellvertretend für den nachhaltigen Ansatz unseres Hauses stehen: Wir haben Bürger_innen mit Schulungen in unserem Bildungszentrum dabei unterstützt, sich mit einem souveränen Umgang der Digitalisierung zu befassen (Kap. 1.1). Wir haben mit Kommunen zusammengearbeitet, einen Datenschutzwettbewerb ausgerufen und sind zu Hospitationen vor Ort gewesen, um die alltägliche Praxis vor Ort noch besser nachzuvollziehen und die Herausforderungen der Fachleute vor Ort zu verstehen (Kap. 1.2). Mit der E-Akte haben wir uns befasst, an der exemplarisch sichtbar wird, wie sehr Digitalisierung und Datenschutz zusammengehören (1.3). Im Bereich der Nutzung von Gesundheitsdaten haben wir Beratungsleistung zur Verfügung gestellt, um daran mitzuwirken, dass medizinische Versorgung datenschutzkonform weiterentwickelt werden kann (1.4). Wir haben eine Themenwoche zu Künstlicher Intelligenz organisiert, um neue Erkenntnisse und einen gesellschaftlichen Diskurs zu fördern. Diese Erkenntnisse haben wir mit der Bürgerschaft geteilt und auch in unser künftiges Beratungsangebot aufgenommen (1.5).

1.1 Austausch mit Bürger_innen

In Jahr 2022 verzeichneten wir einen Rekord: Über 3.200 Menschen interessierten sich für unsere Veranstaltungen. Unser Fortbildungsprogramm „Schule digital" erfreute sich eines herausragenden Interesses. Darüber hinaus haben wir zahlreiche Veranstaltungen für Bürger_innen organisiert – etwa die Reihe „Digitale Selbstverteidigung" eingeführt und etabliert. Wir fingen an mit „Eine Reise durch den Messenger-Dschungel", es folgte „Horch! Was kommt von drinnen raus? Über die Kommunikationsfreudigkeit mobiler Endgeräte". Wir widmen uns der alltäglichen Praxis, nehmen Themen auf, die immer wieder auftauchen. Das Smartphone ist unbestrittener Bestandteil des Alltags sehr vie-

ler Menschen – Veranstaltungen dazu, was digitale Endgeräte und Softwareanbieter tatsächlich alles können, interessieren viele.

Es folgte die Veranstaltung „Digital souverän bleiben, aber wie?“ mit dem renommierten IT-Sicherheitsexperten Manuel Atug; als HonkHase ist er im Internet bekannt und immer dann auf dem Plan, wenn Sicherheitsdefizite erkennbar sind in der IT Infrastruktur. In Jahr 2022 war Atug zuletzt medial extrem präsent – offenbar ist das Thema IT Sicherheit virulent.

Die Resonanz auf die Reihe war sehr erfreulich und wird im Jahr 2023 fortgeführt. Fatalismus und Pauschalismus im Zusammenhang mit Digitalisierung und Anbietern von Technologien in der digitalen Welt führen dazu, dass sich Bürger_innen von der Entwicklung entkoppeln und diese nicht mehr mitgestalten. Wir arbeiten aktiv für mehr Partizipation.

Die DS-GVO will, dass wir uns um die Anliegen der Bürger_innen kümmern, wenn uns ihre Eingaben erreichen. Wir ergreifen Partei für die Bürgerrechte. Art. 57 der DS-GVO trägt uns auf, dass wir informieren, sensibilisieren, beraten und an den Debatten über Datenschutz teilnehmen.

Manchmal gehen wir dabei auch neue Wege. Wir haben im vergangen Jahr an der Langen Nacht der Museen teilgenommen – es war ein großer Erfolg. Etwa 3.000 Menschen interessierten sich für uns und unser Programmangebot. Manche warfen nur einen kurzen Blick auf den „Neuling“ Aufsichtsbehörde, andere hatten Spaß an der Freude und blieben länger. Wir hatten ein tollen Programm, eine herausragende und als „Instagram-kompatibel“ attestierte Lichtinstallation. Auch als Datenschützer verstehen wir dies als Kompliment. Teil des attraktiven Programms waren Kurzvorträge unserer Kolleg_innen aus dem Haus – etwa zu Tracking und Cookies und zu Videoüberwachung auf öffentlichen Plätzen. Die Vorträge waren sicher weniger Instagram-tauglich, erfuhren aber eine sehr gute Resonanz. Auffällig viele junge Menschen schauten bei uns vorbei.

Choose your guide: Die etwas andere Stadttour mit Studierenden

Apropos neue Wege: Im Wintersemester 2021/2022 widmete sich ein Hauptseminar an der Universität Stuttgart unter dem Titel „Surveillance. Techniken, Praktiken und Diskurse der Überwachung“ dem Thema Überwachung. Im Rahmen der Lehrveranstaltung wandten sich Studierende an

© LfDI BW

„Digital souverän bleiben, aber wie?“ IT-Sicherheitsexperte Manuel Atug (rechts) war zu Gast im Bildungszentrum BIDIB, seine Bürger_innenveranstaltung lockte knapp 100 Neugierige zu uns. BIDIB-Leiter Frank Feucht (Mitte) war sichtlich zufrieden, und der Leiter der Abteilung Technisch-Organisatorischer Datenschutz, Datensicherheit beim LfDI Alvar Freude (links) gesellte sich dazu und beantwortete zusammen mit Manuel Atug zahlreiche Fragen der Teilnehmenden.

uns und baten um Begleitung bei einer geplanten Exkursion und Diskussion.

Erste Abstimmungen erfolgten per Videokonferenz. Schon bald konnten die Vorschläge und Wünsche der Studierenden in die Realität umgesetzt werden. An einem sonnigen Nachmittag im Januar unternahmen unsere Fachreferent_innen mit einer Gruppe Studierender und der Hauptseminarleiterin einen Ausflug durch die Stuttgarter Innenstadt. Wir suchten gemeinsam verschiedene Standorte auf, an denen Videotechnik zu Überwachungszwecken zum Einsatz kommt. Hier ging es um die offene Videoüberwachung durch private Stellen, aber auch durch öffentliche Stellen. Wir informierten hierbei über die jeweiligen Zulässigkeitsvoraussetzungen und die zur Erfüllung der datenschutzrechtlichen Informationspflichten erforderliche Hinweisbeschilderung. Die Exkursion endete mit einem Gespräch zu Fragen des Einsatzes von Videotechnik durch öffentliche Stellen.

Die Seminarreihe endete mit einer virtuellen Abschlussveranstaltung, in welcher zum einen noch einmal die verschiedenen datenschutzrechtlichen Regelungen auf europäischer, nationaler und landesrechtlicher Ebene aufgezeigt sowie andere datenschutzrelevante Themen angesprochen wurden. Aus der anschließenden Fragerunde mit unterschiedlichsten Fragen, die im Rahmen des Hauptseminars aufgekommen waren, entwickelte sich eine interessante Diskussion. Der interdisziplinäre Austausch mit Studierenden verschiedener Studiengänge war für uns eine wertvolle Erfahrung. Wir nehmen auch künftig gerne an solchen Veranstaltungen teil.

1.2 Austausch mit Behörden

Die Verwaltung in den Kommunen und Landratsämter ist ständig in Kontakt mit Bürger_innen vor Ort. Dabei werden auch viele personenbezogene Informationen aufgenommen, eingetragen, zusammengeführt und an andere Stellen übermittelt. Das bedeutet: Fast in jedem kommunalen Arbeitsschritt muss auch an den Datenschutz gedacht werden. Gerade in Kommunen, dort, wo auf lokaler Ebene Dienst für die Bürgerschaft geleistet wird und das alltägliche Leben stattfindet, werden also auch viele personenbezogene Daten verarbeitet.

Hospitationen bei öffentlichen Stellen

Im Sommer dieses Jahres besuchten in Umsetzung des in der Einleitung skizzierten Austauschgedankens zwei unserer Referentinnen ein Landratsamt und eine Stadt in Baden-Württemberg. Zwei Wochen haben sie aus nächster Nähe gesehen, wie der Alltag eines behördlichen Datenschutzbeauftragten (DSB) aussieht, wo der Schuh (noch) drückt beziehungsweise wo es schon rund läuft, und wo und wie wir noch unterstützen können. Das Ergebnis:

Beliebt auch im vergangenen Jahr: Das LfDI-Tool DS-GVO.clever. Vereine und kleinere Unternehmen können damit in sehr kurzer Zeit Datenschutzhinweise für ihre Homepage erstellen. Das Tool steht auf der Homepage des Landesbeauftragten.

Wir haben jede Menge gute Ideen und Eigeninitiative gesehen, aber auch an der einen oder anderen Stelle noch etwas Optimierungsbedarf.

Für behördliche Datenschutzbeauftragte in den Kommunen und Landratsämtern ist der Arbeitsalltag eine echte Herausforderung: Als Einzelperson, oftmals nicht mit einer 100%-Stelle in dieser Funktion, müssen sie in der Regel innerhalb kurzer Zeit sehr unterschiedliche Datenschutzfragen beantworten. Dort meldet sich zuerst das Jugendamt, dann die Waffenbehörde und dann noch die IT-Abteilung – ob man sich „mal kurz" diese Auftragsverarbeitungsvereinbarung ansehen könne. Dass Datenschutzfragen regelmäßig Abwägungsentscheidungen sind, vereinfacht die Sache auch nicht unbedingt. Datenschutzbeauftragte – und insoweit meinen wir alle behördlichen und betrieblichen Datenschutzbeauftragten – sind somit auch im fünften Jahr der DS-GVO weiterhin wichtig und tragen entscheidend zur Beratung der verantwortlichen Stellen und somit zum Schutz der Freiheitsrechte jedes _jeder Einzelnen bei.

Immer wieder wird dabei verkannt, dass Datenschutzbeauftragte nicht die Verantwortung für Entscheidungen tragen, sondern als Expert_in für Datenschutzfragen die Sachverantwortlichen bei deren Entscheidung beraten. „Kannst du das mal unterschreiben?" gibt es also nicht. Jede_r Beschäftigte einer öffentlichen Stelle sollte demnach ein Grundverständnis davon haben, was Datenschutz überhaupt ist, um sich im Zweifel (rechtzeitig) beraten lassen zu können. Gerade in großen Organisationsstrukturen kann das eine echte Herausforderung sein.

Eine von uns besuchte öffentliche Stelle hatte dies so gelöst, dass sie in jeder Abteilung eine Datenschutzansprechperson benannt hat. Diese Person ist dann nicht selbst Datenschutzbeauftragte, sondern Mittlerin zwischen den eigenen Kolleg_innen und dem_der Datenschutzbeauftragten – in beide Richtungen. Dadurch wird die Hürde zum Nachfragen reduziert und der_die Datenschutzbeauftragten können ihre Anliegen effizient unter die Belegschaft streuen. Eine gute Idee ist definitiv auch ein den Behördenstrukturen angepasster Leitfaden zum Umgang mit Datenschutzfragen von Bürger_innen. Verlangt bspw. jemand eine Auskunft nach Artikel 15 DS-GVO, muss selbstverständlich nicht jede_r Sachbearbeiter_in dessen Voraussetzungen im Detail kennen. Es sollte jedoch eine Anleitung zur Verfügung stehen, um nachlesen zu können, wie das geht, oder wer für die Erteilung zuständig ist. Überhaupt lohnt sich eine Dienstanweisung zum Thema Datenschutz. So können sich wiederholende Fragen abschließend geklärt und aufbereitet werden und jede_r kann nachlesen, was seine_ihre Aufgabe bei Datenschutzfragen ist.

Das Kennenlernen des Alltags einer kommunalen öffentlichen Stelle ist auch für uns wichtig. Wir wollen nicht erst dann zu agieren, wenn bereits etwas schiefgelaufen ist. Hinterher zu sagen: „So geht es nicht!" ist immer leichter als mitzuüberlegen, wie es gehen kann. Deswegen suchen wir nach Wegen, kommunale Stellen bei der Vielzahl an Aufgaben, bei denen personenbezogene Daten verarbeitet werden, zu unterstützen. Dazu gehören insbesondere unser Schulungsangebot (Datenschutzgrundlagen für öffentliche Stellen – ohne Vorkenntnisse für alle Beschäftigten kommunaler Stellen) und auch unser Forum kommunaler Datenschutz (regelmäßige Treffen mit Landkreistag, Städtetag und Gemeindetag sowie in wechselnder Besetzung behördliche Datenschutzbeauftragte, aber auch weitere, noch laufende Projekte.

Also: Der Arbeitsalltag behördlicher Datenschutzbeauftragter ist extrem vielseitig, und es war lehrreich, dieses Alltagsgeschäft aus nächster Nähe zu

☛ Mehr Informationen:

Der Kommunale Datenschutzwettbewerb ist ein doppeltes Best Practice-Beispiel: Zunächst: Für eine typisches Handeln beim LfDI, das konsequent auf das Interesse der Zielgruppe ausgerichtet ist – unsere Fachabteilung, die für öffentliche Stellen ansprechbar ist, hat den Kommunalen Datenschutzwettbewerb erdacht und gemeinsam mit unseren Projektexpert_innen aus der Taufe gehoben. Und weiter, erst recht Best Practice: Zahlreiche öffentliche Stellen haben bei dem Wettbewerb mitgemacht – Ideen und Preisträger_innen des Kommunalen Datenschutzwettbewerbs 2022: www.baden-wuerttemberg.datenschutz.de/preistraeger-des-kommunalen-datenschutzwettbewerbs-2022-gekuert

beobachten. Ein herzlicher Dank an die öffentlichen Stellen, die furchtlos die Aufsichtsbehörde ins Haus gelassen haben! Das Konzept der gegenseitigen Hospitation wollen wir auch im nächsten Jahr fortsetzen und freuen uns dabei auch auf interessierte Datenschutzbeauftragte von öffentlichen Stellen, die einen näheren Einblick in unsere Tätigkeit gewinnen möchten. Miteinander und voneinander zu lernen trägt zum gegenseitigen Verständnis der jeweiligen Ziele und Herausforderungen bei und führt damit zu einem noch besseren kommunalen Datenschutz.

Kommunaler Datenschutzwettbewerb

Um Kommunale Stellen zu unterstützen und die Arbeit vor Ort zu würdigen, haben wir zudem im Juni erstmals einen Kommunalen Datenschutzwettbewerb ausgerufen und Kommunale Stellen eingeladen, kreative und innovative Vorschläge einzureichen, die das Thema Datenschutz bei kommunalen Stellen erleichtern, erklären und umsetzen. Die Fachjury – unter dem Vorsitz unserer Hausspitze bestand sie aus drei Vertreter_innen der Kommunalen Spitzenverbände – hat sechs Preisträger ausgezeichnet, deren unterschiedliche Ideen allesamt Vorbildcharakter haben: Die Große Kreisstadt Laupheim, das Landratsamt Calw, das Landratsamt Konstanz, das Landratsamt Neckar-Odenwald-Kreis, die Stadt Knittlingen, die Große Kreisstadt Böblingen.

Die innovativen Ideen der Kommunen können auch anderen Behörden als Impuls dienen, diese Anregungen aufzunehmen und für die eigene Arbeit fruchtbar zu machen. Dabei geht es nicht zuletzt darum alle Beschäftigte und Bürger_innen darin zu unterstützen, die anzuwendenden Datenschutzregeln besser zu verstehen und nachzuvollziehen. Denn auch der Schutz der personenbezogenen Daten muss nicht bürokratisch-kompliziert sein, sondern funktioniert am besten leicht und gut integriert.

1.3 Beratung von Behörden: Regelung von Zugriffsrechten bei der E-Akte

Das notwendige Zusammenspiel von Datenschutz und Digitalisierung zeigt sich auch an einem für die Behörden des Landes sehr konkreten und für die Arbeit in den Behörden grundlegenden Thema: der E-Akte.

Die elektronische Verwaltungsakte E-Akte BW erhält immer weiter Einzug bei den Behörden des Landes: Nach Mitteilung der Stabsstelle „Projekt Landeseinheitliche E-Akte“ (StEA) sind mit Abschluss des Jahres 2022 alle Ministerien und alle Regierungspräsidien mit der E-Akte BW ausgestattet. Und auch wir bereiten uns auf die Einführung der E-Akte in unserer Behörde zum Starttermin Mai 2023 vor (siehe Kapitel 10). In diesem Zusammenhang wurden wir um Beratung gebeten, welche datenschutzrechtlichen Vorgaben bei der Ausgestaltung der Zugriffsrechte auf einzelne Vorgänge in der E-Akte zu beachten sind.

Die Einführung einer elektronischen Akte in der Verwaltung verspricht nicht nur eine Erleichterung und Beschleunigung der Arbeit – etwa auch im Homeoffice – an den Dienststellen des Landes. Sie kann auch erhebliche Vorteile für den Datenschutz und die Informationsfreiheit mit sich bringen: So kann die Kommunikation über einzelne Vorgänge (die gegebenenfalls personenbezogene Daten enthalten) in der E-Akte selbst erfolgen und damit eine Parallelverarbeitung personenbezogener Daten in weiteren Kommunikationsmedien (beispielsweise in E-Mails) weitgehend vermieden werden. Auch lassen sich Löschroutinen einrichten und so die Einhaltung von Löschfristen sicherstellen. Überdies ist die Integration von sicheren Schwärzungstools denkbar. Solche Tools können hilfreich sein, wenn bei der Überlassung einer Kopie nach Artikel 15 Absatz 3 DS-GVO oder bei der Gewährung von Zugang zu amtlichen Informationen nach dem Landesinformationsfreiheitsgesetz einzelne Informationen nicht herausgegeben werden dürfen.

Rechte- und Rollenkonzepte für Nutzer_innen

Andererseits birgt die elektronische Form der Aktenführung die Gefahr, dass eine kaum begrenzte Vielzahl von Beschäftigten der Dienststelle auf jeden Vorgang – auch solche mit personenbezogenen Daten – zugreifen könnte: Anders als bei der Papierakte, die nur einmal existiert und bei der schon aus diesem Grund die gleichzeitige Bearbeitung durch mehrere Personen physisch kaum (beziehungsweise nur nach Erstellung von Ablichtungen) möglich ist, kann bei der elektronischen Akte ein gleichzeitiger Zugriff durch mehrere – oder sogar alle – Bedienstete der jeweiligen Stelle ohne Weiteres ermöglicht werden. Ist es hier datenschutzrechtlich zulässig, ei-

nen Zugriff durch alle Bedienstete auf alle Vorgänge der Dienststelle, auch solche mit personenbezogenen Daten, zuzulassen? Wäre eine solche allgemeine Zugriffsberechtigung aller Beschäftigten auf alle Vorgänge eventuell damit zu rechtfertigen, dass man auf diese Weise Textbausteine aus anderen Vorgängen übernehmen möchte oder für eine einheitliche Rechtsanwendung in der Behörde sorgen möchte? Oder spricht etwa gerade das Recht auf Informationsfreiheit in einem Erst-Recht-Schluss für eine weite Ausgestaltung der Zugriffsrechte? Denn wenn jede_r Bürger_in auf Antrag möglichst viel an amtlichen Informationen zugänglich gemacht werden soll, müsste dann nicht erst recht innerhalb der Behörde eine weite Zugriffsmöglichkeit bestehen? Oder welche Eingrenzungen sind bei der Zugriffsausgestaltung datenschutzrechtlich vorzunehmen? Mit diesen Fragen mussten wir uns nicht nur wegen der bevorstehenden Einführung der E-Akte BW bei uns selbst beschäftigten (siehe Kapitel 10.1), sondern wir wurden auch von außerhalb um Beratung gebeten.

Ausgangspunkt der datenschutzrechtlichen Überlegungen ist das Prinzip der Datenminimierung (Artikel 5 Absatz 1 Buchstabe c DS-GVO). Aus diesem ergibt sich, dass der Verantwortliche Zugriffe auf personenbezogene Daten in einer (E-)Akte grundsätzlich nur insoweit (rechtlich) zulassen darf, als es für die Zweckerreichung – im Falle einer Behörde also in der Regel für die Aufgabenerfüllung – erforderlich ist. Dies bezieht sich sowohl auf Daten externer betroffener Personen als auch – mit Blick auf den Beschäftigtendatenschutz – auf personenbezogene Daten der Beschäftigten. Der Verantwortliche muss daher zunächst die bei ihm tätigen Beschäftigten (etwa durch eine Dienstanweisung) rechtlich verpflichten, Zugriffe auf personenbezogene Daten auf das zur Aufgabenerfüllung notwendige Maß zu beschränken, und darüberhinausgehende Zugriffe untersagen.

Diesem Prinzip entspricht eine (auch unter den Behörden des Landes) weit verbreitete Formulierung in den Datenschutz-Informationen verschiedener öffentlicher Stellen, wenn es dort beispielsweise auf die Frage „Wem gegenüber werden Ihre personenbezogenen Daten offengelegt?“ heißt:

„[Die Behörde] legt Ihre personenbezogenen Daten ihren Mitarbeiterinnen und Mitarbeitern sowie Dritten gegenüber nur auf der Grundlage gesetzlicher Vorschriften offen oder wenn eine ausdrückliche Einwilligung Ihrerseits vorliegt.“

Oder:

„Innerhalb des …-ministeriums erhalten nur diejenigen Personen Zugang zu Ihren personenbezogenen Daten, die mit der Durchführung des Vorgangs, in welchem Ihre Daten relevant sind, betraut sind.“

Die Einhaltung des Prinzips der Datenminimierung (dass also nur Personen zugreifen dürfen, die zuständig sind) hat der Verantwortliche aber nicht nur rechtlich durch eine entsprechende Dienstanweisung festzulegen, sondern auch durch geeignete technische und organisatorische Maßnahmen risikoadäquat sicherzustellen (vgl. Artikel 5 Absatz 1 Buchstabe f, Artikel 24, 25 und 32 DS-GVO).

Es muss also ein Rollen- und Berechtigungskonzept vorhanden sein – auch beispielsweise bezogen auf Geheimschutzvorgänge, auf die keinesfalls ein behördenweiter Zugriff möglich sein darf. Unzulässige Zugriffe sind dabei vorrangig auch technisch zu unterbinden und nicht nur organisatorisch zu untersagen. Die (tatsächliche) Zugriffsmöglichkeit hat somit – soweit möglich – der (datenschutzrechtlichen) Zugriffsbefugnis zu entsprechen.

Nur soweit eine technische Beschränkung der Zugriffsmöglichkeiten auf personenbezogene Daten in der E-Akte unter Berücksichtigung des Aufwandes und der Risiken und des Standes der Technik nicht angemessen wäre, käme hilfsweise in Betracht, die Einhaltung der Verpflichtung der Beschäftigten, den Zugriff auf das zur Aufgabeerfüllung Erforderliche zu beschränken, durch andere angemessene technische und organisatorische Maßnahmen risikoadäquat sicherzustellen – etwa durch eine Protokollierung der Zugriffe unter Festlegung und Durchführung von Stichproben und Prüfroutinen sowie gegebenenfalls von Sanktionen. Bei der Entscheidung zwischen technischer Beschränkung und der bloßen Einführung organisatorischer Maßnahme ist allerdings zu bedenken, dass solche organisatorischen Maßnahmen zur Überwachung der Anweisung nicht nur weniger wirksam vor unzulässigen Zugriffen schützen, sondern ihrerseits Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen würden.

Das hier in Rede stehende Zugriffs- und Rollen- beziehungsweise Berechtigungskonzept ist also eine Abhilfemaßnahme zur Minimierung derjenigen Risiken, die im Rahmen der zur Einführung der E-Akte erforderlichen Datenschutz-Folgenabschätzung identifizierten Risiken. Insoweit können wir auf die Vorlage zur Erstellung der organisationsspezifischen Datenschutz-Folgenabschätzung „DSFA E-Akte BW" – „Datenschutz-Folgenabschätzung für die E-Akte BW nach Art. 35 DS-GVO" verweisen, die die StEA den betroffenen Behörden zur Verfügung stellt. Dort heißt es unter anderem (Abschnitt I.X.2):

„Zur Minimierung der im Rahmen der DSFA identifizierten Risiken sind geeignete Abhilfemaßnahmen erforderlich. Die Auswahl erfolgt nach der DS-GVO, dem BSI-Grundschutz und insbesondere entsprechend den mit der Risikobewertung (siehe die Excel-Tabelle DSFA Risikobewertung_VX.X.xlsx) ermittelten Abhilfemaßnahmen.

Mit der Auswahl der Abhilfemaßnahmen sind die Grundsätze für die Verarbeitung von personenbezogenen Daten nach Art. 5 der DS-GVO zu erfüllen (siehe oben Ziff. IX.1.a)."

Und als Abhilfemaßnahmen Nummer 1 sind dort genannt:

„Zugriffs- und Rollenkonzept, Need-To-Know-Prinzip/Aufgabentrennung, Zugangs- und Zugriffssteuerung, Verwaltung privilegierter Zugangsrechte".

Es ist mithin Aufgabe eines jeden Verantwortlichen zu prüfen und risikoangemessen sicherzustellen, wer nach dem "Need-To-Know-Prinzip" einen Zugriff benötigt oder wer ihn beispielsweise erst nach einer entsprechenden Anfrage erhalten soll (zum Beispiel, wenn ein Vorgang für eine weitere Abteilung bedeutsam wird).

Vor diesem Hintergrund erscheint es uns grundsätzlich angemessen, denjenigen Personen, die für die Bearbeitung des jeweiligen Vorgangs in der (E-)Akte intern zuständig sind (etwa aufgrund des jeweiligen Geschäftsverteilungsplans), sowie deren Vertretung(en), gegebenenfalls auch noch deren unmittelbaren Vorgesetzten die Möglichkeit des Zugriffs zu gewähren. Ob indes auch die Behördenleitung und deren Vertretung beziehungsweise Beauftragte als weitere Vorgesetzte der für die Bearbeitung der jeweiligen E-Akte Zuständigen auf alle personenbezogenen Daten in allen E-Akten der Behörde jederzeit ohne Weiteres zugreifen können sollten, wäre näher zu betrachten und bedürfte einer entsprechend gewichtigen Begründung. Hier wird es vielmehr – was zu erwägen und abzuwägen ist – regelmäßig genügen, dass jene weiteren Person(en) sich die jeweilige E-Akte von der/dem betreffenden Abteilung/Referat (je nachdem, wie das Verfahren das vorsieht) etwa „freigeben" lässt/lassen.

Das eingangs als mögliches Argument zur Erweiterung des Kreises der Zugriffsberechtigten genannte Ziel, einheitliche Maßstäbe für bestimmte Rechtsfragen in einer Behörde zu erreichen, also etwa referats- oder abteilungsübergreifende Rechtsmeinungen zu erzielen, ist nicht tragfähig. Es rechtfertigt keine Ausweitung der Erlaubnis des Zugriffs auf personenbezogene Daten in (E-)Akten. Vielmehr sind solche Maßstäbe allgemein und ohne Personenbezug zu entwickeln und festzulegen. Fragen nach ähnlichen Vorgängen könnten etwa mit den für die Bearbeitung der entsprechenden Vorgänge (und der jeweiligen E-Akte) Zuständigen oder deren Vertretung(en) und Vorgesetzten ohne Personenbezug geklärt werden.

E-Akte aus Sicht des Datenschutzes- und der Informationsfreiheit betrachten

Auch das in der oben wiedergegebenen Argumentation angeführte Informationsfreiheitsrecht führt zu keinem anderen datenschutzrechtlichen Ergebnis. Es handelt sich dabei um einen vom Datenschutzrecht verschiedenen Rechtsbereich.

Die DS-GVO und das Landes-Informationsfreiheitsgesetz (LIFG) sind nebeneinander anwendbar. Die Vorschrift des Art. 86 DS-GVO, die das Verhältnis in Bezug zur Informationsfreiheit regelt, enthält eine Öffnungsklausel für die nationalen Regelungen und ermöglicht die Anwendung mitgliedstaatlicher Regelungen wie der Informationsfreiheitsgesetze. Die Bestimmungen aus Art. 6 Abs. 2 und 3 DS-GVO erlauben es den Mitgliedstaaten, eigene Vorschriften zu erlassen, sofern diese nicht gegen EU-Recht verstoßen.

Auch bei einem Antrag auf Informationszugang nach den Vorschriften des LIFG müssen Datenschutzaspekte geprüft werden, die ggf. den Zugang zur gewünschten Information verwehren oder einschränken, vgl. § 9 LIFG. Wenn geschützte Inte-

resse nach § 4 bis § 6 LIFG dem Antrag nach LIFG entgegenstehen, besteht kein Anspruch auf Informationszugang. Der Antrag muss so entschieden werden, dass durch die Auskunft nicht gegen die Vorschriften der DS-GVO beziehungsweise sonstige Datenschutzgesetze verstoßen wird. Die Vorschrift des § 5 LIFG enthält in diesem Sinne eine zulässige Regelung zum Schutz personenbezogener Daten im Sinne von Art. 4 Nr. 1 DS-GVO. Das Grundrecht auf informationelle Selbstbestimmung ist mit dem verfassungsrechtlich garantierten Zugangsanspruch aus Art. 5 Abs. 1 GG im Wege praktischer Konkordanz in Ausgleich zu bringen (vgl. Brink, in Brink/Polenz/Blatt IFG § 5 Rn. 1–4). Dies wurde in § 5 LIFG umgesetzt. Zweck des LIFG ist der freie Zugang zu Informationen „unter Wahrung des Schutzes personenbezogener Daten" (vgl. § 1 Abs. 1 LIFG).

Der Zugang zu personenbezogenen Daten ist gemäß § 5 LIFG zu gewähren, soweit und solange die geschützte Person im Sinne des Artikels 4 DS-GVO eingewilligt hat. Gemäß § 8 LIFG ist ein Drittbeteiligungsverfahren durchzuführen und die Einwilligung der geschützten Person einzuholen.

Die Norm des § 5 Abs. 1 LIFG enthält zudem eine Abwägungsregelung, wonach der Zugang zu personenbezogenen Daten auch ohne Einwilligung gewährt werden kann, sofern das öffentliche Informationsinteresse an der Bekanntgabe das schutzwürdigen Interesse am Ausschluss des Informationszugangs überwiegt. Dies erfolgt im Rahmen einer Abwägungsentscheidung. Der Anspruch auf Informationszugang ist voraussetzungslos; im Rahmen der Abwägung soll die antragstellende Person den Antrag begründen (§ 7 Abs. 1 S. 3 LIFG). Der Informationszugang ist in der Regel vorrangig, soweit er zur Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechte Einzelner geboten ist (siehe dazu: VGH Baden-Württemberg, Urteil vom 17. Dezember 2020 - 10 S 3000/18). Personenbezogene Daten von Amtsträger_innen (Beschäftigtendaten) regelt § 5 Abs. 4 S. 2 LIFG. Nach dieser Vorschrift überwiegt das öffentliche Informationsinteresse „[…] wenn sich die Angabe auf Name, Titel, akademischen Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und -telekommunikationsnummer beschränkt […]".

Bei sensiblen Daten im Sinne des Art. 9 Abs. 1 DS-GVO hingegen ist nach § 5 Abs. 2 LIFG die Einwilligung der betroffenen Person zwingend erforderlich. Eine Abwägungsentscheidung ist hier ausgeschlossen. Es ist folglich möglich, dass antragstellende Personen nach LIFG Zugang zu personenbezogenen Daten erhalten, die Behördenmitarbeitenden – mangels einer Rechtsgrundlage – zu dem Zeitpunkt der Antragstellung nicht bekannt sind. Darin ist jedoch kein Wertungswiderspruch zu sehen. Es handelt sich um keinen „exklusiven" Zugang, sondern um amtliche Informationen, die nach dem Datennutzungsgesetz (DNG) auch veröffentlicht und weiterverwendet werden dürfen. Der Zugang erfolgte im Rahmen einer Prüfung innerhalb des Verfahrens nach dem Landes-Informationsfreiheitsgesetz.

Behörden müssen also ihre Beschäftigten verpflichten und dahingehend sensibilisieren, dass sie – auch bei der E-Akte – nur insoweit Zugriff auf personenbezogene Daten nehmen, als dies für die Aufgabenerfüllung der Behörde zwingend erforderlich ist. Dies ist außerdem durch geeignete und angemessene technische und organisatorische Maßnahmen – inklusive eines Rechte- und Rollen-Konzepts für die Beschäftigten – sicherzustellen. Dabei hat gefährdungsadäquat eine technische Beschränkung des Zugriffs Vorrang vor einer bloßen organisatorischen Maßnahme (wie z. B. einer Protokollierung von Zugriffen mit konkreten Prüfroutinen und ggf. Verhängung von Sanktionen). Es ist mithin Aufgabe eines jeden Verantwortlichen zu prüfen und risikoangemessen sicherzustellen, wer nach dem "Need-To-Know-Prinzip" einen Zugriff benötigt oder wer ihn beispielsweise erst nach einer entsprechenden Anfrage und Freigabe durch andere erhalten soll.

1.4 Beratung bei der Forschung

Eines der derzeit mit am meisten diskutierten Themengebiete im Datenschutzrecht ist die Frage, wie sich das Datenschutzrecht zur Forschung verhält. Dabei geht es darum, inwieweit und unter welche Voraussetzungen Forscher_innen zum Zwecke des wissenschaftlichen Erkenntnisgewinns personenbezogene Daten verarbeiten dürfen. Sind sie dabei genauso strikt an datenschutzrechtliche Vorgaben gebunden wie andere datenverarbeitende Stellen, etwa die werbende Wirtschaft oder die staatliche Verwaltung? Im Vordergrund der Diskussion steht

hier – sicherlich mitgeprägt durch den Wunsch nach raschen Erkenntnissen über das Virus SARS-Cov-2 und die von ihm ausgelöste Infektionskrankheit COVID-19 während der Pandemie – die Forschung mit Gesundheitsdaten zu medizinischen Zwecken.

Einwilligungslösung

Dabei sind mehrere Entwicklungen im Diskurs auszumachen: In den zurückliegenden Jahren stand zwischen Wissenschaftler_innen und den Datenschutzbehörden, aber auch in der rechtswissenschaftlichen Diskussion die Frage im Vordergrund, inwieweit Forschung mit personenbezogenen Daten auf Einwilligungen der betroffenen Personen gestützt werden könnten. Die Diskussion konzentrierte sich hier insbesondere auf die Frage, wie damit umzugehen sei, dass die Forschenden oftmals nicht im Vorhinein genau beschreiben können, welche Ergebnisse ihre Forschung haben werden und – damit zusammenhängend – für welche Forschungsfragen die Daten Bedeutung erlangen würden. Wie genau muss aber die Einwilligung den Forschungszweck beschreiben, damit sie als hinreichend informiert erteilt und hinreichend bestimmt angesehen werden kann? Die Europäische Gesetzgeber hat diese Problematik bereits beim Erlass der DS-GVO gesehen und im Erwägungsgrund 33 eine Lösung skizziert, indem es dort heißt:

„Oftmals kann der Zweck der Verarbeitung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung zum Zeitpunkt der Erhebung der personenbezogenen Daten nicht vollständig angegeben werden. Daher sollte es betroffenen Personen erlaubt sein, ihre Einwilligung für bestimmte Bereiche wissenschaftlicher Forschung zu geben, wenn dies unter Einhaltung der anerkannten ethischen Standards der wissenschaftlichen Forschung geschieht. Die betroffenen Personen sollten Gelegenheit erhalten, ihre Einwilligung nur für bestimme Forschungsbereiche oder Teile von Forschungsprojekten in dem vom verfolgten Zweck zugelassenen Maße zu erteilen."

Wie das in die Praxis umgesetzt werden kann, war in den zurückliegenden Jahren insbesondere Gegenstand beratender Gespräche zwischen den Arbeitskreisen Wissenschaft und Forschung sowie Gesundheit und Soziales der DSK und der Medizin-Informatik-Initiative (MII) der Technologie- und Methodenplattform für die vernetzte medizinische Forschung (TMF). Die Gespräche führten 2020 zu dem positiven Ergebnis, dass die DSK erklärte, gegen die von der MII entwickelten Mustertexte zur Einwilligung in die medizinische Forschung – die bei Zusicherung gewisser Transparenzverfahren relativ breite Einwilligungserklärungen enthalten – bestünden keine Einwände.

Verhältnis zur ärztlichen Schweigepflicht

Dass die medizinische Forschung zunächst auf Einwilligung gestützt wurde, ist sicherlich kein Zufall. Denn die im Rahmen von medizinischen Behandlungen erlangten Informationen über Patient_innen unterliegen nicht nur dem Schutz des Datenschutzrechts im engeren Sinne, für das die Datenschutzaufsichtsbehörden die zuständigen Ansprechpartner sind. Die Informationen unterliegen vielmehr darüber hinaus auch dem Berufsgeheimnis der Gesundheitsberufe, insbesondere also der ärztlichen Schweigepflicht, die gegenüber der Weitergabe von Informationen oftmals noch strengere Anforderungen aufstellt als das allgemeine Datenschutzrecht. Wenn nun ohnehin eine datenschutzrechtliche Einwilligung eingeholt wird, wird der_die Patient_in in aller Regel gleichlaufend entsprechend der Einwilligung das medizinische Personal auch von der Schweigepflicht entbinden – so dass auf diese Weise beide Fragestellungen, die datenschutzrechtliche und die – der Aufsicht der Heilberufekammern unterliegende – berufsrechtliche, durch eine entsprechende Willensbekundung der_des Patientin_en rechtssicher geklärt werden können.

Gründe für eine über die Einwilligungslösung hinausgehende Verarbeitungsbefugnis

Gleichwohl geht der Wunsch der Forschenden zwischenzeitlich überwiegend von der Einwilligungslösung weg dahin, eine gesetzliche Grundlage zur Erlangung des Zugangs zu medizinischen Informationen und zur Verarbeitung dieser Daten zu Forschungszwecken nutzen zu können. Hierfür wird nicht nur geltend gemacht, dass die Einwilligungsverwaltung einen erheblichen Aufwand verursache. Betont wird vielmehr auch, dass neue Forschungsmethoden (namentlich mit dem Einsatz von künstlicher Intelligenz) nicht mehr darauf gerichtet seien, konkrete Forschungsfragen zu beantworten, sondern die (maschinell unterstützte) Mustererken-

nung künstlicher Intelligenz verwende, weswegen einerseits der konkrete wissenschaftliche Erkenntnisgewinn aus den Daten noch schwerer vorhersagbar sei und andererseits eine möglichst breite Datenbasis erforderlich sei. Wenn hier lediglich auf Basis von Einwilligungen verarbeitbare Daten verwendet würden, berge dies die Gefahr, dass bestimmte Fälle, in denen eine Einwilligung (regelmäßig) nicht erteilt würde, nicht erfasst würden und die Datenbasis daher verzerrende Tendenzen - erhalte (siehe auch Kapitel 1.5.1.2 „KI und Gesundheit“).

Der Europäische Gesundheitsdatenraum

Die Forderung nach einem möglichst einwilligungsunabhängigen Zugang zu medizinischen Daten zu Forschungszwecken ist dabei nicht auf Deutschland beschränkt. Sie wird auch auf Europäischer Ebene gehört: Im Mai 2022 legte die Europäische Kommission den Vorschlag für eine EU-Verordnung über den europäischen Raum für Gesundheitsdaten vor, die für eine flächendeckende digitale Verarbeitung von Gesundheitsdaten aus der medizinischen Versorgung sorgen und es so – wie es in dem ersten Absatz der Begründung heißt – insbesondere „Akteuren aus Forschung und Innovation sowie politischen Entscheidungsträgern“ ermöglichen soll, „diese elektronischen Gesundheitsdaten auf vertrauenswürdige und sichere Weise unter Wahrung der Privatsphäre zu nutzen.“ Dabei ist es bemerkenswert, dass die Europäische Kommission ausgerechnet im Gesundheitsbereich, in dem es mit den Gesundheitsdaten um besonders sensible Datenarten geht, innerhalb ihrer „Europäischen Datenraumstrategie“ als erstes einen spezifischen „Datenraum“ zu Forschungs- und Innovationszwecken schaffen will. Das hängt sicherlich ebenfalls damit zusammen, dass man infolge der Pandemie den besonderen Wert der Gesundheitsforschung erkannt hat. Das Argument der Kommission allerdings, die COVID-19-Pandemie habe deutlich gemacht, dass ein zeitnaher Zugang zu elektronischen Gesundheitsdaten für die Vorsorge und Reaktion bei Gesundheitsbedrohungen und für die Diagnose und Behandlung sowie für die Sekundärnutzung

☛ Mehr Informationen:

Petersberger Erklärung der Datenschutzkonferenz der Länder und des Bundes zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung, 24.11.22:
datenschutzkonferenz-online.de/media/en/20221124_en_06_Entschliessung_Petersberger_Erklaerung.pdf

Pressemitteilung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 24. April 2020, „Datenschutzbehörden des Bundes und der Länder akzeptieren die Einwilligungsdokumente der Medizininformatik-Initiative“:
www.datenschutzkonferenz-online.de/media/pm/20200427_Einwilligungsdokumente_der_Medizininformatik-Initiative.pdf

Gutachten „Digitalisierung für Gesundheit“ des Sachverständigenrats zur Begutachtung der Entwicklung im Gesundheitswesen von 2021:
www.svr-gesundheit.de/fileadmin/Gutachten/Gutachten_2021/SVR_Gutachten_2021.pdf

Im Auftrag der Bundesregierung erstellte „Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität“ von Frau Prof. Dr. Louisa Specht-Riemenschneider:
www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf

Vorschlag der EU-Kommission für eine Verordnung über den europäischen Raum für Gesundheitsdaten:
eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52022PC0197&from=EN

Gemeinsame Stellungnahme des EDSA und des EDPS zum Vorschlag der Kommission betreffend eine Verordnung zum Europäischen Gesundheitsdatenraum:
edpb.europa.eu/system/files/2022-07/edpb_edps_jointopinion_202203_europeanhealthdataspace_en.pdf, nur englisch

von Gesundheitsdaten unerlässlich sei, ist nicht wirklich überzeugend: Die Krise als Ausnahmefall ist selten ein guter Ratgeber für derart grundlegende und weitreichende, in Grundrechte – hier v. a. in das Recht auf Datenschutz (Art. 8 der Grundrechtecharta der EU) – eingreifende Reformen. Es bedarf vielmehr einer angemessenen Abwägung aller relevanten Aspekte. Und da weist der Vorschlag der Kommission noch erhebliche Defizite auf. Diese können hier nicht vollständig aufgelistet werden. Aber als besonders augenfällig ist die mangelnde Harmonisierung mit den Regelungen der DS-GVO hervorzuheben: So heißt es zwar in Artikel 1 Absatz 4 des Verordnungs-Vorschlags der Kommission über den Europäischen Gesundheitsdatenraum, die Regelungen der DS-GVO blieben unberührt. Tatsächlich enthält der Entwurf indes eigene Regelungen zu den Betroffenenrechten, die in inkonsistener Weise von denen der DS-GVO abweichen. Fraglich ist auch die Vereinbarkeit der von dem Verordnungsvorschlag (siehe dessen Artikel 34) ins Auge gefassten Zwecken der Sekundärverarbeitung von Gesundheitsdaten mit den Anforderungen von Artikel 9 DS-GVO für die Verarbeitung besonderer Kategorien personenbezogener Daten, zu denen die Gesundheitsdaten gehören.

Gesetzliche Verarbeitungsbefugnisse aus nach DS-GVO und nationalem Recht

Dabei ist eigentlich die Vorstellung einer gesetzlichen – nicht auf Einwilligung beruhenden – Befugnis, zu Zwecken der Forschung personenbezogene (auch Gesundheits-)Daten zu verarbeiten, der DS-GVO und dem sie umsetzenden deutschen gesetzlichen Regelungen nicht fremd: Die DS-GVO privilegiert vielmehr die Forschung in besonderer Weise, indem sie etwa eine Zweckänderung zu Forschungszwecken in der Regel zulässt (Artikel 5 Absatz 1 Buchstabe b 2. Halbsatz DS-GVO) und zu Forschungszwecken weitgehende Befreiungen vom Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten zulässt (Artikel 9 Absatz 2 Buchstabe j DS-GVO), wenn im Gegenzug geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person vorgesehen werden, insbesondere sichergestellt wird, dass effektive technische und organisatorische Maßnahmen – wie insbesondere eine frühzeitige Anonymisierung oder hilfsweise Pseudonymisierung – bestehen, mit denen insbesondere die Achtung des Grundsatzes der Datenminimierung gewährleistet wird (Artikel 89 Absatz 1 DS-GVO). In Umsetzung dieser Öffnungsklauseln bestimmt etwa § 27 Absatz 1 BDSG eine Ausnahme vom Verarbeitungsverbot für besondere Kategorien personenbezogener Daten aus Artikel 9 Absatz 1 DS-GVO ausdrücklich „auch ohne Einwilligung", soweit „die Verarbeitung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen" und sofern der Verantwortliche angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 BDSG vorsieht. Ähnliche Regelungen enthalten die meisten Landesdatenschutzgesetze, z. B. § 13 LDSG. Dabei umfassen diese Regelungen nach unserem Verständnis, wie sich aus der Definition der „Verarbeitung" in Artikel 4 Nummer 2 DS-GVO ergibt, nicht nur die Weiterverarbeitung von bereits vom Verantwortlichen erhobenen Daten (zuweilen auch „Eigenforschung" genannt), sondern auch die Erhebung und Übermittlung von Daten, soweit diese Vorgänge zum Zweck der Forschung erforderlich ist.

Forschungsfreundlichkeit des Datenschutzrechts

Die Erkenntnis, dass Datenschutzrecht nach der DS-GVO den hohen Wert der Forschung anerkennt und also forschungsfreundlich ist und dass dieser Spielraum von den Forschenden genutzt werden kann, hat sich noch nicht überall durchgesetzt. Auch für uns Datenschützer sind so weitreichende Ausnahmen nicht immer leicht zu akzeptieren, doch aber ist zu sehen, dass Wissenschaft und Forschung außerordentlich wichtig sind und die DS-GVO dies anerkennt.

Immer wieder beklagen sich Forschende, dass „der Datenschutz" die Forschung behindere, und finden damit im öffentlichen Diskurs durchaus Resonanz. Dabei stellt sich zuweilen heraus, dass manche hier „dem Datenschutz" angelasteten Hindernisse gar keinen datenschutzrechtlichen Ursprung haben (sondern zum Beispiel in mangelnder Digitalisierung oder Standardisierung begründet sind, siehe auch Kapitel 1.5.1.2 KI und Gesundheit). Manche Forschende empfinden aber auch generell datenschutzrechtliche Anforderungen schlicht als „lästig" und äußern die Meinung, die Datenschutzbestimmungen würden sie nur Zeit und Aufwand

kosten und damit von ihrer eigentlichen Aufgabe – der Forschung – abhalten, eine Ansicht, die dankenswerter Weise zum Teil auch so offen z. B. auf unserer KI-Woche ausgesprochen wurde.

Dazu ist zu sagen: Sicher geht die Privilegierung der Forschung durch die DS-GVO und die sie umsetzenden Regelungen des deutschen Rechts nicht so weit, dass die Forschenden deswegen datenschutzrechtliche Anforderungen gänzlich ignorieren könnten. Das wäre aber auch kein angemessener Ausgleich zwischen den hier angesprochenen Grundrechten. Die Forschenden bzw. die Forschungseinrichtungen müssen sich vielmehr – je nach Forschungsvorhaben – Gedanken über den Zweck ihrer Forschung, die Auswahl der erforderlichen Datenarten, den Zeitpunkt und die Art der Anonymisierung bzw. Pseudonymisierung, vorzunehmende technische und organisatorische Maßnahmen machen, unter Umständen eine Datenschutzfolgenabschätzung durchführen, die zur Klärung der datenschutzrechtlichen Verantwortung erforderlichen Auftragsdatenverarbeitungsverträge oder Verträge zur gemeinsamen Verantwortung abschließen und die betroffenen Personen über die Verarbeitung der sie betreffenden Daten informieren (vgl. beispielsweise unsere im TB 2021, S. 91 ff. beschriebene Beratung des Universitätsklinikums Tübingen zum Projekt STARKIDS). Das verlangt sorgfältige Planung und kann durchaus einen erheblichen Aufwand darstellen. Dabei ist aber auch zu sehen, dass die ordnungsgemäße Einhaltung der datenschutzrechtlichen Bestimmungen nicht nur im Interesse der betroffenen Proband_innen liegt, sondern auch im Interesse der Forschung selbst. Denn – wie es die Petersberger Erklärung der Datenschutzkonferenz formuliert: „Mit begründetem Vertrauen der betroffenen Personen in die Einhaltung ethischer, rechtlicher und technischer Standards wächst“ die Motivation der betroffenen Patient_innen, „die Forschung zu unterstützen. Deshalb ist es für Bürgerinnen und Bürger unerlässlich, darauf vertrauen zu können, dass ihre personenbezogenen Daten im Einklang mit den sie schützenden datenschutzrechtlichen Vorgaben und unter Wahrung ihrer informationellen Selbstbestimmung verarbeitet werden.“ Es wäre also zu kurz gegriffen, wenn man zur Beurteilung der Frage, unter welchen Voraussetzungen Forschende die personenbezogenen Gesundheitsdaten eines Patienten sollen verarbeiten dürfen, alleine das höchst individuelle, gleichsam „egoistisch“ anzusehende Abwehrrecht des betroffenen Patienten gegen das – möglicherweise gesellschaftlich höchst relevante – Interesse des Forschenden an der wissenschaftlichen Erkenntnis abwägen würde. Mit dem Philosophen und Psychiater Thomas Fuchs der im Jahr 2023 den Erich-Fromm-Preis erhält haben wir – was an dieser Stelle angemerkt sei – unter anderem auch genau darüber gesprochen, welche Bedeutung es haben kann, wenn

Die Datenschutz-Grundverodnung ist forschungsfreundlich.

moralischer Druck auf eine kranke Person aufgebaut wird, ihre Gesundheitsdaten für ein übergeordnetes, der Gesundheit aller Menschen dienendes Ziel, zu teilen, geradezu teilen zu müssen.

Abgesehen davon, dass hier auch weitere Grundrechte außer der informationellen Selbstbestimmung und der Forschungsfreiheit beteiligt sein können (z. B. auch das Recht auf Eigentum, die Berufsfreiheit u. a.), besteht nicht nur ein subjektives Interesse der betroffenen Person an der Einhaltung seiner Datenschutz-Interessen, sondern auch ein objektives Interesse an der vertrauensbildenden Wahrung des Datenschutzes durch die Forschenden.

Besonders deutlich wird dies, wenn personenbezogene Daten aus der Gesundheitsversorgung durch andere als die Behandelnden wissenschaftlich genutzt werden sollen: Dann darf der Umstand, dass mit den personenbezogenen Daten aus der Gesundheitsversorgung geforscht wird, nicht dazu führen, dass Patient_innen das Vertrauen in die vertrauliche Behandlung ihrer Daten durch die Behandler_innen verlieren und deswegen gar auf einen Arztbesuch verzichten. Die Einhaltung datenschutzrechtlicher Anforderungen durch Forschende ist damit letztlich Teil der gesellschaftlichen Verantwortung, die auch Forscher_innen zu tragen haben.

☛ Mehr Informationen

Gespräch mit dem Philosophen und Psychiater Thomas Fuchs über „Verkörperte Freiheit“:
tube.bawü.social/w/xeH2sUUgoveuj9hRqgfpaM

Projekt CoGDat: cogdat.de

Radiologisches Netzwerk „Racoon“:
racoon.network

Forum Gesundheitsstandort Baden-Württemberg:
forum-gesundheitsstandort-bw.de

DSK-Entschließung „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz“ vom 23.3.2022:
datenschutzkonferenz-online.de/media/en/DSK_6_Entschliessung_zur_wissenschaftlichen_Forschung_final.pdf

Unterstützung Forschender und der Forschung im allgemeinen durch den LfDI

Zugleich nehmen wir wahr, dass unter den Forschenden eine erhebliche Unsicherheit über die datenschutzrechtlichen Anforderungen an die Verarbeitung personenbezogener Daten zu Forschungszwecken bestehen. In durchaus nachvollziehbarer Weise wird insoweit auch die dem Datenschutzrecht immanente Verwendung unbestimmter Rechtsbegriffe kritisiert, die vielfach zu unterschiedlichen Auslegungen führt.

Wir haben daher auch im Berichtsjahr darauf hingewirkt, für die Forschenden mehr Klarheit zu erreichen und die Forschungsfreundlichkeit der DS-GVO einschließlich der durch sie eröffnenden Möglichkeiten in der Forschung bekannter zu machen und umzusetzen. Wir haben nicht nur erneut Forschende bei der datenschutzgemäßen Durchführung einzelner Forschungsprojekte beraten (so zum Beispiel beim Projekt CoGDat – einer Forschungsinitiative zur Sammlung, Speicherung und Auswertung aller in Deutschland produzierten SARS-CoV-2 Virus Sequenzdaten). Wir haben darüber hinaus im Rahmen unserer KI-Woche das Gespräch mit Forschenden gesucht, um ihre Perspektive besser einnehmen zu können und zugleich auch die Bedeutung des Grundrechts auf Datenschutz in der Forschung mit ihnen zu erörtern. Aus diesen und weiteren Kontakten entstand die Idee, im kommenden Jahr über unser Bildungszentrum BIDIB Fortbildungen für Forschende und Forschungseinrichtungen anzubieten, um mit ihnen gemeinsam den Weg durch den Artikel- und Paragraphen-Dschungel zu bahnen, ihnen also ganz praktische Unterstützung anzubieten, und zugleich das Verständnis für Belange des Datenschutzes zu stärken. Selbstverständlich können darüber hinaus Forschende und Forschungseinrichtungen auch weiterhin auf uns zukommen, um datenschutzrechtliche Aspekte ihrer Vorhaben zu besprechen.

Außerdem haben wir uns zu dieser Thematik in der Datenschutzkonferenz engagiert: Diese hat zunächst mit ihrer Entschließung „Wissenschaftliche Forschung – selbstverständlich mit Datenschutz“ vom 23. März 2022 den forschungsfreundlichen Ansatz der DS-GVO unterstrichen und Hinweise an die deutsche Gesetzgebung gegeben, wie die nationalen Regulatorien noch verbessert werden kön-

nen. Zugleich hat sie die Task-Force Forschungsdaten eingesetzt, die mit Mitgliedern verschiedener Arbeitskreise der DSK (insbesondere aus dem AK Technik, dem AK Wissenschaft und Forschung und dem AK Gesundheit und Soziales) besetzt ist, um schneller auf zur Forschungsthematik aufkommenden Fragen und Beratungswünsche überregionaler Forschungsprojekte reagieren zu können. An dieser beteiligten wir uns intensiv. Als erstes solcher Forschungsprojekte griffen wir in dieser Taskforce den Beratungswunsch das radiologische Netzwerk der deutschen Universitätskliniken „Racoon" auf. Die Taskforce Forschungsdaten bereitete außerdem die (bereits oben zitierte) vertiefende Petersberger Erklärung der DSK zur datenschutzkonformen Verarbeitung von Gesundheitsdaten in der wissenschaftlichen Forschung vor, die am 24. November 2022 von der DSK verabschiedet wurde.

Nicht zuletzt berieten wir aber auch die Landesregierung und die im „Forum Gesundheitsstandort Baden-Württemberg" zusammengefassten Einrichtungen einschließlich der Landesgesellschaft Bio-Pro Baden-Württemberg GmbH mit Blick auf deren Ziel, die medizinische Forschung und die Gesundheitswirtschaft zu stärken sowie die Gesundheitsversorgung der Menschen in Baden-Württemberg weiter zu verbessern – und werden diese Beratung auch weiterhin fortsetzen.

Ganz konkret wandte sich auch eines derjenigen Start-ups an uns, um die sich das Forum Gesundheitsstandort Baden-Württemberg bemüht, nämlich ein junges Unternehmen des Gesundheitssektors, das sich die Verbesserung der Forschungsinfrastruktur im Bereich der Gesundheitsversorgung auf die Fahnen geschrieben hat. Das Start-up hat die Vision, eine Plattform aufzubauen, auf der Akteur_innen der Gesundheitsversorgung nicht nur ihre Versorgungsdaten sicher und qualitätsgesichert speichern können, sondern die auch datenschutzkonform eine Forschung mit Versorgungsdaten ermöglichen soll. Diesen Ansatz fanden wir unbedingt unterstützenswert und sagten unsere Beratung zu. Wir schauten uns das Konzept kritisch an, das u. a. auf den oben bereits erwähnten Befugnissen beruht, personenbezogene Daten auch ohne Einwilligung zu Forschungszwecken zu verarbeiten, und halfen dabei, es noch zu schärfen, z. B. mit Blick auf die Klärung der datenschutzrechtlichen Verantwortungen, Entscheidungsabläufe und auf das Prinzip der Datenminimierung. Die so entwickelte Grundkonzeption halten wir für datenschutzrechtlich gut aufgestellt. Um letzte Fragen zu klären, setzen wir die Beratung fort – und auch bei der Weiterentwicklung der Plattform konsultiert uns das Unternehmen.

Die Erfolge solcher Start-ups könnte nicht nur die medizinische Forschung in Baden-Württemberg und Deutschland anhaltend fördern, sondern auch schon im Vorfeld zum Ausbau der Digitalisierung und der Standardisierung der Datenverarbeitung in der Gesundheitsversorgung beitragen – ein gutes Beispiel, das zeigt, dass Datenschutz und Digitalisierung zusammengehören und so eine nachhaltige Entwicklung unserer Gesellschaft bewirken können.

1.5 Zukunftsthemen annehmen: Künstliche Intelligenz und Datenschutz

Das Thema der Künstlichen Intelligenz (KI) sorgt seit einiger Zeit immer wieder für Schlagzeilen. Die Fähigkeiten von sogenannten intelligenten Systemen erzielen dabei regelmäßig neue Höchstleistungen und verursachen bei den Bürger_innen sowohl Begeisterung als auch Verunsicherung.

Ende des Jahres 2022 sorgte etwa die KI „ChatGPT" des Softwareunternehmens OpenAI für Aufsehen. Sie gilt als besonders gut trainiert. Journalistische Texte wurden mit ihr schon geschrieben und publiziert, Diskussionen darüber, dass Schüler_innen künftig ihre Hausaufgaben und Studierende ihre Hausarbeiten mit der Software schreiben, werden bereits intensiv geführt. Auch wird darüber diskutiert, dass die KI derzeit noch eher auf „eloquentes Plappern" setze, um Menschen zu beeindrucken, und es dabei auch zu Fehl-Erzählungen kommen könne.

Die Datenschutzaufsichtsbehörden beschäftigen sich schon seit Jahren mit dem Thema KI. Während andere europäische Aufsichtsbehörden, wie die französische CNIL und die britische ICO sich in Diskussionspapieren und Berichten bereits 2017 mit verschiedenen Fragestellungen rund um das Thema KI befassten, haben die deutschen Aufsichtsbehörden unter unserer Mitwirkung im April 2019 in der sogenannten „Hambacher Erklärung" datenschutzrechtliche Grundanforderungen aufgestellt, die bei der Entwicklung und der Anwendung von KI zu beachten sind.

Es genügt indes nicht unserem Verständnis des Beratungsauftrags unserer Behörde, lediglich abstrakte Anforderungen aufzustellen. Denn liest man die Hambacher Erklärung oder die Grundsätze der DS-GVO in Art. 5, so scheinen sich auf den ersten Blick datenschutzrechtliche Anforderungen und (vermeintliche) Notwendigkeiten von künstlicher Intelligenz diametral entgegenzustehen. Da sind beispielsweise die Grundsätze der Datenminimierung gem. Art. 5 Abs. 1 lit. c und der Speicherbegrenzung gem. Art. 5 Abs. 1 lit. e DS-GVO einerseits und das Bestreben andererseits, für das effektive Training einer KI große Datenmengen zu nutzen. Und der Grundsatz der Transparenz gem. Art. 5 Abs. 1 lit. a DS-GVO steht einem sogenannten selbstlernenden System gegenüber, welches allenfalls bedingt nachvollziehbare Ergebnisse produziert. Transparenzdefizite, seien sie vermeidbar oder nicht, ziehen zudem Folgefragen nach sich: Je weniger transparent der Entscheidungsweg de künstlichen Intelligenz ist, umso schwieriger sind die Ergebnisse der selbstlernenden Systeme auf Richtigkeit und Rechtmäßigkeit prüfbar und die Verfahren zur Produktion der Ergebnisse korrigierbar.

Neben diesen Herausforderungen bietet KI aber auch für den Datenschutz und die Arbeit der Aufsichtsbehörden enorme Potentiale. So können KI-basierte Entscheidungen bei richtiger Entwicklung und bias-bewusstem Training nicht nur gerechtere, sondern auch datensparsamere Ergebnisse erzielen. KI könnte außerdem etwa Verantwortliche bei der Erstellung einer Datenschutzfolgenabschätzung unterstützen – oder auch Aufsichtsbehörden helfen, die Vielzahl an Eingaben effektiver zu bearbeiten.

1.5.1 KI-Woche beim LfDI

Für uns boten diese und viele weitere Fragen Anlass, uns intensiver mit dem aktuellen Thema der Künstlichen Intelligenz zu beschäftigen. Hierzu haben wir vom 7. bis zum 14. Juli 2022 die Veranstaltungsreihe mit dem Titel „Künstliche Intelligenz und Datenschutz: Was heißt hier Selbstbestimmung?“ durchgeführt, die wir in die Unterthemen KI und Mobilität, KI und Gefühle, KI in der Arbeitswelt, KI und Gesundheit sowie KI und Gesellschaft gliederten.

Die Veranstaltungsreihe hatte dabei im Wesentlichen die folgenden Ziele: Sie sollte es ermöglichen, uns mit relevanten Akteuren der KI-Entwicklung und -Anwendung in Baden-Württemberg auszutauschen und mehr über das Thema und die Bedürfnisse und Herausforderungen in den einzelnen Handlungsfeldern zu erfahren. Sie sollte zudem die Akteure aus Wissenschaft, Wirtschaft, Verwaltung, Politik und Kultur miteinander vernetzen, um KI-Entwicklung und -Anwendung in Baden-Württemberg als Baustein digitaler Souveränität gemeinwohlnützlich zu fördern. Nicht zuletzt sollte die Veranstaltungsreihe für Bürger_innen die Möglichkeit bieten, sich über das Thema KI und die verschiedenen Anwendungsfelder in der Praxis zu informieren.

Um diese Ziele zu erreichen, haben wir sowohl organisatorisch als auch inhaltlich neue Maßstäbe für unsere Arbeit gesetzt. Erstmals haben wir eine Veranstaltung im hybriden Format durchgeführt: Die Expert_innen diskutierten mit uns und unseren Besucher_innen sowohl vor Ort in den für solche Veranstaltungen hervorragend geeigneten Räumen unserer Dienststelle als auch via Videokonferenz – und gleichzeitig wurde die gesamte Diskussion zudem live über unseren eigenen Peertube-Kanal gestreamt. Inhaltlich konnten wir führende Köpfe als Referent_innen zusammenbringen. Weltspitze der KI-Forschung traf auf Weltmarktführer, Gesundheitsexperten auf Philosoph_innen, Mittelständler auf Großkonzern, Bundes- auf Landespolitik.

Die Zahlen der online Teilnehmenden haben gezeigt, dass unser Livestream gefragt ist, weshalb wir ihn auch zukünftig nutzen werden. Einzelne Veranstaltungsteile stellen wir zudem als Videos auf unserer Homepage und auf PeerTube zur Verfügung.

Die Veranstaltungsreihe war für unsere Behörde ein gemeinsamer Kraftakt und gleichzeitig ein großer Erfolg. Denn neben den erreichten Zielen ist sie ein Beleg für die Leistungsfähigkeit der Dienststelle. Beschäftigte aus allen Fachabteilungen, die Koordinierungs- und Pressestelle sowie das Bildungszentrum BIDIB haben hier engagiert zusammengewirkt.

Für uns war die KI-Woche die Möglichkeit, das Gespräch mit herausragenden Expert_innen aufzunehmen, die in Baden-Württemberg arbeiten, forschen, entscheiden und die technische Entwicklung fördern, und intensiv zu diskutieren. Dies wollen wir weiter tun und uns mit den wichtigen

Akteur_innen auf diesem Feld stärker verknüpfen. Denn nur wenn wir auf Seiten der Datenschutzaufsicht die wesentlichen Funktionsprinzipien und Methoden, die Ziele, Einsatzmöglichkeiten und Risiken der neuen Technologien kennen, werden wir auch die datenschutzrechtlichen Anforderungen richtig auf sie beziehen und dabei sowohl grundrechtewahrende als auch praktikable Lösungen erkennen oder entwickeln können. Und nur wenn die Entwickler_innen und Anwender_innen der neuen Technologien frühzeitig die Auswirkungen auf Grundrechte und Gesellschaft bedenken und sich dem offenen Diskurs hierüber stellen, werden diese Technologien zu einer nachhaltigen, unsere freiheitliche Gesellschaftsordnung wahrenden Entwicklung beitragen.

Die KI-Woche im Überblick

Unsere Referent_innen sprachen oftmals statt von Künstlicher Intelligenz eher von Maschinenlernen. Den Auftakt der Reihe machte die Autorin Kathrin Passig, die über die Geschichte und Semantik des Begriffs sprach: Ist Künstliche Intelligenz immer das, was wir grade noch nicht oder gerade erst einsetzen? Anschließend fragte die Philosophin Catrin Misselhorn, ob Maschinen moralisch handeln können und sollen. Die Informatikerin und Professorin für „Digitale Methoden in der Produktion" an der Hochschule Aalen Doris Aschenbrenner warf einen Blick auf die Praxis und berichtete davon, wie Anwender_innen in Unternehmen etwa mit der Technik umgehen. Zuletzt berichtete am ersten Tag unser Referent Kristof Meding über technische Aspekte der KI.

Wie dieser erste Tag mit den Fachleuten, Wissen und Diskursivität die interessierte Zuschauerschaft in seinen Bann zog, wurden die folgenden Tage nicht minder interessant. Wir sprachen mit dem Verkehrsministerium, einem führenden Autobauer aus Baden-Württemberg, Forschern sowie Praktikern aus den Kommunen über Mobilität der Zukunft. Wir wandten uns dem Themenfeld KI und Gefühle zu, schauten in zwei Panels auf „KI in der Arbeitswelt" – zum einen in der Praxis, zum anderen aus der Forscherperspektive. Wir diskutierten über den Einsatz von KI im Sicherheitsbereich, etwa mit dem LKA-Präsidenten Andreas Stenger. Und wir diskutierten das Thema „KI und Gesundheit". Eine ausführliche Betrachtung dieses und auch des Panels zur Praxis von KI in der Arbeitswelt folgen weiter unten.

Die letzte Tag der KI-Woche betrachtete die KI im gesellschaftlichen Kontext. Christopher Coenen vom Karlsruher Institut für Technologie warf einen historisch-utopischen Blick aufs Thema, wir erfuhren vieles aus der Perspektive des Landes und ihrer Digitalisierungsstrategie von Matthias Pröfrock des Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg. Abschließend folgte ein Gespräch zwischen LfDI Stefan Brink, Christopher Coenen und der Bundestagsabgeordneten Anna Christmann – unter anderem ist sie Mitglied im Ausschuss für Bildung, Forschung und Technikfolgenabschätzung sowie Beauftragte des Bundeswirtschaftsministerium für die Digitale Wirtschaft und Start-ups – zur Frage, wie KI für die Gesellschaft nutzbar sein kann. Das Gespräch war ein herausragender Abschluss unserer KI-Themenwoche.

☛ Mehr Informationen:

Programm der KI-Woche vom 7.7.-14.7.:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/06/Final_KI-und-DS_Programm.pdf

Zahlreiche Vorträge der Referent_innen der KI-Woche stehen auf unserem PeerTube-Kanal zur Verfügung:
tube.bawü.social/c/ki_woche_lfdi/videos

Dokument der französischen CNIL zu KI:
www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf

Dokument der britischen Aufsicht ICO zu KI:
ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

„Hambacher Erklärung":
www.datenschutzkonferenz-online.de/media/en/20190405_hambacher_erklaerung.pdf

Eva Wolfangel über die KI „ChatGPT":
www.spektrum.de/news/maschinelles-lernen-chatgpt-wird-immer-plappern/2090727

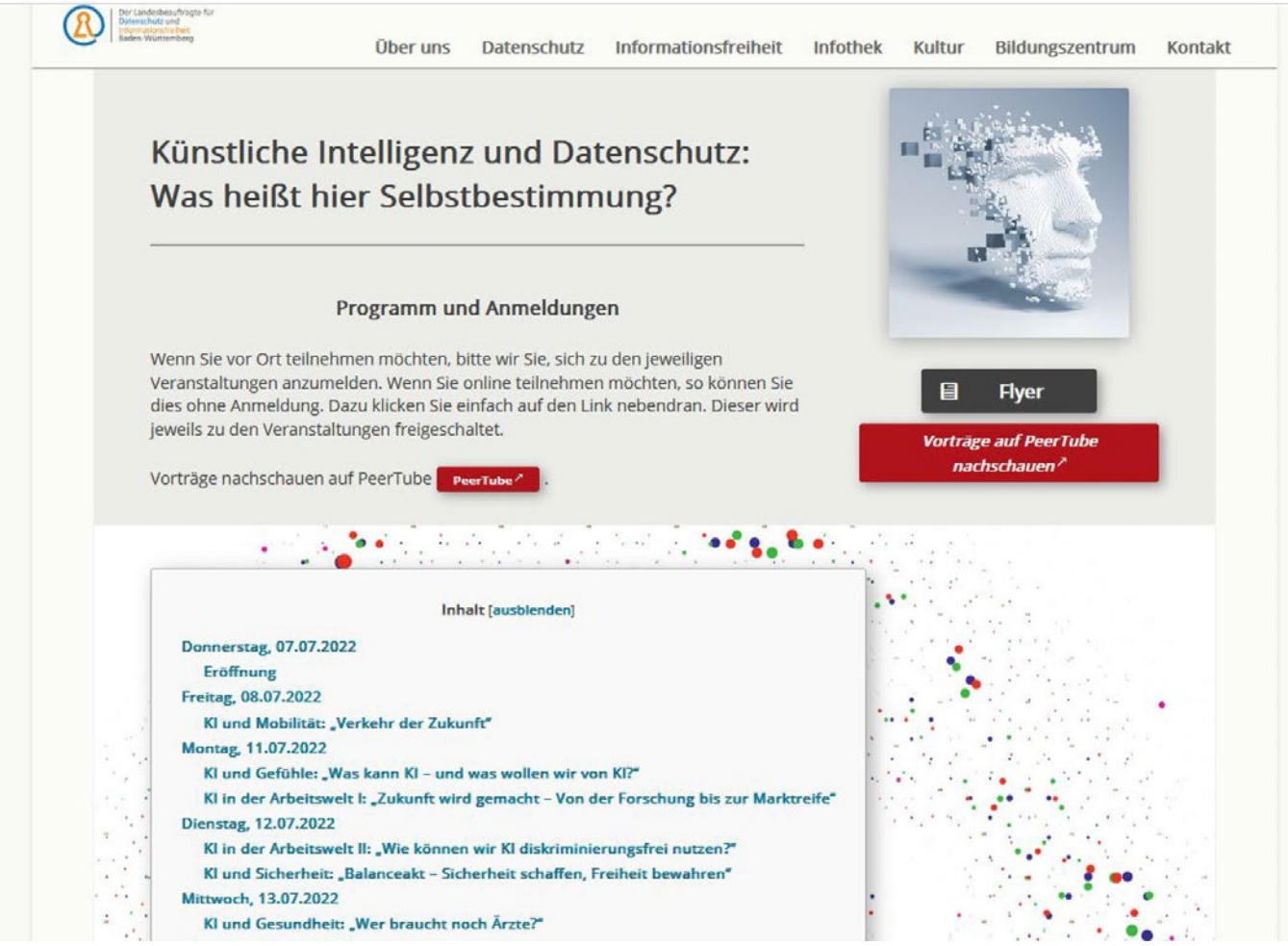
Insgesamt zählte die Reihe 29 Referent_innen, 27 (Impuls-)Vorträge und sieben Diskussionsrunden. Zu den Vorträgen und Diskussionsrunden kamen Teilnehmende in unsere Räumlichkeiten und verfolgten sie online – zwischen 25 und 70 Personen. Auf PeerTube wurde derweil manches Video mehrere Tausend Mal geklickt, so etwa der ins Thema einführende und KI einordnende Vortrag der Autorin Kathrin Passig.

Es würde den Rahmen dieses Tätigkeitsberichts sprengen, wenn wir unsere Erkenntnisse im Einzelnen aus der KI-Woche zu allen aufgeführten Themen wiedergeben würden. Beispielhaft wollen wir aber die wesentlichen Veranstaltungsinhalte zu den Bereichen „KI in der Arbeitswelt" sowie „KI und Gesundheit" detaillierter darstellen und einen näheren technischen Blick auf Künstliche Intelligenz werfen.

1.5.1.1 KI in der Arbeitswelt

In der Arbeitswelt wird KI voraussichtlich eine immer größer werdende Rolle spielen. KI-Anwendungen im Bereich der Wirtschaft und Industrie sollen bestehende Arbeitsprozesse sowie Verfahrensabläufe vereinfachen und beschleunigen, die Qualität steigern und neue Lösungswege aufzeigen.

Dabei geht es aber nicht nur um die Entwicklung rein sachbezogener Prozesse, sondern KI kann in der Arbeitswelt auch bei unmittelbar menschliche Schicksale betreffenden Entscheidungen zum Einsatz kommen – so insbesondere dann, wenn KI im Bereich der Personalgewinnung und -auswahl eingesetzt und dabei zur Analyse der Eigenschaften und Fähigkeiten der Bewerber_innen eingesetzt werden soll. Hier erhält die von unseren Expert_innen mit uns diskutierte Frage eine besondere Rele-



© LfDI BW

29 Referent_innen sprachen beim LfDI über Künstliche Intelligenz.

vanz, inwieweit KI zu Diskriminierung neigen und wie dem entgegengewirkt werden kann, wie KI also im Idealfall diskriminierungsfrei entwickelt und eingesetzt werden kann. Ein schon länger bekanntes Beispiel aus den USA stammt zwar aus einem Bereich außerhalb der Arbeitswelt, verdeutlicht aber in besonderer Weise das Diskriminierungspotential von KI und damit die enorme Bedeutung des Themas: So kam in der US-Justiz eine Software namens Compas (Correctional Offender Management Profiling for Alternative Sanctions) der Firma Northpointe zur Anwendung, die mit Hilfe eines Algorithmus die Rückfallwahrscheinlichkeit von Strafgefangenen berechnen sollte. Der Algorithmus berechnete allerdings für afroamerikanische Gefangene aufgrund verschiedener Faktoren in der Regel eine höhere Rückfallwahrscheinlichkeit als für weiße Angeklagte. Der Fall zeigt plakativ, dass das Diskriminierungspotenzial von KI vor allem dann von Relevanz ist, wenn Menschen zum Gegenstand einer Bewertung werden – und diese Bewertung unter Umständen gravierende Folgen nach sich ziehen kann.

Die von uns in unserer Dienststelle eingeladenen Expert_innen aus Wirtschaft, Wissenschaft und Gewerkschaft verschafften uns einen ersten Überblick, welche konkreten Herausforderungen sich bei der Entwicklung einer diskriminierungsfreien KI stellen und welche Lösungsansätze es in der Praxis bereits gibt. Wir erfuhren, dass der Begriff der Diskriminierung recht unterschiedlich verstanden werden kann, es allgemein aber um eine Form von Benachteiligung aufgrund eines unzulässigen Differenzierungsmerkmals geht. Ein Grund für eine Benachteiligung durch KI-Systeme kann in einer fehlerhaften Würdigung der Entscheidungsgrundlage liegen, was auf eine mangelnde Ausgewogenheit der Datensätze (sogenannte Bias in the data) zurückzuführen sein kann. Denn bevor die KI-Systeme ihre eigentliche Funktion erfüllen können, müssen diese mit entsprechenden Datensätzen trainiert werden. Hierfür werden in der Regel maschinelle Lernverfahren verwendet mit dem Ziel, Zusammenhänge in den Datensätzen zu erkennen und zu klassifizieren, um darauf aufbauend Vorhersagen treffen zu können. Werden die KI-Systeme nun mit statistisch unausgewogenen Datensätzen trainiert, dann spiegelt sich eben diese Voreingenommenheit auch in der späteren Anwendung wieder. Damit Diskriminierungen durch KI-Systeme vermieden werden können, ist demnach insbesondere eine umfassende und ausgewogene Datengrundlage wichtig, mit der das KI-System trainiert wird.

Bei dem Austausch mit den Fachleuten konnten wir darüber hinaus in Erfahrung bringen, dass sich bereits verschiedene technische Lösungen etabliert haben, die der Problematik entgegensteuern. Zudem gibt es die Möglichkeit, dass zur Entwicklung und Validierung von bestimmten KI-Systemen nicht zwangsläufig personenbezogene Daten benötigt werden. Ausreichend können für das Training unter Umständen auch anonymisierte Daten sein, also Daten, bei denen der Personenbezug dauerhaft aufgehoben ist, so dass es sich nicht mehr um Informationen über eine identifizierte oder identifizierbare natürliche Person handelt. Sogar künstlich generierte (sogenannte „synthetische“) Daten – die mithin von Anfang an keinen Bezug zu lebenden Personen aufweisen – können für das Training von Künstlicher Intelligenz verwendet werden.

Ferner konnten wir durch den Austausch erfahren, wo inzwischen Systeme mit Künstlicher Intelligenz im Arbeitskontext angewendet werden und wie der derzeitige Entwicklungsstand solcher KI-Systeme ist. Insgesamt konnten wir im Rahmen dieses Panels mitnehmen, dass (ggf. auch personenbezogene) Daten die Grundlage für bestimmte funktionierende KI-Systeme sind, weshalb die Thematik rund um die Künstliche Intelligenz in einem gewissen Spannungsverhältnis zum Datenschutzrecht stehen kann. Wir haben zugleich auch erfahren: In vielen Bereichen, wo KI eingesetzt wird, werden

☛ Mehr Informationen:

Über Bias beim KI-Einsatz:
www.zeit.de/wirtschaft/2019-07/algorithmus-facebook-google-datensicherheit/komplettansicht?utm_referrer=https%3A%2F%2Fwww.google.com%2F

heise.de/newsticker/meldung/US-Justiz-Algorithmen-benachteiligen-systematisch-Schwarze-3216770.html

KI made in BW: Innovationspark Heilbronn:
tube.bawü.social/w/whtWcKUpHcDFxNqGqrkj8i

überhaupt keine personenbezogenen Daten verarbeitet. Eine wesentliche Aufgabe für uns wird es daher auch weiterhin sein, neben dem umfassenden Angebot von Beratungsleistungen aktiv auf Beteiligte zuzugehen, um so den technologischen Fortschritt zu stärken und etwaige Spannungsverhältnisse aufzulösen.

Zu diesem Zweck hat unser Kollege aus der Abteilung, der sich mit Fragen des Datenschutzes in der Privatwirtschaft befasst, kurz nach unserer Themenwoche die Initiative ergriffen und einen Kontakt zum Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg als einem wesentlichen Akteur der Innovationsstrategie des Landes hergestellt, um die Bereitschaft unserer Behörde zu signalisieren, bei der Fortentwicklung der technischen Möglichkeiten und beim Einsatz von KI frühzeitige Unterstützung zu leisten und Unternehmen – wobei es sich in diesem jungen und innovativen Betätigungsfeld vielfach um Starthandeln wird – zu beraten, damit ihnen eine die rechtlichen Rahmenbedingungen wahrende, nachhaltige Technologieentwicklung gelingt.

1.5.1.2 KI und Gesundheit

Als Titel der Veranstaltungspanels zum KI-Einsatz im Gesundheitswesen haben wir provokativ gewählt: „Brauchen wir noch Ärzte?" Der Titel deutete allerdings schon an, worum es beim Einsatz von Künstlicher Intelligenz geht: Um statistische Auswertung und Unterstützung der Ärzt_innen bei ihrer Arbeit. In den Vorträgen und der anschließenden Diskussion klärte sich die Frage recht eindeutig: Das Vertrauensverhältnis von Ärzt_innen und Patient_innen muss ein solches bleiben.

Die Expert_innen aus Medizin, Informatik, Physik und Ethik stellten uns verschiedene Einsatzgebiete und Verwendungsmöglichkeiten von Künstlicher Intelligenz im Gesundheitswesen vor. Die dargestellten Einsatzgebiete der KI betrafen im Gesundheitswesen sowohl die Behandlung von Patient_innen als auch die medizinische Forschung. Hierbei können die Methoden des Maschinellen Lernens zu wesentlichen Erkenntnissen beziehungsweise Verbesserungen der Behandlungsqualität beitragen. Durch die Verarbeitung einer großen Menge an Gesundheitsdaten als Trainingsdaten in neuronalen Netzen können – so die bei uns referierenden Expert_innen – relevante Modelle entstehen, die für die Behandlung, wissenschaftliche Forschung und Prävention nutzbar gemacht werden können. Denn mit KI-basierten Anwendungen können umfangreiche Datenbestände – beispielsweise über Infektionen mit SARS-Cov-2, einschließlich der Symptome, Krankheits- und Behandlungsverläufe, möglicher Ansteckungswege und weiterer Umstände (Impfungen, Vorerkrankungen, Alter, Geschlecht, Lebensweisen etc.) zur infizierten Person – besser und schneller mit dem Ziel der Erlangung von Erkenntnissen – etwa über Ansteckungsrisiken, Risikofaktoren für schwere Verläufe, Präventionsmöglichkeiten bei Covid-19 – ausgewertet werden. Die Fähigkeit zur Mustererkennung durch künstliche Intelligenz könne beispielsweise auch in der Krebsdiagnostik sehr gut dafür eingesetzt werden, frühzeitig und mit hoher Treffsicherheit maligne Strukturveränderungen in Geweben auszumachen.

Allerdings hänge die Qualität der mittels der neuronalen Netzwerke gewonnen medizinischen Erkenntnisse von der Qualität der verfügbaren objektiv aussagekräftigen und repräsentativen Datensätzen ab. Die Trainingsdaten bestünden aus Gesundheitsdaten, mit denen Modelle im neuronalen Netz trainiert würden, die eine medizinische Aussage erlauben sollen. Dies würde vielfach dazu führen, dass vollständig anonymisierte Daten als Trainingsdaten wohl nicht ausreichend seien, um hinreichend valide Erkenntnisse zu erlangen. Auch synthetische Daten (also durch einen Computeralgorithmus generierte Daten) könnten reale Daten als Trainingsdaten nicht vollständig ersetzen. Bislang würden typischerweise personenbezogene Daten aus bildgebenden Verfahren, wie beispielsweise Röntgen-, MRT-Aufnahmen, Messwerten über die Herz- und Atem-Frequenz zum Einsatz kommen. Aber auch Abrechnungsdaten seien als Trainingsdaten sinnvoll.

Die Expert_innen schilderten als besondere Hürde für den Einsatz von KI und die Erlangung geeigneter Trainingsdaten, dass bislang die Art und Weise der Dokumentation medizinischer Daten im Rahmen der Gesundheitsversorgung zu wenig standardisiert sei. Die Daten seien teilweise gar nicht digitalisiert, sondern fänden sich in individuell angefertigten, zuweilen noch handschriftlichen Unterlagen (und die Unlesbarkeit ärztlicher Handschriften ist ja beinahe schon sprichwörtlich). Aber auch soweit die Daten digitalisiert seien, seien die Formate nicht

einheitlich und gebe es auch sonst keine einheitliche Handhabung im Sinne einer Standardisierung.

Dadurch steige das Risiko, dass eine KI Fehlinterpretationen vornehme. Außerdem seien die Daten über die Historie einer Behandlung auch nicht immer vollständig, da beispielsweise Trainingsdaten mit Befunden nach der Heilung (sogenannte Follow-Up-Daten) seltener zur Verfügung stünden. Gleichzeitig würde aber der Aussagewert der Modelle steigen, wenn eine hohe Anzahl von Trainingsdaten zugänglich wäre, die idealerweise über den Lebensweg der Patienten gespeichert würden. Hier könne es unter Umständen in Zukunft mit der elektronischen Patientenakte Verbesserungen geben. Ferner sei ein besonderes Augenmerk auf die Qualität und Streubreite der eingegebenen Trainingsdaten sowie auf die Gefahr zu setzen, dass die neuronalen Netze im Rahmen des Erlernens den Daten einen falschen Aussagewert zumessen. Denn auch (s. hierzu schon oben bei „KI in der Arbeitswelt) aus der Forschung mit Gesundheitsdaten sei bekannt, dass infolge des Lernvorgangs des neuronalen Netzes diskriminierende Effekte entstehen könnten. Dies könne beispielsweise auf die Auswahlkriterien der Trainingsdaten oder den KI-Algorithmus zurückzuführen sein.

In der weiteren Diskussion ging es um den praktischen Einsatz von KI-basierten Anwendungen durch Ärzt_innen im therapeutischen Bereich. Die bisher eingesetzten KI-basierten Anwendungen seien reine Therapieempfehlungen. Die Algorithmen träfen also nicht selbst Entscheidungen über die einzuschlagende Therapie, sondern gäben lediglich Empfehlungen ab. Den KI-basierten Anwendungen komme mit anderen Worten eine assistierende Funktion zu. Stets habe nicht die KI, sondern hätten die behandelnden Ärzt_innen die endgültige Entscheidung zu treffen. Indes gaben die Experten an, dass Menschen sich durchaus von technischen Entscheidungsempfehlungen beeinflussen lassen. Dieser Einfluss werde um so größer, je mehr das Risiko steige, dass ein Abweichen von der KI als Behandlungsfehler gewertet werden könnte. Auch könnten die Ärzt_innen nur dann eine eigenständige, gegebenenfalls auch von dem Ergebnis der KI abweichende Entscheidung treffen, wenn der Vorschlag der KI von dieser nachvollziehbar erklärt werde und so insbesondere ermöglicht werde, eine durch die Auswahl und Art der Trainingsdaten oder durch das neuronale Netzwerk selbst erzeugte Fehleinschätzung („Bias“) zu erkennen.

Diese Veranstaltung war für uns sehr lehrreich, wir konnten die Vorstellungen und Einschätzungen der Expert_innen aufnehmen, was für sie wichtig ist, welche Ziele sie verfolgen und welche Mittel sie dafür brauchen. So können wir unsere Beratungsqualität kontinuierlich verbessern. Die Wahrscheinlichkeit, dass wir im Gespräch datenschutzrechtlich tragfähige Lösungen finden, steigt, wenn wir tiefgreifend verstehen, welche Bedürfnisse die Mediziner_innen haben – und wenn sie die Anforderungen des Datenschutzes frühzeitig beachten. Es ist uns ein Anliegen, dass gerade bei medizinischen Anwendungen, die so wertvoll für Menschen sind und bei denen besonders sensible Gesundheitsdaten verarbeitet werden, die datenschutzrechtlichen Anforderungen beachtet werden. Denn Patient_innen kommen etwa aufgrund einer schweren Krankheit enorm unter Druck, freie und selbstbestimmte Entscheidungen zu treffen, und verlassen sich darauf, dass die Mediziner_innen schon alles richtig machen. Daher setzen wir uns sehr dafür ein, dass Datenschutz und medizinische Fortschritte im Sinne der Patient_innen gestärkt werden.

1.5.1.3 Technischer Blick auf KI

Auch die technische Umsetzung von KI war eine der maßgeblichen Fragen der KI-Woche. Die Referent_innen legten hierbei verschiedene Schwerpunkte auf die verwendeten Technologien. Es wurde anschaulich, dass zwar die Mathematik die Sprache der Informatik ist, die KI jedoch auch immer wieder verständlich erklärt werden kann.

Zunächst erscheint es wichtig, dass KI von der Statistik abgegrenzt wird. Die Statistik dient vornehmlich der Analyse von Daten. Bei statistischen Auswertungen werden die Aspekte der Analyse von den Nutzenden häufig selbst festgelegt. Künstliche Intelligenz geht jedoch darüber hinaus. Zu einem gewissen Grad ist es möglich, dass die KI Probleme selbstständig(er) löst.

Die Bilderkennung war maßgeblicher Treiber der Entwicklungen im Bereich KI der 2010er Jahre. Es zeigten sich in der Folgezeit erstaunliche Fähigkeiten, Objekte auf Bildern zu erkennen, wenngleich es zuweilen immer noch Fehler gibt, welche Men-

schen klar vermeiden würden, indem zum Beispiel ein evident unbeachtliches Kriterium wie das Wasserzeichen der radiologischen Aufnahmen von der KI als potentiell für die Erkennung einer bösartigen Veränderung im abgebildeten Gewebe entscheidungsrelevant eingestuft werden könnte.

Zuletzt wird die Entwicklung der KI jedoch durch sogenannte Transformer Modelle, welche ihre Grundlagen in der Sprachverarbeitung haben, dominiert. Stellvertretend für diese beeindruckenden Fähigkeiten stehen Modelle wie „GPT-3" oder auch „ChatGPT". Wie mächtig diese Modelle sind, zeigt die folgende Antwort von GPT-3 zur Frage, ob der LfDI Baden-Württemberg die beste Datenschutzbehörde ist:

„Das ist eine schwierige Frage, die ich nicht pauschal beantworten kann. Die LfDI BW hat in den letzten Jahren viel dazu beigetragen, den Datenschutz in Deutschland weiterzuentwickeln. Allerdings gibt es auch andere Datenschutzbehörden, die ebenfalls sehr engagiert sind."

Die Antwort ist typisch für die aktuellen Sprachmodelle. Bei auf Fakten abzielenden Fragen bekommen wir sehr konkrete Antworten, die entweder richtig oder falsch sind. Bei Bewertungsfragen erhalten wir dagegen Antworten, die sich nicht immer konkret fassen lassen. Dies ist jedoch auch nachvollziehbar, da sich diese Antworten ungleich schwerer aus den Trainingsdaten lernen lassen.

Auch die Verbindung von Sprach- und Bildmodellen wird zunehmend populärer. Die text-to-image Modelle bauen auf den bisherigen Technologien auf und bringen durch weitere Ansätze (insbesondere sogenannte diffusion models) beeindruckende neue Fähigkeiten zur Bilderzeugung durch sprachliche Eingaben hervor. Damit lassen sich sogar fotorealistische Abbildungen erstellen. Dabei ist es mittlerweile fast eine eigenständige „Kunst" geworden, die prompts, also die Eingaben für text-to- image Modelle, zu entwerfen. Erst mit den richtigen prompts entsteht das gewünschte Bild (sogenanntes prompt engineering). Es bleibt damit weiterhin zu beobachten, welche Entwicklungen sich in der Zukunft zeigen und welche Auswirkungen sich auf den Datenschutz ergeben.

1.6 Ausblick: Beratungsansatz intensivieren

Wir kommen mit Bürger_innen ins Gespräch, holen uns Wissen ins Haus und beteiligen uns an Debatten und Diskussionen über den Datenschutz mit den Ziel, für die Bürgerrechte zu wirken. Wir beraten Behörden und Unternehmen, besuchen Städte und Gemeinden vor Ort, um wirksam helfen zu können und unterstützen wo immer möglich die nachhaltige Entwicklung der Digitalisierung.

Die DS-GVO ist noch relativ jung. Gleichwohl sind ihre wesentlichen Grundsätze gut reflektiert und stehen der Digitalisierung offen gegenüber. Hiervon können sowohl die Bürger_innen als auch die verantwortlichen Stellen profitieren.

Unseren Beratungsansatz, unser Fort- und Weiterbildungsangebot, wollen wir weiter forcieren. Die hier beschriebenen Beispiele zeigen, wie wir den Austausch stärken, ein besseres Verständnis von datenschutzrechtlichen Belangen fördern und lösungsorientiert vorgehen. Statt als sanktionierende Behörde Europameister beim Erlassen von Bußgeldern zu sein, sehen wir den Erfolg unserer Arbeit darin, so weit wie möglich daran mitzuwirken, dass Bürger_innen erst gar nicht in ihren Rechten verletzt werden. Dabei sind wir uns bewusst, dass in gravierenden Fällen Sanktionen erforderlich sind, um Recht durchzusetzen. Vorrangig wollen wir aber dafür eintreten, dass Datenschutz als selbstverständlicher Teil der Digitalisierung verstanden wird und so eine nachhaltige digitale Entwicklung in der alltäglichen behördlichen, unternehmerischen und gesellschaftlich kulturellen Praxis gestärkt wird.

2. Corona-Pandemie

Die Corona-Pandemie prägte in den Jahren 2020 und 2021 maßgeblich unsere Arbeit. Zur Bekämpfung der Pandemie mussten Bürger_innen Grundrechtseingriffe hinnehmen. Hierzu wurden gesetzliche Regelungen getroffen, insbesondere zahlreiche „Corona-Verordnungen" erlassen. Auch das Recht auf informationelle Selbstbestimmung – der Datenschutz – unterlag in der Pandemie erheblichen Eingriffen. Die pandemiebedingten Einschränkungen der Bürgerrechte dienten dem Schutz eines hohen Guts unserer Verfassung, nämlich des Rechts auf Leben und körperliche Unversehrtheit. Hier einen vernünftigen Ausgleich mit unseren Freiheitsrechten zu finden, war und ist auch die Aufgabe des Datenschutzes. Wir haben, soweit wir eingebunden wurden und uns einbringen konnten, beratend an Verordnungen der Landesregierung mitgewirkt und so darauf hingearbeitet, dass die Regelungen datenschutzrechtlich tragfähig sind.

Das Jahr 2022 markiert vermutlich einen Übergang: Zahlreiche pandemiebedingte Einschränkungen wurden im Laufe des Jahres aufgehoben. Dies hatte seine Ursache insbesondere darin, dass unser Gesundheitssystem nicht mehr unter demselben enormen Druck wie zuvor stand und daher das Recht auf körperliche Unversehrtheit der Bürger_innen auch mit weniger werdenden Grundrechtseingriffen gewährleistet werden konnte. Inzwischen äußerten sich etwa Professor Thomas Mertens, Vorsitzender der Ständigen Impfkommission (STIKO), sowie weitere führende Fachleute, darunter der Virologe Professor Christian Drosten und der Intensivmediziner Professor Christian Karagiannidis (beide wie Professor Mertens Mitglieder im Expert_innenrat, der die Bundesregierung zur Covid-19-Pandemie berät) dahingehend, dass die Pandemie überwunden sei.

Gleichwohl haben uns die Pandemie und die Maßnahmen zu ihrer Bekämpfung auch noch im Jahr 2022 beschäftigt, wenn auch in deutlich abnehmendem Maße. So hatten wir beispielsweise weiterhin mit zum Teil erheblichen Datenschutzmängeln bei Corona-Testzentren zu tun (siehe Kapitel 2.1). Auch berieten wir das Sozialministerium zur Durchführung der sogenannten einrichtungsbezogenen Impfpflicht (siehe Kapitel 2.2) und zur Errichtung eines Impfterminportals (siehe Kapitel 9.2.3) und befassten uns weiter mit der Software SORMAS für Gesundheitsämter (siehe Kapitel 9.2.4).

Die Pandemie war aber auch und gerade mit Blick auf ihr Auslaufen Gegenstand unserer Aufsichtstätigkeit: So prüften wir beispielsweise bei verschiedenen Verantwortlichen nach, ob sie noch nach Wegfall der jeweiligen Corona-Regelung pandemiebedingte Daten speichern oder sonst verarbeiten. Die diesbezüglichen Ergebnisse waren ganz überwiegend erfreulich (siehe Kapitel 2.3). Dennoch werden wir hier künftig noch weitere Untersuchungen vornehmen. Und auch die wenigen noch verbliebenen regulatorischen Vorgaben werden wir noch weiter im Auge zu behalten haben und prü-

☛ Mehr Informationen:

Äußerungen von Prof. Mertens zum Ende der Pandemie:
www.br.de/nachrichten/deutschland-welt/stiko-chef-corona-ist-mittlerweile-endemisch,TLTQjSW

Prof. Christian Drosten zum Ende der Pandmie:
www.tagesschau.de/inland/gesellschaft/corona-pandemie-drosten-101.html
www.zdf.de/nachrichten/panorama/drosten-corona-pandemie-vorbei-100.html
www.tagesspiegel.de/wissen/corona-experte-drosten-nach-meiner-einschatzung-ist-die-pandemie-vorbei-9089959.html

Die Expert_innenkommission der Bundesregierung:
www.bundesregierung.de/breg-de/themen/bundeskanzler-scholz-beruft-expertengremium-zur-wissenschaftlichen-begleitung-der-covid-19-pandemie-1991366

Beitrag „Datenschutz in Corona-Testzentren" Kapitel 1.4 unseres 37. Tätigkeitsberichts zum Datenschutz 2021:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf

fen, ob die mit der Pandemie-Bekämpfung begründeten Eingriffe in die informationelle Selbstbestimmung noch notwendig sind. Sofern sie nicht mehr notwendig sind, werden wir darauf hinwirken, dass diese Grundrechtseingriffe beendet werden (siehe Kapitel 2.4).

2.1 Testzentren

Auch im Berichtsjahr 2022 hatten wir verschiedentlich Anlass, uns mit der Umsetzung datenschutzrechtlicher Anforderungen durch Testzentren auseinanderzusetzen. Bereits aus unserem letzten Tätigkeitsbericht ist zu entnehmen, dass uns verschiedene dieser Zentren negativ aufgefallen waren. Verschiedene Eingaben bei uns sowie Datenpannenmeldungen ließen auch weiterhin deutliche Mängel bei manchen Betreiber_innen erkennen. Darüber hinaus haben wir von Amts wegen stichprobenartige Kontrollen bei einigen Corona-Testeinrichtungen vor Ort durchgeführt. Diese führten zu weiteren Erkenntnissen, die wir mittels einer rein schriftlicher Aufforderung zur Stellungnahme so nicht erhalten hätten.

Die uns erreichenden Eingaben zu Testzentren gingen im Laufe des Jahres ganz erheblich zurück, vermutlich wegen des Wegfalls der verschiedenen Testobliegenheiten und nicht zuletzt aufgrund der Mitte des Jahres erfolgten weitgehenden Wiederabschaffung der kostenlosen Bürgertests. Bei den Eingaben ging es – wie schon im Berichtszeitraum unseres letzten Tätigkeitsberichts – vielfach beispielsweise darum, dass es bei der Übermittlung von Testterminen oder gar Testergebnissen zu Fehlversendungen kam. Die Beschwerdeführenden erhielten mithin zum Teil gar keine Testergebnisse oder gar Terminbestätigungen beziehungsweise Testergebnisse von Dritten mit deren Personalien zugesandt. Oder die Beschwerdeführenden berichteten, dass die Testzentren Listen auslegten, in die die zu testenden Personen ihre Personalien – für die nächsten sichtbar – eintragen sollten. Andere Beschwerdeführende bekamen von Testzentren nicht erwünschte Werbung zugesandt. Kritikwürdig war vor allem nach wie vor vielfach die Form der Übermittlung von Testergebnissen. Diese erfolgte etwa via nicht ausreichend verschlüsselter E-Mails, mit leicht zu erratenden Passwörtern (Geburtsdatum, Postleitzahl etc.) oder mit Passwörtern, die auf demselben Weg – zuweilen sogar mit derselben E-Mail – übersandt wurde. Auch erreichten uns Beschwerden, in denen die Beschwerdeführenden geltend machten, dass die Testzentrenbetreiber_innen auf die Geltendmachung von Betroffenenrechten – insbesondere Berichtigungs-, Lösch- oder Auskunftsbegehren nicht reagierten.

Bei unseren Vor-Ort-Stichproben war vielfach schon nicht oder nur schwer zu erkennen, wer für die Datenverarbeitung durch das jeweilige Testpersonal verantwortlich war. Dies ist aber die Grundvoraussetzung dafür, dass betroffene Personen etwaige datenschutzrechtliche Anliegen – etwa Auskunft, Berichtigung oder Löschung, aber auch beispielsweise Schadensersatzforderungen – richtig adressieren und gegebenenfalls durchsetzen können. Dabei kann es ohne den rechtlich gebotenen expliziten Hinweis (Artikel 13 DS-GVO) bei den Betroffenen durchaus zu Fehlvorstellungen über den Verantwortlichen kommen: Etwa wenn Teststellen unmittelbar vor einer Gaststätte betrieben werden, dabei ersichtlich auch Beschäftigte der Gaststätte eingesetzt werden, konnte der Eindruck entstehen, die Gaststätte sei zugleich die Betreiberin der

© Heiko Küverling – stock.adobe.com

Wir schauen bei Testzentren genau hin, ob sie mit sensiblen Daten der Bürger_innen auch gut umgehen.

Teststelle und damit auch datenschutzrechtlich verantwortlich. Auf Nachfragen erfuhren wir aber beispielsweise, dass das Personal der Gaststätte wegen des pandemiebedingt verminderten Gästeaufkommens und damit auch geringeren Arbeitskraftbedarfs der Gaststätte – insoweit wirtschaftlich durchaus sinnvoll und nachvollziehbar – einen weiteren Anstellungsvertrag mit einem von der Leitung der Gaststätte verschiedenen Teststellenbetreiber geschlossen und dieser lediglich gewisse organisatorische Kooperationsabsprachen mit der Gaststättenleitung beispielsweise zur Mitnutzung bestimmter Räumlichkeiten getroffen hatte. Damit war also tatsächlich – für die Getesteten schwerlich erkennbar – der vom Gastwirt verschiedene Teststellenbetreiber verantwortlich.

Erst recht waren die weiteren nach Artikel 13 DS-GVO erforderlichen Datenschutzinformationen vielfach nicht ohne weiteres auffindbar oder sogar gar nicht vorhanden. Die vom europäischen Gesetzgeber angestrebte Transparenz nicht nur über den Verantwortlichen der Datenverarbeitung, sondern auch zum Beispiel über die Rechtsgrundlagen der Datenverarbeitung, Empfänger, Speicherdauer und Betroffenenrechte, wurde insoweit vielfach verfehlt.

Weitere Mängel offenbarten sich uns bei unseren Vor-Ort-Stichproben im Bereich der technischen und organisatorischen Maßnahmen, von denen wir hier nur beispielhaft berichten wollen: Erstaunlich war etwa der Ein-Personen-Betrieb einer Teststelle: Der Laptop zur Registrierung im Empfangsbereich war weder gegen Einsichtnahme noch gegen Wegnahme gesichert, obwohl er unter anderem während der Probennahme am Testplatz infolge einer Sichtschutzwand nicht im Blickfeld des Mitarbeiters war – und das mit der Fußgängerzone direkt vor der offenstehenden Eingangstüre. Dabei lässt sich – unabhängig vom auch datenschutzrechtlich gebotenen Schutz vor Diebstahl – unerwünschtes Mitlesen eigentlich mittels sogenannter Blickschutzfilter für Monitore leicht verhindern, und beim Verlassen des Arbeitsplatzes sollte ein aktivierter Bildschirmschoner mit Kennwortschutz selbstverständlich sein.

Die Aufbewahrung der Testdokumentation wurde unterschiedlich gehandhabt. Die Bandbreite war weit: Zum Teil wurden die Unterlagen täglich abgeholt und in eine ordnungsgemäß gesicherte Verwahrung verbracht. Auf dem anderen Ende der Skala konnten wir dagegen feststellen, dass in einem Fall Unterlagen über mehrere Tage (und damit auch über Nacht) in einem schlichten Testzelt in einfachen Büroschränken gelagert wurden.

Was die Kommunikation innerhalb der Mitarbeitenden eines Testzentrums angeht, wurde uns zum Teil berichtet, dass diese über WhatsApp-Gruppen laufe. Auch würden im Falle eines positiven Testergebnisses die Personalien der betroffenen Person über eine solche Gruppe weitergegeben, damit von der Zentrale aus die nach dem Infektionsschutzgesetz erforderliche Meldung an das Gesundheitsamt vorgenommen werden könne. Die Verwendung von WhatsApp-Gruppen ist schon zur bloßen Kommunikation über die Arbeitsorganisation rein innerhalb des Testteams grenzwertig, zumal wenn sie für die Beschäftigten verbindlich vorgegeben wird. Als Kommunikationsweg für positive Testnachweise sind sie jedoch gänzlich ungeeignet und datenschutzrechtlich unzulässig.

Nachdem wir im 4. Quartal auf unsere wiederholt geäußerte Bitte von der Kassenärztlichen Vereinigung Baden-Württemberg eine umfassende Liste mit Kontaktdaten der dort bekannten Corona-Testeinrichtungen erhalten haben, planen wir, auf Grundlage dieser Liste weitere Testeinrichtungen prüfen. Wer weiterhin – trotz der Beschränkung der Berechtigung zu kostenlosen Bürgertests auf Ausnahmefälle und trotz der zum 25. November

☛ Mehr Informationen:

Wiederabschaffung der kostenlosen Bürgertests:
www.swr.de/swraktuell/baden-wuerttemberg/faq-neue-coronaverordnung-tests-drei-euro-100.html

sozialministerium.baden-wuerttemberg.de/de/gesundheit-pflege/gesundheitsschutz/infektionsschutz-hygiene/informationen-zu-coronavirus/testen

Unsere Hinweise zum Datenschutz in Testzentren:
www.baden-wuerttemberg.datenschutz.de/testzentren-lfdi-empfiehlt-dringend-sicherheitsvorkehrungen-bei-der-datenverarbeitung-zu-ueberpruefen

und www.baden-wuerttemberg.datenschutz.de/pandemie-bekaempfung-datenschutz-in-testzentren

2022 erfolgten Abschaffung der sogenannten 3-Euro-Bürgertests – Testungen auf das Coronavirus anbietet, der_dem sei deswegen noch einmal dringend nahegelegt, unsere Hinweise zum Datenschutz in Testzentren, welche auf unserer Homepage zu finden sind, zu beachten. Unsere Prüfung wird sich aber auch darauf erstrecken, wie bei eingestelltem Teststellenbetrieb die nach § 7 Absatz 5 Satz 1 der Coronavirus-Testverordnung (TestV) bis zum Jahresende 2024 vorgeschriebene Speicherung der Auftrags- und Leistungsdokumentation erfolgt und die Durchsetzung von Betroffenenrechten ermöglicht wird.

2.2 Die sogenannte einrichtungsbezogene Impfpflicht

Der Begriff der einrichtungsbezogenen Impfpflicht war und ist, soweit wir das erkennen können, in der öffentlichen Diskussion weit verbreitet und fest etabliert; er wird beispielsweise auch vom Bundesministerium für Gesundheit (BMG) in seiner „Handreichung zur Impfprävention in Bezug auf einrichtungsbezogene Tätigkeiten" vom 22. März 2022 und vom Sozialministerium Baden-Württemberg verwendet. Ein näherer Blick auf die Materie zeigt dies: Die hier bedeutsamen Rechtsvorschriften ergeben sich insbesondere aus § 20a des Gesetzes zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen (Infektionsschutzgesetz, IfSG). Im Text des § 20a IfSG 1 findet sich der Begriff „Impfpflicht" nicht, auch nicht in der Paragrafenüberschrift.

Tatsächlich ging es auch nicht um eine (echte und vollstreckbare) Rechtspflicht, sich unter bestimmten Voraussetzungen impfen zu lassen oder eine bestimmte Art von Impfung zu dulden. Es läuft also niemand Gefahr, aufgrund dieser Regelungen gegen seinen Willen auf einem Behandlungsstuhl festgeschnallt und mit einer Impfinjektion versehen zu werden.

Vielmehr ging es um die Erfassung nicht geimpfter und nicht genesener Personen, die in den vulnerablen Einrichtungen beschäftigt waren, um deren Meldung an das Gesundheitsamt und die Prüfung, ob aus Gründen des Infektionsschutzes ihre Weiterbeschäftigung in der jeweiligen Einrichtung zu untersagen sei. Ein ganz wesentlicher Teil der Regelung betraf mithin die Verarbeitung personenbezogener (Gesundheits-)Daten.

Gegen die Regelung wandten sich einige Betroffene mit Verfassungsbeschwerden an das Bundesverfassungsgericht. Dieses wies die Beschwerden mit seinem Beschluss vom 27. April 2022 – 1 BvR 2649/21 zurück und sorgte insoweit für Rechtssicherheit hat. So heiß, wie über die sogenannte Impfpflicht diskutiert wurde: Die Vorschriften des § 20a IfSG sind zum 1. Januar 2023 außer Kraft getreten.

Wir wissen nicht, wie die Vorschriften des § 20a IfSG in allen Einzelfällen durch die zuständigen Fachbehörden des Landes umgesetzt wurden und werden. Das Sozialministerium hat jedenfalls am 20. September 2022 darauf hingewiesen, dass Beschäftigte *„ab 1. Oktober keinen Nachweis über dritte Impfung oder Genesung vorlegen"* müssen (siehe Kasten), was folgen lässt, dass jedenfalls nach den Vorstellungen des Ministeriums nicht alle rechtlichen Möglichkeiten ausgeschöpft werden sollen; und damit, aus der Sicht des Datenschutzes erfreulich, manche rechtlich zulässige Datenverarbeitung wohl unterbleibt. Die gesetzliche Regelung der einrichtungsbezogenen Impfpflicht erschien bei genauerer Lektüre als „mit heißer Nadel gestrickt", indem sie viele – auch datenschutzrechtlich relevante – Fragen ungeklärt lässt.

Beispielsweise mangelte es mit Blick auf den Beginn des Textes von § 20a Absatz 1 Nummer 1 IfSG (*„Personen, die in folgenden Einrichtungen oder Unternehmen tätig sind"*) an der klaren und ohne Weiteres dem Gesetzestext zu entnehmenden Abgrenzbarkeit des Kreises der Personen, die in diesem Sinne „tätig sind". Sollen nach dem Willen des Bundesgesetzgebers zu diesem Kreis etwa auch (minderjährige) Praktikanten und Auszubildende gehören? Und wie verhält es sich mit Blick auf Mitarbeiter einer externen Reinigungsfirma? Gehören dem betroffenen Personenkreis nur bei der jeweiligen Einrichtung selbst angestellte Hausmeister an? Oder gehören auch Mitarbeiter einer Fremdfirma für Hausmeisterservice (oder, wie häufig formuliert: Facility-Management) dazu? Macht es einen Unterschied, ob ein bei einer Fremdfirma angestellter Handwerker im Klinikgebäude neue Stromkabel verlegt, oder ob er nur in einem davon räumlich getrennten Parkhaus der Klinik tätig ist?

Obwohl im Text von § 20a Absatz 1 Nummer 1 IfSG bestimmte *„Einrichtungen oder Unternehmen"* unter den Buchstaben a bis o aufgelistet sind, waren bestimmte Detailfragen nicht für jeden sogleich klar zu beantworten. So war beispielsweise (er)klä-

rungsbedürftig, was konkret unter „Praxen sonstiger humanmedizinischer Heilberufe“ im Sinne von § 20a Absatz 1 Nummer 1 Buchstabe i IfSG zu verstehen ist. Gehören dazu beispielsweise auch Praxen von Physiotherapeuten, Heilpraktikern und Hebammen? Welchen Inhalt muss und darf ein von bestimmten Personen vorzulegendes ärztliches Zeugnis im Sinne des § 20a Absatz 2 Satz 1 Nummer 4 IfSG („ein ärztliches Zeugnis darüber, dass sie auf Grund einer medizinischen Kontraindikation nicht gegen das Coronavirus SARS-CoV-2 geimpft werden können“) haben? Muss und darf dort, etwa zur zweifelsfreien Identifikation der jeweils betroffenen Person, neben deren Namen auch deren Anschrift und Geburtsdatum genannt werden? Muss und darf ein solches Zeugnis auch Diagnosen, Befunde oder die Angabe des konkreten medizinischen Grundes, der Grundlage für die Kontraindikation ist, enthalten? Ist ein solches Zeugnis stets im Original vorzulegen? Oder genügt insofern eine Kopie? Darf die Leitung der jeweiligen Einrichtung oder des jeweiligen Unternehmens eine Kopie eines ihr vorgelegten derartigen Zeugnisses fertigen und für eine gewisse, gegebenenfalls welche, Dauer aufbewahren, etwa als Teil einer Akte?

Insoweit war es sehr zu begrüßen, dass das Sozialministerium viele dieser offenen Fragen vor Beginn der Umsetzung durch im Internet abrufbare Handreichungen und Hinweise zu klären versuchte. Dankenswerter Weise wurden wir zudem bei der Erstellung dieser Handreichungen und Hinweise sowie bei der Gestaltung des sogenannten digitalen Meldeportals zur einrichtungsbezogenen Impfpflicht intensiv beteiligt.

Selbstverständlich standen wir auch den Gesundheitsämtern hierzu zur Beratung zur Verfügung. Gleichwohl kam es – wie es bei der sehr sensiblen Materie und der wenig ausgefeilten gesetzgeberischen Ausgestaltung nicht anders zu erwarten war – auch zu einigen von uns zu bearbeitenden Datenschutz-Beschwerden in diesem Zusammenhang.

Nach dem Außerkrafttreten der einschlägigen Regelungen werden wir mit dem Sozialministerium nun auch „Bilanz ziehen“ und mit Blick auf unsere Aufgaben klären, welche datenschutzrechtlichen Probleme es im Vollzug der Vorschriften nach Kenntnis des Ministeriums gab, wie diese gegebenenfalls gemeistert wurden und was dar-

☛ Mehr Informationen

Infektionsschutzgesetz:
www.gesetze-im-internet.de/ifsg/__22a.html

Die „Handreichung zur Impfprävention in Bezug auf einrichtungsbezogene Tätigkeiten“ des Bundesgesundheitsministeriums, 22.3.2022:
www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/C/Coronavirus/FAQs_zu_20a_IfSG.pdf

Ausführungen zur einrichtungsbezogenen Impfpflicht vom Sozialministerium BaWü:
sozialministerium.baden-wuerttemberg.de/de/gesundheit-pflege/gesundheitsschutz/infektionsschutz-hygiene/informationen-zu-coronavirus/einrichtungsbezogene-impfpflicht

Bundesverfassungsgericht, Beschluss 27.4.2022 – 1 BvR 2649/21:
www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2022/04/rs20220427_1bvr264921.html;jsessionid=CF9F52B51D434B3B01AC67CFF0FF2D9A.1_cid344

Pressemitteilung Sozialministerium Baden-Württemberg, 20.9.2022, zum Nachweis über dritte Impfung oder Genesung: sozialministerium.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/einrichtungsbezogene-impfpflicht-aktuell-beschaeftigte-muessen-ab-1-oktober-keinen-nachweis-ueber-dri

„Handreichung zum Gesetz zur Stärkung der Impfprävention gegen COVID-19“ (Für Einrichtungen/Unternehmen in BaWü), Stand: 21.2.2022:
sozialministerium.baden-wuerttemberg.de/fileadmin/redaktion/m-sm/intern/downloads/Downloads_Gesundheitsschutz/Corona_Handreichung_20a-IfSG-Einrichtungen_mitAnlage.pdf

Handreichung zum Gesetz zur Stärkung der Impfprävention gegen COVID-19 (Für Gesundheitsämter in BaWü), Stand: 13.5.2022:
sozialministerium.baden-wuerttemberg.de/fileadmin/redaktion/m-sm/intern/downloads/Downloads_Gesundheitsschutz/Corona_Handreichung_20a-IfSG-Gesundheitsaemter.pdf

aus mit Blick auf vergleichbare künftige Aufgaben zu lernen ist. Es ist wertvoll, eine kollegial-kritische Reflektion vorzunehmen. So können wir alle neue Erkenntnisse gewinnen und sie zielführend im Interesse der Bürger_innen künftig einsetzen.

2.3 Nachlese bei Verantwortlichen

Mit Blick auf das Ende vieler datenschutzrechtlich relevanter Regelungen zur Pandemiebewältigung haben wir uns nach mehrfacher Ankündigung zu Beginn des Jahres dann auch mit dem „Aufräumen" befasst und pandemiebedingte Grundrechtseingriffe datenschutzrechtlich „auf den Prüfstand" gestellt. Im Zuge dessen sind wir auf verschiedene Verantwortliche zugegangen, die personenbezogene Daten – insbesondere Gesundheitsdaten – im Zusammenhang mit der Corona-Pandemie verarbeitet haben. Offenbar sind unsere Hinweise zu Beginn des Jahres bei vielen Verantwortlichen angekommen: Die Rückmeldungen waren daher auch überwiegend erfreulich und ließen kaum datenschutzrechtliche Defizite erkennen. Unsere Untersuchungen sind indes noch nicht abgeschlossen, wir sind mittendrin in der Arbeit. Wir werden uns noch an weitere Verantwortliche wenden und nachfragen, ob datenschutzrechtlich soweit alles in Butter ist.

2.3.1 Nachlese bei Hochschulen

Während der Pandemie wurden unter anderem auch in Hochschulen spezielle Datenverarbeitungen zur Pandemiebekämpfung nötig. So waren die Hochschulen zur Überprüfung der Impf-, Genesenen- oder Testnachweise verpflichtet (vgl. § 6 Absatz 2 Satz 1 der Corona-Verordnung Studienbetrieb vom 20. September 2021 in der ab 19. März 2022 gültigen Fassung – CoronaVO Studienbetrieb –, nach deren § 12 Absatz 2 mit Ablauf des 2. April 2022 außer Kraft getreten).

Außerdem konnten sie unentgeltlich einen Hochschulnachweis über einen vorhandenen Impf-, Genesenen- oder Teststatus ausstellen (vgl. § 6 Absatz 2 Satz 2 Teilsatz 1 CoronaVO Studienbetrieb). Dabei durften die Hochschulen einen Nachweis außer in den Fällen des § 6 Absatz 2 Satz 5 Nummer 1 CoronaVO Studienbetrieb nicht speichern (vgl. § 6 Absatz 2 Satz 4 CoronaVO Studienbetrieb).

Darüber hinaus bestand die Pflicht zum Tragen einer medizinischen Maske oder einer Atemschutzmaske nicht für Personen, die glaubhaft machen konnten, dass ihnen das Tragen einer medizinischen Maske oder einer Atemschutzmaske aus gesundheitlichen Gründen nicht möglich oder nicht zumutbar war, wobei diese Gründe in der Regel durch eine ärztliche Bescheinigung glaubhaft zu machen waren (vgl. § 4 Absatz 2 Nummer 6 CoronaVO Studienbetrieb). Auch waren die Hochschulen auf der Basis der Regelung in § 28b des Infektionsschutzgesetzes in der bis zum 19. März 2022 geltenden Fassung verpflichtet, Informationen über den sogenannten 3G-Status ihrer Beschäftigten zu verarbeiten.

Wir gingen und gehen davon aus, dass eine weitere Verarbeitung aller personenbezogenen Daten, die im Zusammenhang mit der Überprüfung der Impf-, Genesenen- oder Testnachweise, mit dem Ausstellen einen Hochschulnachweis über einen vorhandenen Impf-, Genesenen- oder Teststatus, mit dem Glaubhaftmachen der Unmöglichkeit oder Unzumutbarkeit des Tragens einer medizinischen Maske oder einer Atemschutzmaske und mit dem 3G-Status von Beschäftigten verarbeitet wurden, jedenfalls inzwischen nicht mehr zur Aufgabenerfüllung erforderlich ist und diese personenbezogenen Daten daher, soweit sie doch noch gespeichert sein sollten, jedenfalls grundsätzlich zu löschen sind.

Vor diesem Hintergrund haben wir Hochschulen in Baden-Württemberg gebeten, uns gegenüber

☛ Mehr Informationen

Unsere Pressemitteilung „Wege aus der Pandemie – zurück zur Freiheit" vom 8. April 2022:
www.baden-wuerttemberg.datenschutz.de/wege-aus-der-pandemie-zurueck-zur-freiheit

Bericht Kontext Wochenzeitung:
www.kontextwochenzeitung.de/politik/570/brink-raeumt-auf-8046.html

Corona-Verordnung Studienbetrieb vom 20. September 2021 in der ab 19. März 2022 gültigen Fassung:
baden-wuerttemberg.de/fileadmin/redaktion/m-mwk/intern/dateien/pdf/22_03_18_CVO_Studienbetrieb_Lesefassung_Homepage_ENDG%C3%9CLTIG.pdf

schriftlich zu bestätigen, dass sie keine solchen soeben genannten personenbezogenen Daten (mehr) speichern oder anderweitig verarbeiten und, sofern dies doch der Fall sein sollte, uns das mitzuteilen sowie Näheres zu Betroffenenzahl, Datenarten, Verarbeitungszweck und Rechtsgrundlage.

Die Antworten der Hochschulen besagten, dass sie keine der genannten personenbezogenen Daten (mehr) speichern oder anderweitig verarbeiten. Teils haben Hochschulen dankenswerter Weise vorsorglich, um sicherzugehen, dass es insoweit keine unbeabsichtigten Löschversäumnisse gibt, auf unsere Anfrage hin alle Beschäftigten darauf aufmerksam gemacht und aufgefordert, eventuell noch vorhandene Daten sofort zu löschen.

2.3.2 Nachlese bei Kindertagesstätten

Auch Kindertageseinrichtungen haben im Laufe der Pandemie zu deren Bekämpfung neuartige Datenverarbeitungen durchgeführt. Dies betraf beispielsweise die Verarbeitung personenbezogener Daten von Kindern im Zusammenhang mit der Testpflicht. So haben die Einrichtungen gegebenenfalls selbst Testungen vorgenommen (vgl. beispielsweise zuletzt § 2 Absatz 1 Nr. 1 der Verordnung des Kultusministeriums über den Betrieb der Kindertageseinrichtungen und Kindertagespflegestellen unter Pandemiebedingungen [Corona-Verordnung Kita – CoronaVO Kita] vom 1. April 2022; außer Kraft getreten am 13. April 2022). Zusätzlich beziehungsweise alternativ haben sich die Einrichtungen Testnachweise im Sinne von § 22a Absatz 3 Nummer 3 des Infektionsschutzgesetzes (IfSG) oder die Eigenbescheinigung der Erziehungsberechtigten nach ordnungsgemäß durchgeführtem Selbsttest auf dem von der Einrichtung vorgegebenen Musterformular vorlegen lassen (vgl. § 2 Absatz 2 Nr. 2 bzw. 3 der letzten Corona-Verordnung Kita vom 1. April 2022).

Ähnliches galt für die Testpflicht des Personals: Das Personal war unter der Geltung der Corona-Verordnung Kita gehalten, bei täglicher Anwesenheit in der Kindertageseinrichtung einen negativen Schnelltest oder einen negativen PCR-Test durchzuführen (§ 3 Absatz 1 Nummer 2 Buchstabe a Corona-VO Kita vom 1. April 2022). Alternativ konnten die Beschäftigten ein negatives Testergebnis im Sinne des § 22a Absatz 3 Nummer 3 IfSG vorlegen. Ebenso mussten Personen, die nicht zum Personal gehörten und die nicht in der Kindertageseinrichtung betreut wurden, negative Testergebnisse im Sinne von § 22a Absatz 3 IfSG vorlegen, um die Einrichtung betreten zu dürfen (§ 3 Absatz 1 Nummer 3 CoronaVO Kita vom 1. April 2022).

Neben den Testergebnissen selbst erfolgten auch Datenverarbeitungen im Zusammenhang mit Impfungen (vgl. § 2 Absatz 1 Satz 2 CoronaVO Kita vom 1. April 2022) und ärztlichen Bescheinigungen, durch die glaubhaft gemacht wurde, dass ein Test nicht durchgeführt werden konnte (vgl. § 3 Absatz 3 Nr. 1 CoronaVO Kita vom 1. April 2022) oder es sich um quarantänebefreite Personen handelt (§ 3 Absatz 3 Nr. 2 CoronaVO Kita vom 1. April 2022). Darüber hinaus wurden von den Einrichtungen vielfach auch Informationen zur Unzumutbarkeit des Tragens einer Maske erhoben und gespeichert.

Nachdem die zugrundeliegenden Vorschriften der Corona-Verordnung außer Kraft getreten sind, ist unseres Erachtens eine weitere Verarbeitung der beschriebenen Arten personenbezogener Daten nicht mehr erforderlich, so dass die Daten zu löschen sind. Einige der Nachweise und Bescheinigungen waren ohnehin nur vorzulegen und von den Einrichtungen gar nicht zu speichern.

Angesichts dieser Sach- und Rechtslage haben wir uns an zufällig ausgewählte Kindertageseinrichtungen gewandt und diese aufgefordert mitzuteilen, ob sie noch personenbezogene Daten im oben beschriebenen Sinne speichern beziehungsweise anderweitig verarbeiten. Soweit dies der Fall sein sollte, sollten die Kindertageseinrichtungen insbesondere den Zweck und die Rechtsgrundlage der Verarbeitung mitteilen. Sämtliche Kindertageseinrichtungen, von denen wir bislang eine Rückmeldung erhalten haben, haben erfreulicher Weise erklärt, keine personenbezogenen Daten mehr zu speichern.

2.3.3 Nachlese bei Apotheken

Auch bei ausgewählten Apotheken haben wir uns danach erkundigt, inwiefern dort noch personenbezogene Daten im Zusammenhang mit der Bekämpfung der Corona-Pandemie verarbeitet werden.

Die Apotheken sind schon früh in Maßnahmen zur Bewältigung der Corona-Pandemie eingebunden

gewesen. Sie haben zu diesem Zweck insbesondere kostenlose beziehungsweise kostengünstige Schutzmasken an berechtigte Personenkreise abgegeben, Corona-Tests durchgeführt und digitale COVID-19-Impfzertifikate ausgestellt. Aufgrund dieser Maßnahmen haben wir Apotheken angeschrieben und gebeten, uns mitzuteilen, inwieweit sie im Zusammenhang mit der Bewältigung der Corona-Pandemie (noch) personenbezogene Daten verarbeiten und uns gegebenenfalls insbesondere zu bestätigen, dass sie keine personenbezogenen Daten für die Abgabe kostenfreier Schutzmasken, die durchgeführten Corona-Tests und die ausgestellten digitalen COVID-Impfzertifikate mehr verarbeiten.

Der Anspruch auf einmalige Abgabe kostenloser (qualifizierter) Schutzmasken setzte voraus, dass die betreffende Person in der Apotheke zum Nachweis ihrer altersbedingten Berechtigung ihren Personalausweis vorlegte. Bei einer altersunabhängigen Berechtigung wegen Vorerkrankungen oder Risikofaktoren musste sie diese Umstände mittels einer Eigenbescheinigung darlegen. Nach der ersten kostenlosen Abgabe hatten die berechtigten Personen noch zweimal einen Anspruch darauf, jeweils sechs Schutzmasken zu einem (im Vergleich zum damaligen Marktpreis günstig erscheinenden) Eigenanteil von 2 Euro je sechs Schutzmasken zu erwerben. Für diesen Erwerb mit Eigenanteil mussten sie dann allerdings zum Nachweis ihrer Berechtigung eine Bescheinigung ihrer Krankenkasse beziehungsweise ihrer Krankenversicherung in der Apotheke abgeben (so die Regelung in der Coronavirus-Schutzmasken-Verordnung – im Folgenden: SchutzmV).

Bei der kostenlosen Abgabe hatte also nur eine Sichtprüfung des vorgelegten Personalausweises zu erfolgen, ohne dass es zum Beispiel einer Fotokopie und damit verbundenen Verarbeitung personenbezogener Daten bedurfte. Aufgrund unserer Nachfrage haben uns Apotheken bestätigt, dass sie insoweit zur kostenlosen Abgabe keine personenbezogenen Daten speichern. Zu Recht wies allerdings eine der befragten Apotheken darauf hin, dass bei der Abgabe gegen Eigenanteil die von der Krankenkasse oder privaten Krankenversicherung ausgestellte Bescheinigung von der Apotheke nach § 4 Absatz 2 Satz 2 SchutzmV einzubehalten war und gemäß § 7 Absatz 2 Satz 3 SchutzmV zum Nachweis der ordnungsgemäßen Abrechnung noch bis zum 31. Dezember 2024 aufzubewahren ist.

Außerdem haben die Apotheken Bürgertestungen auf das Coronavirus SARS-Cov-2 nach § 4a der Coronavirus-Testverordnung durchgeführt (folgend: TestV). Dies führte dazu, dass die Apotheken infolge der namentlich zuzuordnenden Testung mit den mitzuteilenden Testergebnissen besondere Kategorien personenbezogener Daten in Gestalt von Gesundheitsdaten verarbeitet haben, die zudem dem Berufsgeheimnis unterliegen (vgl. Artikel 9 Absatz 1, Artikel 4 Nummer 15 DS-GVO und Artikel 9 Absatz 2 Buchstabe i und Absatz 3 DS-GVO).

Infolge unserer Bitte an die angeschriebenen Apotheken, uns den aktuellen Stand über eventuell gespeicherte personenbezogenen Daten durchgeführter Corona-Tests mitzuteilen, wies eine Apotheke – wohl zu Recht – darauf hin, es sei hierbei zu differenzieren zwischen den zu übermittelnden personenbezogenen Daten und der notwendigen Auftrags- und Leistungsdokumentation: Der an die Kassenärztliche Bundesvereinigung zu übermittelnde Datensatz darf nach dem Wortlaut des § 7 Absatz 4 Satz 2 TestV keinen Bezug zu den getesteten Personen aufweisen. Dagegen sind die Angaben über den Nachweis der korrekten Durchführung und Abrechnung notwendige Auftrags- und Leistungsdokumentation nach § 7 Absatz 5 Satz 1 TestV bis zum 31. Dezember 2024 aufzubewahren.

☛ Mehr Informationen:

Zur Speicherdauer bei Coronatests vergleiche schon unseren 37. Tätigkeitsbericht auf Seite 29 „1.4. Datenschutz in Corona-Testzentren“:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf

Coronavirus-Schutzmasken-Verordnung:
www.bundesgesundheitsministerium.de/service/gesetze-und-verordnungen/guv-19-lp/schutzmv.html

Coronavirus-Testverordnung:
www.gesetze-im-internet.de/coronatestv_2021-10/BJNR626400021.html

Infektionsschutzgesetz:
www.gesetze-im-internet.de/ifsg/__22a.html

Diese Dokumentation kann, soweit erforderlich, unter anderem den Vornamen, den Familiennamen, das Geburtsdatum und die Anschrift der getesteten Person, die Art der Leistung, der Tag, die Uhrzeit, das Ergebnis der Testung und der Mitteilungsweg an die getestete Person, enthalten (vgl. § 7 Absatz 5 Satz 2 Nr. 5 TestV). Von den angeschriebenen Apotheken hat eine Apotheke von dieser weitergehenden Antrags- und Leistungsdokumentation Gebrauch gemacht.

Darüber hinaus konnten sich geimpfte Personen ihre Schutzimpfung gegen das Coronavirus SARS-CoV-2 von Apotheken in einem digitalen Zertifikat (COVID-19-Impfzertifikate) bescheinigen lassen (vgl. § 22a Absatz 5 Nummer 2 des Infektionsschutzgesetzes). Die Apotheken sind danach verpflichtet, das COVID-19-Impfzertifikat auszustellen, wenn sie die Identität der betroffenen Person und die Authentizität der Impfdokumentation überprüft haben. Dafür sieht das Infektionsschutzgesetz vor, dass die Personen die entsprechenden Unterlagen zum Nachweis ihrer Impfung und gegebenenfalls ihrer Identität den Apotheken vorlegen. Eine Befugnis zur Speicherung seitens der Apotheke ist damit nicht verbunden. Die angeschriebenen Apotheken haben uns erfreulicher Weise auch bestätigt, dass sie im Zusammenhang mit bereits ausgestellten COVID-19-Impfzertifikaten keine personenbezogenen Daten (mehr) verarbeiten.

2.4 Stand der regulatorischen Vorgaben zur Pandemiebewältigung

Um an das Titelblatt unseres 37. Tätigkeitsberichts zum Datenschutz 2021 („Wege aus der Pandemie – zurück zur Freiheit!“) und den dortigen ersten Satz des Vorworts („Noch immer steht der Datenschutz unter dem maßgebenden Einfluss der SARS-CoV-2-Pandemie“) anzuknüpfen: „Corona“ hat – unabhängig von der eingangs erwähnten Frage, ob inzwischen die Pandemie vollständig überwunden ist oder noch nicht vollständig – seinen maßgebenden Einfluss auf den Datenschutz (und damit auch auf unseren Dienstbetrieb) verloren, viele – auch datenschutzrechtlichen – Freiheiten wurden zurückgewonnen.

Das ist beispielsweise daran zu erkennen, dass der Text der zur Zeit des Redaktionsschlusses dieses Tätigkeitsberichts aktuellen Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2 (Corona-Verordnung – CoronaVO) vom 27. September 2022 (in der ab dem 30. November 2022 geltenden Fassung) nur noch wenige datenschutzrechtlich bedeutsame Vorschriften enthält. Doch auch diese gehören auf den Prüfstand – insbesondere auch mit Blick auf ihre Erforderlichkeit angesichts der Standes der Verbreitung des Virus SARS-Cov-2 und dessen aktuellen Gefahrenpotentials.

Zu den wenigen verbliebenen „harten“ Regelungen gehören die des § 3 Absatz 1 CoronaVO über die „Pflicht zum Tragen einer medizinischen Maske“ in geschlossenen Fahrzeugbereichen von Verkehrsmitteln des öffentlichen Personennahverkehrs, in bestimmten Einrichtungen der Gesundheitsvorsorge und des öffentlichen Gesundheitsdienstes und in Rettungsdienstes sowie in Einrichtungen der Wohnungslosenhilfe. Datenschutzrechtlich bedeutsam ist dabei nicht die Regelung der vielfach sogenannten Maskenpflicht selbst, sondern die dazugehörigen Ausnahmeregelungen, die – worauf wir schon mehrfach hingewiesen haben (siehe unseren 37. Tätigkeitsbericht 2021, S. 16, und unseren 36. Tätigkeitsbericht 2020, S. 17) in ihrer Bedeutung und Reichweite sowie hinsichtlich der Kontrollbefugnisse in der Praxis unklar sind und die die davon betroffenen Personen noch immer mit dieser Rechtsunsicherheit belasten. Auch wenn es inzwischen einzelne Rechtsprechung zu konkreten Fallgestaltungen gibt: Immer wieder erscheint fragwürdig, wem gegenüber die Ausnahmegründe wie glaubhaft gemacht werden müssen und wie die Person, der gegenüber die Glaubhaftmachung erfolgt, mit diesen Daten und Erkenntnissen umgehen (also diese Daten weiterverarbeiten) darf. Die Unklarheiten beziehen sich unter anderem darauf, welche konkreten Anforderungen etwa an die ärztliche Bescheinigung gestellt werden sollen, mit der die „Glaubhaftmachung gesundheitlicher Gründe in der Regel“ erfolgen soll, und wer unter welchen Voraussetzungen die Glaubhaftmachung (also beispielsweise die Vorlage der ärztlichen Bescheinigung) soll verlangen können. Unsere Hinweise, die Vorschrift zu überarbeiten und zu konkretisieren, wurden ebenso wenig erhört wie etwa unser Vorschlag (siehe schon in unserem 36. Tätigkeitsbericht), auf die „Glaubhaftmachung“ bei gesundheitlicher Beeinträchtigung ganz verzichten und stattdessen eine datensparsame Bescheinigung über die Befreiung durch den öffentlichen Gesundheitsdienst oder durch von diesem ermächtige qualifizierten Ärzt_innen ausstel-

len zu lassen, deren Vorlage nur gegenüber konkret zu benennenden prüfberechtigten Personen erfolgt, wurden bislang nicht aufgegriffen.

Im Zeitpunkt des Redaktionsschlusses wird aber vermehrt öffentlich diskutiert, ob die Maskenpflicht insbesondere im öffentlichen Personennahverkehr abgeschafft werden soll. Voraussichtlich wird sich die datenschutzrechtliche Problematik letztlich wohl mit einer Abschaffung der Maskenpflicht erledigen.

Von besonderer Problematik ist auch die noch immer in der Corona-Verordnung enthaltene Regelung über „Zuständigkeiten des Polizeivollzugsdienstes" (aktuell § 8 CoronaVO). Dieser lautet:

„Der Polizeivollzugsdienst ist neben den nach der Verordnung des Sozialministeriums über Zuständigkeiten nach dem Infektionsschutzgesetz zuständigen Behörden (Infektionsschutzbehörden) zuständig für die Überwachung der sich aus dieser Verordnung ergebenden Verpflichtungen

1. *zum Tragen einer medizinischen Maske oder einer Atemschutzmaske,*

2. *zur Vorlage eines Impf-, Genesenen- oder Testnachweises in Betrieben der Gastronomie, Diskotheken, Clubs sowie sonstigen Einrichtungen und Veranstaltungen, die clubähnlich betrieben werden, und*

3. *zur Überprüfung von Nachweisen nach Nummer 2 durch die Betreiberinnen und Betreiber der Gastronomie, von Diskotheken, Clubs sowie sonstigen Einrichtungen und Veranstaltungen, die clubähnlich betrieben werden.*

Soweit im Rahmen der Überwachung nach Satz 1 eine Speicherung von Daten erforderlich ist, sind diese Daten von anderen Datenbeständen zu trennen. Dabei darf die Verarbeitung der in den zu überprüfenden Nachweisen enthaltenen personenbezogenen Daten nur lokal in dem von der prüfenden Person verwendeten Endgerät und nur soweit und solange erfolgen, wie es zur Durchführung einer Sichtkontrolle des von der Anwendung angezeigten Prüfergebnisses erforderlich ist. Der Polizeivollzugsdienst darf die von ihm nach Satz 1 erhobenen Daten nur zur Überwachung und Ahndung der sich aus dieser Verordnung ergebenden Verpflichtungen verarbeiten. Die Sätze 2 und 4 finden keine Anwendung, soweit die vom Polizeivollzugsdienst nach Satz 1 erhobenen Daten auch zu einem anderen Zweck hätten erhoben werden dürfen oder sich nachträglich Umstände ergeben, nach denen eine Erhebung zu einem anderen Zweck zulässig wäre. In diesem Fall finden für die weitere Verarbeitung der

Ist die Pandemie vorbei, schauen wir genau hin, welche rechtlichen Einschränkungen der Bürgerrechte noch vorhanden sind und

nach Satz 1 erhobenen Daten die Regelungen Anwendung, die für die Verarbeitung zu dem anderen Zweck maßgeblich sind."

Diese Regelung ist erstmals mit der Zwölften Verordnung der Landesregierung zur Änderung der Corona-Verordnung vom 18. März 2022 in die Corona-Verordnung eingefügt worden (seinerzeit als § 23a der Corona-Verordnung). Ihr ist im Rahmen der Beteiligung unserer Dienststelle gemäß Artikel 36 Absatz 4 DS-GVO, § 26 Absatz 2 LDSG eine längere Diskussion zwischen den betroffenen Ministerien und unserer Behörde vorausgegangen. Die Landesregierung war damals der Auffassung, die an sich (nach § 1 Absatz 6 Satz 1 der Verordnung des Sozialministeriums über Zuständigkeiten nach dem Infektionsschutzgesetz) zuständigen Ortspolizeibehörden seien angesichts der vielfältigen Verpflichtungen, Schutzmasken zu tragen und Nachweise über Impfungen oder Testungen auf SARS-Cov-2 vorzulegen sowie diese zu kontrollieren, personell (beispielsweise auch nachts und an Wochenenden) nicht ausreichend in der Lage, die Einhaltung dieser Verpflichtungen effektiv zu überwachen. Deswegen solle (nicht etwa die Ortspolizeibehörde personell verstärkt, sondern) die uniformierte Polizei hier unterstützend tätig werden. Die Begründung zur zwölften Änderungsverordnung vom 18. März 2022 der Corona-Verordnung vom 15. September 2021 hierzu führte aus:

„Die Landesregierung trifft hiermit erforderliche Maßnahmen zur Gewährleistung der auf Grundlage des Beschlusses aus der Videoschaltkonferenz des Bundeskanzlers mit den Regierungschefinnen und Regierungschefs der Länder vom 18. November 2021 geeinten Position. Demnach haben sich die Länder unter anderem dazu verpflichtet, die Kontrolldichte der Einhaltung von Schutzmaßnahmen ihrerseits zu erhöhen und Verstöße hiergegen entschieden zu sanktionieren."

Indes ist die Betrauung des Polizeivollzugsdienstes mit Aufgaben des Infektionsschutzes durchaus problematisch. Der Polizeivollzugdienst ist für die Gefahrenabwehr und die Strafverfolgung zuständig (§ 1 des Polizeigesetzes [PolG] und § 163 Absatz 1 der Strafprozessordnung [StPO]).

Im Rahmen seiner Aufgaben im Bereich der Strafverfolgung unterliegt er dabei dem allgemeinen Strafverfolgungszwang aus §§ 152, 160, 163 StPO. Das bedeutet, dass er bei jedwedem Anfangsverdacht auf eine Straftat Ermittlungen aufzunehmen und im Rahmen dieser Ermittlungen die ihm verfügbaren Erkenntnisse zur Aufklärung der Straftat

prüfen, ob das noch sein muss.

☛ Mehr Informationen:

Zwölften Verordnung der Landesregierung zur Änderung der Corona-Verordnung vom 18.3.22:
im.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Coronainfos/Corona_2022/220318_Zwoelfte_VO_der_LReg_zur_Aenderung_der_CoronaVO.pdf

Verordnung des Sozialministeriums über Zuständigkeiten nach dem Infektionsschutzgesetz:
www.baden-wuerttemberg.de/de/service/aktuelle-infos-zu-corona/verordnung-zustaendigkeiten-ifsg

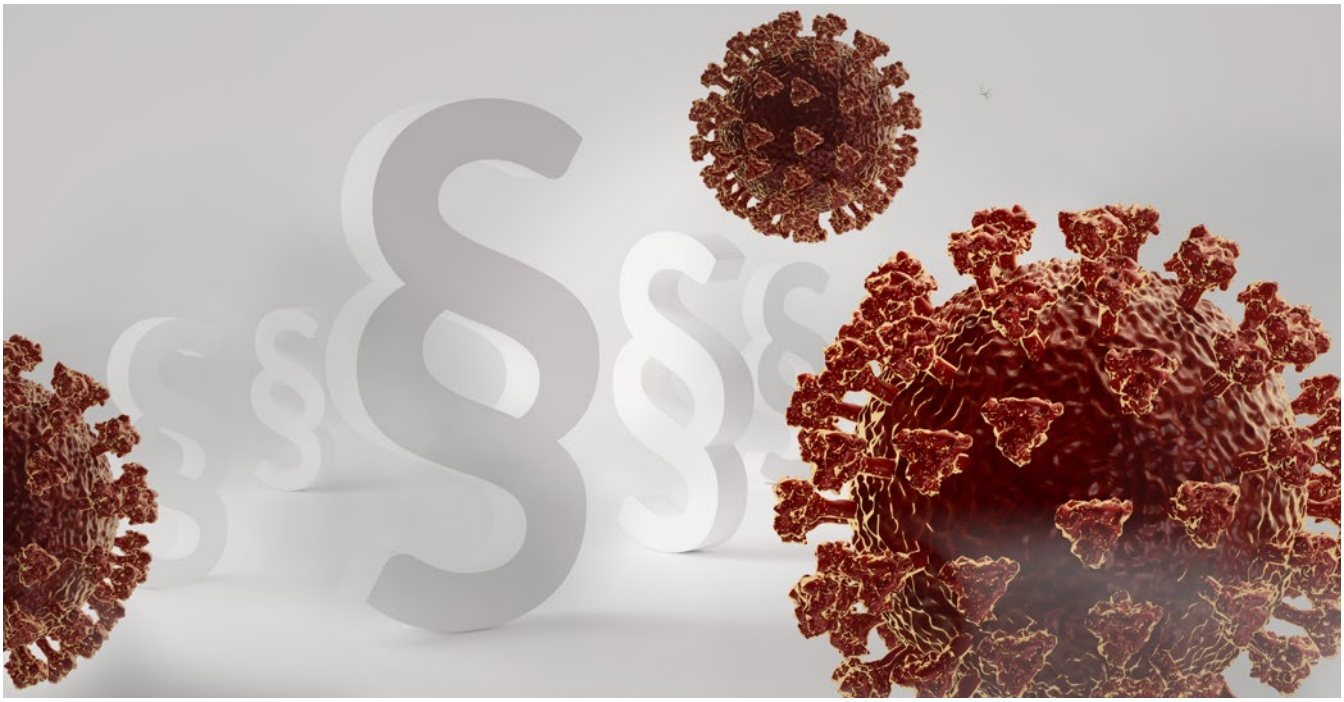
SWR-Bericht – „Missbrauch der Luca-App: Auch Polizei in BW fragte bei Gesundheitsämtern nach Daten":
www.swr.de/swraktuell/baden-wuerttemberg/polizei-in-drei-kreisen-bw-abfrage-daten-luca-app-100.html

zusammentragen hat (wobei er der Staatsanwaltschaft sachlich weisungsunterworfen ist).

Dieser Grundsatz ist nur schwerlich vereinbar mit den Aufgaben der Infektionsschutzbehörde. Diese ist vielfach darauf angewiesen, im überragenden Interesse des Infektionsschutzes wahrheitsgemäße Angaben und sensible Informationen von zur Auskunft beziehungsweise Information verpflichteten Personen zu bekommen, und zwar auch dann, wenn solche Auskünfte und Informationen Hinweise auf Ordnungswidrigkeiten oder Straftaten geben könnten. Insbesondere deswegen enthält das Infektionsschutzgesetz (IfSG) den Grundsatz, dass die zu Infektionsschutzzwecken von der zuständigen Behörde erhobenen personenbezogenen Daten ausschließlich für Zwecke des Infektionsschutzgesetzes verarbeitet werden dürfen. Das Infektionsschutzgesetz unterwirft die zu seinem Vollzug zu verarbeitenden personenbezogenen Daten also einer strengen Zweckbindung (vgl. z. B. § 16 Absatz 1 Satz 2 IfSG, auch in Verbindung mit § 25 Absatz 2 Satz 1 IfSG, sowie ferner § 25 Absatz 3 Satz 4, § 28a Absatz 4 Satz 3, 6 und 7, § 30 Absatz 3 Satz 3, § 36 Absatz 9 Satz 3 und 5 IfSG).

Demnach dürfen zu Zwecken des Infektionsschutzgesetzes erhobene personenbezogene Daten insbesondere nicht zu Zwecken allgemeiner Strafverfolgung verwendet werden. Hiergegen hatten bereits zuvor – ohne Regelung einer Zuständigkeit des Polizeivollzugsdienstes für Aufgaben des Infektionsschutzgesetzes – einzelne Beamte des Polizeivollzugsdiensts bei mehreren Gelegenheiten verstoßen: Diese hatten in Einzelfällen (in Baden-Württemberg aber, soweit uns bekannt, jeweils ohne Erfolg) versucht, von Gaststätten oder Veranstalter zur Kontaktnachverfolgung erhobene Kontaktdaten ihrer Besucherinnen und Besucher (gegebenenfalls auch unter Einbeziehung des Gesundheitsamts im Falle der Nutzung der Luca-App) zu Strafverfolgungszwecken zu erheben, obwohl dies nach Wortlaut und Intention der Regelungen in § 28a Absatz 4 IfSG eindeutig ausgeschlossen ist. Hierüber war in der Presse verschiedentlich berichtet worden.

Wenn aber die grundsätzlich verschiedenen Aufgaben der allgemeinen Strafverfolgung und des Infektionsschutzes in einer Hand vereinigt werden, erschwert dies massiv die Durchhaltung der engen Zweckbindung der zu Infektionsschutzzwecken zu verarbeitenden Daten. Der Gesetzgeber des Polizeigesetzes war daher bislang zu Recht zurückhaltend bei der Übertragung infektionsschutzrechtlicher Aufgaben auf den Polizeivollzugsdienst (s. lediglich die ihrerseits ebenfalls nicht unproblematische Ausnahmevorschrift des § 105 Absatz 3 PolG). Die Landesregierung hat diese von uns seinerzeit geäußer-



© Nuthawut – stock.adobe.com

Zahlreiche Einschränkungen aufgrund der Pandemie wurden im Jahr 2022 aufgehoben.

ten Bedenken immerhin dadurch berücksichtigt, dass sie den dem Polizeivollzugsdienst übertragenen Aufgabenbereich eng gefasst hatte, im Normentext die Datenminimierung betonte (s. derzeit noch § 8 Satz 2 und 3 CoronaVO), die Trennung etwaig entstehender Datenbestände von denen der sonstigen Bereiche des Polizeivollzugsdiensts angeordnet und eine enge Zweckbindung normiert hat (siehe noch derzeit § 8 Sätze 2 und 4 DS-GVO). Inwieweit diese Vorgaben umsetzbar waren, insbesondere ob der Polizeivollzugsdienst angesichts der Kurzfristigkeit der übertragenen Zusatzaufgaben tatsächlich ausschließlich separat geführte EDV-Systeme einrichten konnte, und inwieweit die in den Sätzen 5 und 6 normierten Durchbrechungen des bundesrechtlich normierten engen Zweckbindungsprinzips zulässig sind, soll an dieser Stelle dahinstehen.

Denn zumindest dürfte aus unserer Sicht inzwischen – zum Zeitpunkt des Redaktionsschlusses – jeder Grund entfallen sein, den Polizeivollzugsdienst mit Aufgaben der Infektionsschutzbehörde zu betrauen: Wie ausgeführt, besteht die nach Nummer 1 vom Polizeivollzugsdienst zu überwachende Maskenpflicht nur noch in äußerst wenigen Fällen. Dass es jetzt noch sachgerecht sein könnte, wie in der oben wiedergegebenen Begründung zur Änderungsverordnung vom 18. März 2022 ausgeführt, „die Kontrolldichte der Einhaltung von Schutzmaßnahmen […] zu erhöhen und Verstöße hiergegen entschieden zu sanktionieren", erscheint wenig plausibel. Hinzu kommt, dass die meisten „Schutzmaßnahmen" (also Pflichten der Bürger_innen), für deren Überwachung der Polizeivollzugsdienst nach § 8 der aktuellen Corona-Verordnung zuständig sein soll, gar nicht mehr bestehen: Die sogenannte Maskenpflicht (§ 8 Nummer 1 CoronaVO) gilt nur noch in wenigen Ausnahmefällen, Pflichten zur Vorlage eines Impf-, Genesenen- oder Testnachweises in Betrieben der Gastronomie, Diskotheken, Clubs oder in clubähnlichen Einrichtungen (§ 8 Nummer 2 CoronaVO) bestehen gar nicht mehr, und erst recht sind die Betreiber_innen solcher Einrichtungen nicht mehr zur Kontrolle solcher Nachweise verpflichtet (§ 8 Nummer 3 CoronaVO). Dass noch die Zuständigkeit des Polizeivollzugsdiensts für die Überwachung von gar nicht existenten Verpflichtungen normiert wird, könnte man – in Anlehnung an die Problematik der Vorratsdatenspeicherung (zu der zuletzt das Urteil des Europäischen Gerichtshofs vom 20. September 2022 – ECLI:EU:C:2022:702 erging) – als „Vorratsgesetzgebung" bezeichnen, deren Sinnhaftigkeit deutlich zu hinterfragen ist.

Ähnlich wie § 8 CoronaVO dringend erneut auf den Prüfstand zu stellen ist, ist auch die uneingeschränkte Fortgeltung der Corona-Verordnung Datenverarbeitung (und der mit ihr verbundenen Corona-Verordnung Datenverarbeitung im Auftrag) zu hinterfragen. Mit diesen Regelungen (siehe zu ihnen bereits unseren 36. TB 2020, S. 22 f.) wurde ein Abrufsystem begründet, mit dem einerseits unter bestimmten Voraussetzungen Daten über mit SARS-Cov-2 Infizierte oder Infektionsverdächtige zwischen den Gesundheitsämtern und den Ortspolizeibehörden ausgetauscht werden können (§ 1 CoronaVO Datenverarbeitung). Andererseits kann auch der Polizeivollzugsdienst in bestimmten Sonderfällen Daten über Personen, gegen die eine laufende vollziehbare Schutzmaßnahme nach dem Infektionsschutzgesetz wegen des auf die akute Infektion der betroffenen Person hinweisenden Nachweises des Krankheitserregers SARS-Cov-2 angeordnet wurde, aus diesem System abrufen (§ 2 CoronaVO Datenverarbeitung). Dabei muss stets der Abruf auch zum Schutz der Beamt_innen des Polizeivollzugsdienstes bei einem bevorstehenden polizeilichen Einsatz in Bezug auf diese Person erforderlich sein.

Die Vorhaltung eines Systems, mit dessen Hilfe die Gesundheitsämter mit dem ebenfalls für die Vollziehung des Infektionsschutzgesetzes zuständigen Ortspolizeibehörden sicher kommunizieren können, hat sich unseres Erachtens bewährt. Auf diese Weise kann dem im 36. TB beschriebene „Wildwuchs" der Kommunikationsformen zwischen diesen Behörden (beispielsweise der Nutzung von ungesicherten E-Mails oder des Telefaxes) entgegengewirkt werden. Insoweit erscheint es unbedingt empfehlenswert, aus diesem Verfahren zu lernen und ein derartiges System zur sicheren Kommunikation zwischen Gesundheitsämtern und Ortspolizeibehörden auch über die Corona-Krise hinaus aufrechtzuerhalten. Die Notwendigkeit der weiteren Aufrechterhaltung eines Abrufsystems von Daten des Öffentlichen Gesundheitsdienstes durch den Polizeivollzugsdienst scheint uns dagegen sehr fragwürdig. Die in § 2 Absatz 3 Nummer 1 bis 4 CoronaVO Datenverarbeitung enumerativ aufgelisteten Abrufgründe dürften kaum noch von Bedeutung sein.

Abgeordneter Marc Biadacz:

„Teilt die Bundesregierung die Einschätzung des Datenschutzbeauftragten des Landes Baden-Württemberg, Stefan Brink, dass Behörden die gängigen Cloud-basierten Microsoft-Office-365-Produkte wie Word, Excel, PowerPoint, Outlook und Teams nur „nach intensiver Prüfung und erheblichem Begründungsaufwand“ nutzen können […]; und in welchem Umfang werden das Bundeskanzleramt, die Bundesministerien und ihre nachgeordneten Behörden Microsoft-Office-365-Produkte nutzen (bitte nach Ministerien aufschlüsseln)?

Parlamentarische Staatssekretärin Katja Hessel:

„Ja, die Bundesregierung teilt im Grunde nach die Einschätzung des Datenschutzbeauftragten des Landes Baden-Württemberg, Stefan Brink, bezüglich der datenschutzrechtlichen Problematik beim Einsatz von Office 365-Proukten der Firma Microsoft in der öffentlichen Verwaltung. Anwendende haben erhebliche Schwierigkeiten, die Rechtmäßigkeit der Verarbeitung personenbezogener Daten nachzuweisen. Dieser Nachweis muss durch verantwortliche Stellen aber erbracht werden. Es ist zum einen nicht zu jedem Zeitpunkt klar, welche Verarbeitungen zu welchem Zweck vorgenommen werden, zum anderen, welche Verarbeitungstätigkeiten von Microsoft im Auftrag und welche in eigener Verantwortung erfolgen […]“

Deutscher Bundestag, 9.12.2022

Drucksache 20/4852

Schriftliche Fragen mit den in der Woche vom

5. Dezember 2022 eingegangenen Antworten

der Bundesregierung

dserver.bundestag.de/btd/20/048/2004852.pdf

3. Digitale Bildungsplattform

Auch im Jahr 2022 haben wir mit hoher Intensität das Ministerium für Kultus, Jugend und Sport bei seinem Vorhaben der Gestaltung einer Digitalen Bildungsplattform weiter beraten. Im Rahmen dieser Bildungsplattform soll den Schulen – wie schon im letzten Tätigkeitsbericht (S. 47 ff. TB 2021) dargestellt – zusätzlich zu dem bereits bereitgestellten Messenger Threema eine digitale Büroarbeitsplatzumgebung für Lehrkräfte mit Textverarbeitung, Tabellenkalkulation, E-Mail und Online-Speicher, ein weiteres Lernmanagementsystem neben Moodle und ein Identity and Access Management System (IdAM) zur Verfügung gestellt werden. Außerdem sucht das Kultusministerium derzeit einen Provider für das Lernmanagementsystem Moodle als Nachfolgelösung für den bisherigen Anbieter. Dankenswerter Weise hat uns das Kultusministerium nicht nur weiter an den regelmäßigen Sitzungen des Lenkungskreises zur Digitalen Bildungsplattform beteiligt. Sondern auch im Übrigen gab es zahlreiche Besprechungen sowie schriftlichen Austausch.

Digitaler Arbeitsplatz für Lehrkräfte

Nachdem das Kultusministerium in Umsetzung unserer diesbezüglichen Beratung beschlossen hat, MS 365 nicht mehr als Teil der Bildungsplattform zu verwenden (siehe hierzu ausführlich S. 47 ff TB 2021), hat es im Berichtsjahr begonnen, in einem Pilotversuch mit einer bestimmten Anzahl von Schulen als digitalen Arbeitsplatz für Lehrer_innen die dPhoenix-Suite des Anbieters Dataport zu testen. Diese beruht auf Open-Source-Software, also auf Tools, deren Quellcode unter einer Open-Source-Lizenz veröffentlicht und frei zugänglich ist: Die Suite enthält Collabora als Textverarbeitungs-, Tabellenkalkulations- sowie Präsentationsprogramm. Für E-Mail, Kalender und Kontakte der Lehrkräfte soll die Software Open-Xchange verwendet werden. Und als Cloud-Speicher soll Nextcloud zum Einsatz kommen. Der Anbieter Dataport ist eine Anstalt öffentlichen Rechts. Sie wurde durch einen Staatsvertrag verschiedener Länder Deutschlands für die Übernahme von Informations- und Kommunikationsdienstleistungen der Verwaltungen der beteiligten Länder gegründet. Derzeit gehören dem Staatsvertrag Hamburg, Schleswig-Holstein, Bremen, Sachsen-Anhalt, Mecklenburg-Vorpommern und Niedersachsen an.

Nach unseren bisherigen Erkenntnissen findet bei der von dem Kultusministerium ausgewählten dPhoenix-Suite die gesamte Datenverarbeitung innerhalb der Europäischen Union statt, und es erfolgen keine Drittstaatentransfers nach Artikel 44 ff. DS-GVO. Ausgehend von den oben genannten Produkten sehen wir derzeit keine grundlegenden Probleme beim Datenschutz, sofern eine entsprechende Konfiguration gewählt wird. Sollten wir im weiteren Verlauf des Pilotversuchs doch noch Probleme im technischen Bereich erkennen, welche nicht durch Anpassung der Konfiguration zu lösen sind, besteht die Möglichkeit, den Quellcode entsprechend anzupassen, da dieser – wie dargestellt – als Open-Source-Code offen liegt und angepasst werden darf. In Bezug auf die Datenschutzinformationen, das Löschkonzept und weitere Fragen sind wir mit dem Kultusministerium noch im beratenden Gespräch.

Lernmanagementsysteme

Als Lernmanagementsysteme sieht die Digitale Bildungsplattform neben der Fortführung der bisher bereits angebotenen Plattform Moodle alternativ die Verwendung von itslearning vor. Auch zu itslearning haben wir uns in unserem letzten Tätigkeitsbericht schon geäußert (s. S. 48 f. TB 2021). Wir halten den Einsatz von itslearning unter der derzeitigen Gesamtsituation an den Schulen für vertretbar, empfehlen aber dringend, einzelne unter dem Blick des Datenschutzes bedenkliche Punkte – wie bereits im letzten Tätigkeitsbericht dargestellt, vorwiegend im Bereich des Drittstaatentransfers, des Tracking und der technischen und organisatorischen Maßnahmen sowie der Dokumentation derselben – zu verbessern. Zum Drittstaatentransfer sollten insbesondere die zusätzlichen Schutzmaßnahmen genauer untersucht werden, um zu klären, dass ein angemessenes Schutzniveau unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen vorliegt. Nach wie vor gehen wir davon aus, dass die Probleme überwindbar sind, und befinden uns

auch hierzu weiter im Beratungsprozess mit dem Kultusministerium.

Die Nutzung von Moodle wurden den Schulen bislang im Wege einer Kooperation des Kultusministeriums mit dem Ministerium für Wissenschaft, Forschung und Kunst über das von der IT-Koordinierungsstelle „BelWü" betriebene Netz der Universitäten und Hochschulen ermöglicht. Nach Angaben der beiden Ministerien haben diese bereits Ende 2019 entschieden, diese Kooperation zu beenden, um eine Refokussierung der IT-Kooperationsstelle auf hochschulspezifische Belange vorzunehmen, und einen Transformationsprozess zur Umsetzung dieser Entscheidung vereinbart.

Das Kultusministerium beabsichtigt – was wir sehr begrüßen –, auch nach dem Ende der Kooperation mit dem Wissenschaftsministerium den öffentlichen Schulen des Landes das Lernmanagement Moodle in datenschutzkonformer Weise zur Verfügung zu stellen. Gerne begleiten wir deswegen das Kultusministerium mit unserer Beratung bei der Vergabeentscheidung. Dabei bedauern wir allerdings, dass wir bei der Erstellung der schriftlichen Ausschreibungsunterlagen noch nicht hinzugezogen wurden. Infolgedessen wurde eine wesentliche Chance nicht vollständig genutzt sicherzustellen, dass konkrete datenschutzrechtliche Anforderungen an die zu erbringende Leistung von Anfang an bei der Erstellung der Angebote zugrunde gelegt werden. Nach Eingang der Erstangebote nehmen wir aber nunmehr umfassend an den Verhandlungsrunden des Vergabeverfahrens zur Beurteilung der datenschutzrechtlichen Fragen teil, um das Kultusministerium unter dem Aspekt des Datenschutzes bei der Auswahl des Anbieters und der angebotenen Leistung zu unterstützen.

Identitätsmanagement

Die zentrale Anmeldung zur Bildungsplattform soll über ein Identity Access Management (IdAM) erfolgen. Aus Sicherheitsgründen empfahlen wir hierzu dem Kultusministerium dringend eine verpflichtende Anmeldung mit zwei Faktoren, zumindest für Lehrer_innen, um die dort zu verarbeitenden Daten, unter anderem Schulnoten und Beurteilungen von Schüler_innen, hinreichend sicher zu schützen. Einer der kritischen Punkte der Planungen des Kultusministeriums war indes noch, dass es eine Passwortrücksetzung per E-Mail ermöglichen wollte. Dies würde unseres Erachtens indes das gebotene Sicherheitsniveau unterlaufen, da die Sicherheit der hierfür zu verwendenden privaten E-Mail-Accounts nicht garantiert werden kann. Sollte etwa ein privater E-Mail-Account einer Lehrperson durch einen Angriff gekapert sein, stände der Weg zu den sensiblen Daten auf diese Weise offen. Das Kultusministerium hat uns in der Zwischenzeit mündlich zugesichert, auf die Rücksetzung der Passwörter per E-Mail zu verzichten. Im Übrigen fehlt es bislang an einer hinreichend detaillierten datenschutzrechtlichen Dokumentation, die das Kultusministerium noch durchführen und erstellen muss.

Schlussbemerkung

Das Kultusministerium plant, mit der Ausrollung der beschriebenen Angebote der digitalen Bildungsplattform in der ersten Hälfte des Jahres 2023 zu beginnen. Wir gehen davon aus, dass uns rechtzeitig zuvor eine umfassende datenschutzrechtliche Dokumentation vorgelegt wird, die unsere vollständige Prüfung und Beratung erst ermöglicht, und unsere beratenden Hinweise zum Datenschutz umgesetzt werden. Seit nunmehr geraumer Zeit arbeiten wir vertrauensvoll mit dem Kultusministerium zusammen. Wir wollen diese Zusammenarbeit auch im Jahr 2023 fortführen.

3.1 Microsoft 365 an Schulen

Bei unseren Untersuchungen zu Microsoft 365 im Rahmen des Pilotversuchs des Kultusministeriums stellten wir datenschutzrechtliche Probleme bei der Verwendung durch Schulen fest (siehe S. 47, TB 2021). Unsere Stellungnahme gegenüber dem Kultusministerium, inklusive unserer Befunde und Messungen sind in der Zwischenzeit bei „Frag den Staat" abgelegt (siehe Block „Mehr Informationen"). Auch wenn nun Microsoft 365 nicht mehr Teil der Digitalen Bildungsplattform in Baden-Württemberg sein wird, so verwenden doch einzelne Schulen selbst diesen Cloud-Dienst beziehungsweise Teile des Cloud-Dienstes, wie beispielsweise MS Teams. Gegen den jeweiligen Einsatz von Microsoft 365 durch die Schule lagen uns zahlreiche Beschwerden von Eltern und Schülern vor, welchen wir nachgingen. Hierzu haben wir alle von derartigen Beschwerden betroffenen Schulen angeschrieben.

Wir konnten im Rahmen unseres Pilotversuchs mit einer speziell konfigurierten Version von Microsoft

365 einen datenschutzkonformen Betrieb nicht feststellen, insbesondere konnten wir für zahlreiche Datenflüsse und Übermittlungen personenbezogener Daten keine Rechtsgrundlage finden. Dies muss eine verantwortliche Schule aber können, da sie rechenschaftspflichtig ist. Dass wir mit unserer intensiven Arbeit und unter Einbezug des Kultusministeriums und Microsoft selbst keine datenschutzrechtlich tragfähige Lösung finden konnten, sollte aber nicht ausschließen, dass die Schulen doch noch einen anderen Weg gefunden haben könnten, einen datenschutzkonformen Betrieb sicherzustellen. Daher gaben wir den angeschriebenen Schulen die Möglichkeit, gemäß ihrer Rechenschaftspflicht nach Artikel 5 Absatz 2 DS-GVO die Datenschutzkonformität ihrer Konfiguration nachzuweisen. Dazu bezogen wir uns auf unsere im Rahmen des Pilotversuchs erhobenen Befunde und Messungen und baten um entsprechende Nachweise. Alternativ baten wir um einen Zeitplan zur Umstellung zu anderen Produkten.

Wir erkannten bald, dass zu dieser Problematik ein großer Beratungsbedarf an den Schulen bestand. Dies ist sehr verständlich, da die Prüfungen und Messungen sehr komplex sind und die Schulen in der Regel überfordern. Wir begannen daraufhin die Schulen datenschutzrechtlich zu beraten. Von den Schulen beziehungsweise Schulträgern wurden uns dabei auch weitere technische Lösungen vorgeschlagen, wie die datenschutzrechtliche Problematik bei der Verwendung von Microsoft 365 vermieden werden könne. Es zeigte sich jedoch, dass die genannten Lösungen im schulischen Umfeld nicht umsetzbar sind beziehungsweise die vorhandenen datenschutzrechtlichen Probleme nicht lösen können.

Weiterhin verwiesen einige Schule auf ein Urteil des OLG Karlsruhe vom 7. September 2022 zur Ausschreibung einer öffentlichen Stelle (OLG Karlsruhe, Beschl. v. 7.9.2022 – 15 Verg 8/22). Demnach darf ein öffentlicher Auftraggeber bei einem Vergabeverfahren grundsätzlich davon ausgehen, dass ein Bieter seine vertraglichen Zusagen erfüllen wird. Allerdings muss er aber auch, wenn sich konkrete Anhaltspunkte dafür ergeben, dass dies zweifelhaft ist, durch Einholung ergänzender Informationen die Erfüllbarkeit des Leistungsversprechens beziehungsweise die hinreichende Leistungsfähigkeit des Bieters prüfen (RndNr 35 a.a.O.). Dieser zweite Teil des Urteils war den Schulen leider vielfach nicht bekannt.

Ausgehend von unseren veröffentlichten Aussagen liegen hier entsprechende Anhaltspunkte vor, sodass die Schule, auch nach diesem Urteil, die Einhaltung der Anforderungen prüfen muss. Das Urteil entspricht insoweit unserem Vorgehen gegenüber den Schulen.

Hinreichende Nachweise, welche unsere Befunde und Messungen für die bei ihnen angewandte Konfiguration widerlegen, konnte uns bisher keine der von uns angeschriebenen Schulen vorlegen. Einige der angeschriebenen Schulen waren bereits vorher auf andere Produkte umgestiegen beziehungsweise planten bereits einen Umstieg. Mit Blick auf derartige Umstiege oder konkrete Umstellungspläne ge-

Digitalisierung und Datenschutz gehören auch in der Schule zusammen.

hen wir davon aus, dass in absehbarer Zeit die Umstellung abgeschlossen ist. Wir empfehlen dringend allen Schulen rasch umzustellen. Sollten weitere Beschwerden bei uns eingehen, werden wir auch diesen nachgehen. Aufgrund der den Schulen nun seit längerem bekannten Problematik wird in diesen Fällen die Zeit zur Umstellung in Zukunft jedoch deutlich kürzer bemessen sein, um die Rechte und Freiheiten der betroffenen Personen schneller zu gewährleisten. Inwieweit Schadenersatzforderungen nach Artikel 82 DS-GVO auf die Schulen zukommen werden und wie diese die Gerichte bewerten, muss sich noch zeigen. Dem Kultusministerium, als der obersten Dienstaufsicht der Schulen, empfehlen wir dringend die Schulen mit Nachdruck auf diese Problematik hinzuweisen, um sie vor Schaden zu bewahren, zumal nun gute Alternativen im Rahmen der Digitalen Bildungsplattform zur Verfügung stehen werden.

Bundesregierung teilt Einschätzung des LfDI

Ende November vergangenen Jahres hat die Datenschutzkonferenz der Länder und des Bundes ein einem einstimmigen Beschluss folgende festlegung getroffen: *„Die DSK stellt unter Bezugnahme auf die Zusammenfassung des Berichts fest, dass der Nachweis von Verantwortlichen, Microsoft 365 datenschutzrechtskonform zu betreiben, auf der Grundlage des von Microsoft bereitgestellten ‚Datenschutznachtrags vom 15. September 2022' nicht geführt werden kann. Solange insbesondere die notwendige Transparenz über die Verarbeitung personenbezogener Daten aus der Auftragsverarbeitung für Microsofts eigene Zwecke nicht hergestellt und deren Rechtmäßigkeit nicht belegt wird, kann dieser Nachweis nicht erbracht werden."* Auch der LfDI hat sich an der Arbeitsgruppe beteiligt.

Wir haben öffentlich erklärt, dass aus unserer Sicht es ohne weitere Maßnahmen der verantwortlichen Stellen beim Einsatz der Software sehr schwer wird, ihrer Rechenschaftspflicht nachzukommen. Am 9. Dezember 2022 hat die Bundesregierung auf eine Anfrage eines Bundestagsabgeordneten sich unserer rechtlichen Auffassung angeschlossen (siehe S. 44).

☛ Mehr Informationen:

Unsere Pressemitteilungen: www.baden-wuerttemberg.datenschutz.de/ms-365-schulen-hinweise-weiteres-vorgehen
www.baden-wuerttemberg.datenschutz.de/nutzung-von-ms-365-an-schulen
www.baden-wuerttemberg.datenschutz.de/microsoft-365-an-schulen-was-kommt-auf-die-schulen-zu
www.baden-wuerttemberg.datenschutz.de/schulen-auf-dem-weg-zu-datenschutzfreundlichen-loesungen

Unsere Stellungnahme mit unseren Befunden und Messungen im Piloten des Kultusministeriums zu Microsoft 365: fragdenstaat.de/anfrage/neubewertung-des-lfdi-bezuglich-der-dsfa-von-microsoft-office-365-1 mit den Anlagen unter fragdenstaat.de/anfrage/bewertungen-und-empfehlungen-des-lfdi-zu-office-365-an-schulen

Festlegung der Datenschutzkonferenz zu „Microsoft Online-Diensten" vom 24.11.22: datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365.pdf

Zusammenfassung des Berichts der Arbeitsgruppe DSK „Microsoft Onlines-Dienste" vom 24.11.: datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf

Abschlussbericht der Arbeitsgruppe DSK „Microsoft Onlines-Dienste" vom 7.12.: datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf

Stellungnahme Bundesregierung auf Anfrage Bundestagsabgeordneten vom 9.12.; Ziffer 57 (Seite 52): dserver.bundestag.de/btd/20/048/2004852.pdf

Zu Moodle und „BelWÜ": LT-Drs. 17/15, S. 4 und Beitrag Nr. 26 – „Neuausrichtung der IT-Koordinierungsstelle für das BelWü-Netz (Kapitel 1418)" – Denkschrift 2021 Landesrechnungshofs zur Haushaltsrechnung 2019, in LT-Drs. 17/326: rechnungshof.baden-wuerttemberg.de/de/veroeffentlichungen/denkschriften

4. Europa ruft!

Die Datenschutz-Grundverordnung wahrt die Bürgerrechte der Europär_innen.

Auch im Jahr 2022 hat die Corona-Pandemie natürlich weiterhin die Arbeit auf europäischer Ebene und in unserer Stabsstelle Deutsche und Europäische Zusammenarbeit erheblich beeinflusst. Die Sitzungen sowie die Arbeiten an Projekten der Arbeitsgruppen des Europäischen Datenschutzausschusses (EDSA) waren weiterhin oft in den digitalen Bereich verlagert, es war glücklicherweise jedoch auch wieder vermehrt möglich, sich vor Ort zu treffen oder Sitzungen jedenfalls hybrid durchzuführen. Der über die Zeit erfolgte Ausbau der Online-Möglichkeiten hat jedoch die Kommunikation mit anderen europäischen und deutschen Aufsichtsbehörden zu Einzelthemen verstärkt möglich gemacht. Daneben haben auch wir vermehrt Online-Materialien für unsere Homepage entwickelt und die Anzahl an Online-Inhouse-Schulungen zu aktuellen Entwicklungen aus allen Themenbereichen für das eigene Kollegium noch ausgebaut.

4.1 Aktuelle Leitlinien des Europäischen Datenschutzausschusses

4.1.1. Täuschendes Design auf Social Media Plattformen

Im Frühjahr 2022 nahm der Europäische Datenschutzausschuss die Leitlinien zu sogenannten „Dark patterns“ bei der Oberflächengestaltung sozialer Netzwerke an („Guidelines 03/2022 on dark patterns in social media platform interfaces: how to recognise and avoid them“). „Dark patterns“ werden in letzter Zeit auch verstärkt als „deceptive design patterns“ bezeichnet. Dahinter verbergen sich Manipulationstechniken, die auf die Ausnutzung menschlichen Verhaltens ausgerichtet sind und der Beeinflussung von Menschen dienen. Bereits in den 1970er Jahren beschäftigten sich Forschende mit Verhaltensbeeinflussung, wobei dabei auch positive Effekte der Beeinflussung zum Wohle von

Menschen in den Blick genommen wurden. Die von den Leitlinien thematisierten täuschenden Designs haben dagegen eine für Nutzer_innen nachteilige Beeinflussung zum Ziel. Zum Beispiel verleiten sie dazu, unnötig viele personenbezogene Daten von sich preiszugeben oder sich einer Datenverarbeitung nur zu unterwerfen, um nicht immer wieder nach der dafür gegebenenfalls nötigen Einwilligung gefragt zu werden.

Solche Praktiken sind häufig sehr effektiv, da den Nutzer_innen gar nicht bewusst ist, dass sie gerade manipuliert werden – beispielsweise dadurch, dass sie aufgrund von „drängelnden" Formulierungen vorschnelle Entscheidungen treffen oder wichtige Informationen so unscheinbar gestaltet sind, dass die Nutzer_innen sie schlicht übersehen. Die Leitlinien entstanden in der Social Media Expert Subgroup des EDSA, in der die Stabsstelle für den LfDI sowohl die Rolle einer Ländervertreterin als auch die einer Koordinatorin wahrnimmt. Entworfen wurden die Leitlinien in europäischer Team-Arbeit unter gemeinsamer Federführung durch uns und die französische Aufsichtsbehörde Commission Nationale de l'Informatique et des Libertés (CNIL). Wenngleich sich die Leitlinien thematisch auf soziale Medien konzentrieren, sind täuschende Designs auch auf anderen Plattformen zu finden.

In einer öffentlichen Konsultation wurde Nichtregierungsorganisationen, Unternehmen, Verbänden und interessierten Personen die Möglichkeit geboten, Anmerkungen zur ersten Fassung der Leitlinien einzureichen. Die endgültige Annahme der Leitlinien ist für das erste Halbjahr 2023 zu erwarten und wird auf unserer Homepage sowie auf der des EDSA bekannt gegeben.

Im Rahmen des Global Privacy Enforcement Network (GPEN) stellten wir die Leitlinien Kolleg_innen von Datenschutzaufsichtsbehörden aus aller Welt vor. Zudem bot die BvD-Herbstkonferenz in Stuttgart den dortigen Teilnehmenden die Gelegenheit, neben Informationen zu den Leitlinien auch allgemeine Hinweise zur Vermeidung „manipulativer Designs auf Online-Plattformen" zu erhalten – sowohl aus der Perspektive verantwortlicher Stellen als auch aus derjenigen betroffener Personen. Interessierte Bürger_innen können sich im ersten Quartal 2023 im Rahmen eines BIDIB-Vortrags wertvolle Tipps abholen, wie sie im Internet und insbesondere auf Social Media wieder bewusstere Entscheidungen treffen, um ihre Daten zu schützen und ihr Portemonnaie zu schonen.

4.1.2 Die gütliche Einigung

Im Mai 2022 veröffentlichte der EDSA zudem die Leitlinien 06/2022 zur praktischen Umsetzung gütlicher Einigungen („Amicable Settlements") bei der Bearbeitung grenzüberschreitender Fälle. (Die Leitlinien sind derzeit nur auf Englisch verfügbar. Die deutsche Übersetzung ist zeitnah zu erwarten.) Hierbei sollte das Verfahren des One-Stop-Shop-Mechanismus (Kooperationsverfahren) gemäß der DS-GVO genau so berücksichtigt werden wie die verschiedenen nationalen Verfahrensvorschriften, soweit vorhanden, und das technische Umfeld der Fallbearbeitung im IMI-System. Wir fungierten bei der Erstellung der Leitlinien als federführender Hauptberichterstatter.

Die Leitlinien basieren auf einem Fragebogen, der an alle europäischen Aufsichtsbehörden versendet wurde, um tiefergehende Informationen über den Anwendungsbereich und Erfahrungen im Umgang mit gütlichen Einigungen zu sammeln sowie Kommentare und Vorschläge zu möglichen Vorgehensweisen zu erhalten. Die eingegangenen Beiträge haben gezeigt, dass es verschiedene Varianten von gütlichen Einigungen gibt und diese daher von den Aufsichtsbehörden unterschiedlich gehandhabt werden. Ziel der Leitlinien war es daher, Best Practices für die Handhabung dieser Fälle im Koope-

☛ Mehr Informationen:

LfDI zu den Dark-Pattern-Leitlinien:
www.baden-wuerttemberg.datenschutz.de/mehr-klarheit-mit-den-neuen-europaeischen-leitlinien-zu-dark-patterns

Dark-Pattern-Leitlinien des EDSA:
edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

Leitlinien des EDSA zur gütlichen Einigung:
edpb.europa.eu/system/files/2022-06/edpb_guidelines_202206_on_the_practical_implementation_of_amicable_settlements_en.pdf

rationsverfahren bereitzustellen, um eine einheitliche Anwendung der DS-GVO auf nationaler und EU-Ebene zu gewährleisten.

Die Leitlinien umfassen vier Absätze sowie einen Anhang. Im ersten Teil wird eine Einleitung über den Anwendungsbereich und das Ziel der Leitlinien gegeben, gefolgt von einem kurzen Überblick über mögliche Definitionen des Begriffs „gütliche Einigung" aus verschiedenen Kontexten. Der größte und wichtigste Teil ist eine allgemeine rechtliche Analyse der Gründe für Amicable Settlements und der Befugnisse der Aufsichtsbehörden in verschiedenen Fallkonstellationen, wobei der Schwerpunkt auf den Merkmalen der Fälle liegt, die sich besonders für eine gütliche Einigung eignen können.

Besonders relevant sind die Ausführungen zur Rechtsgrundlage. In einigen Mitgliedsstaaten gibt es explizite nationale Regelungen für gütliche Einigungen und deren (prozessualen) Voraussetzungen sowie Folgen. In vielen Mitgliedsstaaten fehlt es jedoch an einer solchen Normierung. Hier schaffen die Leitlinien Abhilfe. Denn in ihnen wird festgestellt, dass sich Aufsichtsbehörden dort, wo es an nationalen Vorschriften fehlt, grundsätzlich eines Amicable Settlements anhand von Artikel 57 Absatz 1 lit. a) und f) DS-GVO bedienen können, da sich daraus die Grundlage der Behörde ergibt, alle möglichen Wege zu suchen, um Beschwerden zu „bearbeiten" und die Anwendung der Verordnung gegebenenfalls „durchzusetzen".

Im letzten Teil werden die rechtlichen Folgen und die praktischen Empfehlungen für das Kooperationsverfahren und die Anwendung des OSS-Mechanismus dargestellt. Die größte Errungenschaft ist dabei in der Aussage der Leitlinien zu finden, dass in allen Fällen – und damit auch in solchen, in denen Beschwerden mit einer gütlichen Einigung beendet werden – ein formeller Beschlussentwurf gemäß Art. 60 Abs. 3 DS-GVO erstellt werden muss, der der Überprüfung der anderen (betroffenen) Aufsichtsbehörden unterliegt. Während in der Vergangenheit solche Fälle häufig ohne die (hinreichende) Einbeziehung der anderen europäischen Aufsichtsbehörden abgeschlossen wurden, steht damit nun die formelle Voraussetzung fest, das Kooperationsverfahren nach Art. 60 DS-GVO ordnungsgemäß durchzuführen und alle notwendigen Informationen über die Verfahren den übrigen betroffenen Behörden mitzuteilen. Die Leitlinien enthalten jedoch auch einen Vorschlag, wie in solchen Fällen sowohl der Beschlussentwurf als auch das Kooperationsverfahren unter Umständen beschleunigt beziehungsweise „vereinfacht" werden können, um dem beiderseitig gütlichen Ausgang des Falls Rechnung zu tragen. Der Anhang enthält schließlich eine Checkliste, in der die relevanten Schritte aufgeführt sind, die die (federführende) Aufsichtsbehörde bei der Bearbeitung eines Falles im Wege der gütlichen Einigung zu berücksichtigen hat.

4.1.3 Das Auskunftsrecht nach Art. 15 DS-GVO

Bereits im Januar 2022 wurden die Leitlinien 01/2022 zum Auskunftsersuchen nach Artikel 15 DS-GVO angenommen. Darin wird unter anderem klargestellt, dass das Recht auf Kopie nach Artikel 15 Abs. 3 DS-GVO kein zusätzliches Betroffenenrecht ist, sondern eine „Modalität" des Auskunftsrechts. Dabei bedeutet Auskunft über personenbezogene Daten grundsätzlich eine vollständige Information über alle Daten und keine bloße Zusammenfassung.

☛ Mehr Informationen:

Leitlinien zum Auskunftsrecht:
edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_en

Weitere Leitlinien des EDSA:
edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en

edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-062022-practical-implementation-amicable_en

edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en (derzeit nur auf Englisch verfügbar; die übersetzten alten Leitlinien ohne die aktualisierte Rn. 73:
ec.europa.eu/newsroom/article29/items/612052)

Bei der Erteilung der Auskunft sind folgende Schritte zu beachten:

1. Betrifft das Ersuchen personenbezogene Daten?

2. Bezieht sich das Ersuchen auf die ersuchende Person (beziehungsweise deren Vollmachtgeber_in)?

3. Sind neben der DS-GVO weitere spezielle Normen anwendbar?

4. Fällt das Ersuchen unter Artikel 15 DS-GVO? Geht es um eine Voll- oder Teilauskunft?

Der EDSA empfiehlt, für die Form des Auskunftsersuchens die angemessensten und nutzer_innenfreundlichsten Kommunikationskanäle bereitzustellen. Ersuchen sind aber grundsätzlich auch dann zu beantworten, wenn sie über andere Kanäle hereinkommen – zum Beispiel, wenn Betroffene sich an die allgemeine Kontaktadresse aus dem Impressum wenden. Verantwortliche haben durch technische und organisatorische Maßnahmen dafür zu sorgen, dass diese Anfragen an die zuständigen Stellen im Unternehmen oder der Behörde weitergeleitet und fristgerecht beantwortet werden. Bei Auskunftsersuchen, die durch Dritte für Betroffene geltend gemacht werden, sind nationale Vorschriften zu beachten, da die DS-GVO hier keine eigene Regelung trifft. Eine Besonderheit gilt insofern für Auskunftsersuchen zu Daten von Kindern: Tragender Gesichtspunkt für die Bewertung, ob der_die Dritte ersuchensberechtigt ist, sind die wohlverstandenen Interessen des Kindes.

Eine Verweigerung der Erfüllung des Auskunftsersuchens nach Artikel 12 Abs. 2 DS-GVO ist nur möglich, wenn Verantwortliche glaubhaft machen, dass eine Identifizierung der betroffenen Person nicht möglich ist. Für die Identifizierung dürfen Verantwortliche jedoch nicht mehr personenbezogene Daten anfordern, als nötig ist (Artikel 12 Abs. 6 DS-GVO). Hier ist eine Angemessenheitsprüfung durchzuführen. Grundsätzlich gilt: Kopien von Personalausweisen oder Reisepässen stellen ein Sicherheitsrisiko dar und dürfen nur angefordert werden, wenn dies unbedingt erforderlich, zur Identifizierung geeignet und mit nationalem Recht vereinbar ist. Dabei müssen unnötige Daten von Betroffenen geschwärzt oder verborgen werden können. Bei digitalen Kommunikationskanälen sollten Verantwortliche bereits existierende Authentifizierungsprozesse nutzen oder solche Prozesse einrichten.

> ☛ Mehr Informationen:
>
> Beschluss 1/2022 zur Streitigkeit nach Artikel 65 Absatz 1 Buchstabe a DSGVO über den Beschlussentwurf der französischen Aufsichtsbehörde bezüglich der Accor SA:
> edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/decision-012022-dispute-arisen-draft_de
>
> Beschluss 2/2022 zur Streitigkeit nach Artikel 65 Absatz 1 Buchstabe a DSGVO über den Beschlussentwurf der irischen Aufsichtsbehörde bezüglich der Meta Platforms Ireland Limited (Instagram):
> edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-22022-dispute-arisen_en

4.1.4 Hinweis auf weitere Leitlinien

Ebenfalls im Mai 2022 nahm der EDSA die Leitlinien 04/2022 zur Berechnung von Bußgeldern nach der DS-GVO an. Die Bußgeldberechnung steht im Ermessen der verhängenden Aufsichtsbehörde, wobei die Kriterien des Artikel 83 DS-GVO zu beachten sind. Die Leitlinien werden in Deutschland das Bußgeldkonzept der Datenschutzkonferenz ablösen.

Im Herbst 2022 wurden die noch unter der Artikel 29 Arbeitsgruppe entstandenen Leitlinien zu Datenpannen im Rahmen eines „targeted update" an einer Stelle aktualisiert. Daher sind diese hilfreichen Leitlinien nunmehr unter der Nummer 09/2022 auf der Homepage des EDSA zu finden. Wir empfehlen insbesondere einen Blick auf die Tabelle im Anhang B sowie in die Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten. Darin finden sich konkrete Beispiele, wann eine Datenpanne an die Aufsichtsbehörde zu melden ist (Artikel 33 DS-GVO) beziehungsweise wann auch betroffene Personen zu benachrichtigen sind (Artikel 34 DS-GVO).

4.2 Streitbeilegungsverfahren

In grenzüberschreitenden Fällen haben betroffene Aufsichtsbehörden die Möglichkeit, maßgebliche

und begründete Einsprüche gegen Beschlussentwürfe der federführenden Aufsichtsbehörde einzulegen. Schließt sich die federführende Behörde dem Einspruch nicht an oder lehnt diesen ab, geht das Verfahren zur Streitbeilegung gemäß Artikel 65 DS-GVO in den Europäischen Datenschutzausschuss. Dieser erlässt dann einen verbindlichen Beschluss, dem die federführende Behörde nachzukommen hat.

In Berichtjahr 2022 gab es gleich mehrere Streitbeilegungsverfahren. Im Juni wurde die französische Aufsichtsbehörde vom EDSA verpflichtet, bei der Berechnung des Bußgelds gegen die Accor SA den Umsatz des Jahres 2021 zu berücksichtigen und die abschreckende Wirkung der Geldbuße sicherzustellen. Auch im nächsten Verfahren ging es unter anderem um die Bußgeldhöhe: Der EDSA verpflichtete die irische Aufsichtsbehörde (Irish Data Protection Commission) im Juli, das Bußgeld gegen Instagram (Meta Platforms Ireland Limited) anzupassen. So kam es infolge der Intervention der anderen europäischen Aufsichtsbehörden zu einem Rekordbußgeld in Höhe von 405 Millionen Euro gegen Instagram. In dem Fall ging es um Daten von Kindern: Kinder, die das Instagram Businesskonto nutzten, mussten im maßgeblichen Zeitraum ihre E-Mail-Adressen und Telefonnummer angeben, die per Voreinstellung für die gesamte Öffentlichkeit sichtbar waren. Die Entscheidung ist als eine historische zu würdigen; nicht nur aufgrund der Bußgeldhöhe, sondern auch als EU-weit erster Beschluss zum Datenschutz von Kindern. Man sieht also: Die Europäische Zusammenarbeit wirkt!

4.3 Immer noch aktuell – Die Nutzung sozialer Netzwerke durch öffentliche Stellen

Nicht nur Unternehmen und Vereine, sondern auch öffentliche Stellen setzen für Informations- und Kommunikationsangebote inzwischen verstärkt auf soziale Netzwerke. Viele öffentliche Stellen wie Ministerien, Kommunen oder Verwaltungsbehörden betreiben deshalb sogenannte Fanpages für den eigenen Auftritt in dem sozialen Netzwerk. Aber wo bleibt da der Datenschutz?

Grundsätzlich ist wohl etwas dran an dem Bedürfnis der öffentlichen Stellen, die Bürgerschaft über alle verfügbaren Kanäle mit relevanten Neuigkeiten und Informationen aus der Verwaltung zu versorgen. Über soziale Netzwerke, die der Kommunikation, Interaktion und Präsentation ihrer Mitglieder dienen, soll auf die digitalisierte Welt eingegangen und ein breiteres, oftmals auch jüngeres Publikum erreicht werden. Datenschutzrechtlich gilt es dabei jedoch einiges zu beachten. Denn während die öffentlichen Stellen ihre Informationen über die Plattformen bequem und schnell veröffentlichen können, werden – je nach Plattformbetreiber – bei der Einbindung der Inhalte in der Regel personenbezogene Daten der Besucher_innen wie IP-Adresse oder Cookies an die Plattformbetreibenden und an Drittanbieter (beispielsweise Partnerunternehmen des kommerziellen Plattformanbieters) übermittelt – und zwar sowohl von den Besucher_innen, die bei der Plattform des sozialen Netzwerks registriert sind, als auch von den nicht registrierten. Über die sogenannte „Insights-Funktion" werden personenbezogene Daten der Besucher_innen zur Erstellung von Nutzerprofilen, Seitenstatistiken über die Nutzung von Fanpages und zu Werbezwecken genutzt.

In verschiedenen Entscheidungen (insbesondere Rs. C-40/17 „Fashion ID" und Rs. C-210/16 „Wirtschaftsakademie") hat der Europäische Gerichtshof inzwischen ausdrücklich festgestellt, dass die Stellen, die einen eigenen Auftritt auf sozialen Netzwerken betreiben, für das Erheben personenbezogener Daten und deren Weiterleitung durch Übermittlung an Drittanbieter in der Regel mit den Plattformbetreibenden gemeinsam verantwortlich im Sinne von Artikel 26 der europäischen DS-GVO sind. Dem folgten Urteile des Bundesverwaltungsgerichts (Az. 6 C 15.18) und des Oberverwaltungsgerichts Schleswig (Az. 4 LB 20/13).

Öffentliche Stellen müssen danach insgesamt die Rechtmäßigkeit der gemeinsam zu verantwortenden Datenverarbeitung gewährleisten und die Ein-

☛ Mehr Informationen:

„Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages" (Version 1: www.datenschutzkonferenz-online.de/media/weitere_dokumente/DSK_Kurzgutachten_Facebook-Fanpages_V1_18.03.2022.pdf
In der nächsten Zeit dürfte Version 2 auf der DSK-Homepage veröffentlicht werden.

haltung der Grundsätze aus Artikel 5 Absatz 1 DS-GVO nachweisen. Sie unterliegen als (Mit-) Verantwortliche der Rechenschaftspflicht aus Artikel 5 Absatz 2 DS-GVO und insbesondere der Verpflichtung, technisch-organisatorische Maßnahmen im Sinne der Artikel 24, 25 und 32 DS-GVO zu ergreifen. Zudem ist im Rahmen der gemeinsamen Verantwortlichkeit eine umfassende, für die betroffenen Personen transparente vertragliche Vereinbarung erforderlich (Artikel 26 Absatz 1 Satz 2 und Absatz 2 DS-GVO). Doch unsere Praxis zeigt: Diese Voraussetzungen sind in der Praxis kaum einzuhalten. Die öffentlichen Stellen können ihrer Nachweispflicht hinsichtlich der Rechtmäßigkeit der Datenverarbeitung bei den kommerziellen Plattformbetreibern in der Regel nicht nachkommen und auch keine (hinreichende) Vereinbarung zur gemeinsamen Verantwortlichkeit nach Artikel 26 DS-GVO vorlegen. Sie sind nicht in der Lage, die genauen Verarbeitungen, die mit dem Betrieb ihres Kanals auf dem sozialen Netzwerk einhergehen, zu benennen und können dementsprechend auch nicht die notwenige Transparenz den Betroffenen gegenüber herstellen.

Das macht auch das veröffentlichte „Kurzgutachten zur datenschutzrechtlichen Konformität des Betriebs von Facebook-Fanpages" der Datenschutzkonferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) deutlich. Die DSK beleuchtet darin die datenschutzrelevanten Aspekte, die es bei dem Betrieb einer Facebook-Fanpage zu beachten gilt, (Dabei ist davon auszugehen, dass die in dem Kurzgutachten getroffenen Aussagen auch auf den Betrieb eines Kanals in anderen kommerziellen sozialen Netzwerken übertragbar sind.)

Nach dem Prüfungsergebnis der DSK ist die Datenverarbeitung, die bei dem Besuch einer Fanpage vorgenommen wir, weder mit der DS-GVO noch mit dem TTDSG vereinbar, da es an einer wirksamen Rechtsgrundlage und der erforderlichen Transparenz fehlt. Die Einwilligung der Bürger_innen kann schon mangels hinreichender Informationen über die durchgeführten Datenverarbeitungen nicht wirksam eingeholt werden; und eine Ausnahme vom Einwilligungserfordernis besteht nicht. Auf das berechtigte Interesse können sich öffentliche Stellen nicht stützen. Denn die auf das berechtigte Interesse gestützte Verarbeitungsbefugnis aus Artikel 6 Absatz 1 Satz 1 lit. f) DS-GVO ist nach Satz 2 dieser Vorschrift auf die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung nicht anwendbar. Gerade die Erfüllung ihrer Aufgaben ist aber die Argumentation der öffentlichen Stellen, warum sie soziale Netzwerke nutzen. Überdies lässt die bereits beschriebene mangelhafte Informationslage zu den einzelnen Verarbeitungen beim Betrieb einer Fanpage die für das berechtigte Interesse erforderliche umfangreiche Interessenabwägung nicht zu. Und auch wenn öffentliche Stellen soziale Netzwerke in der Regel für ihre Öffentlichkeitsarbeit nutzen, sodass eine Verarbeitung in Erfüllung einer öffentlichen Aufgabe in Betracht kommt, kann eine über die Öffentlichkeitsarbeit hinausgehende Auswertung der Daten der Bürger_innen nicht mehr von dieser Rechtsgrundlage gedeckt sein. Und: Ohne hinreichende Informationen kommt auch keine rechtskonforme Vereinbarung über die gemeinsame Verantwortlichkeit zustande und lassen sich die Transparenzpflichten nicht erfüllen. Das Problem des Drittstaatentransfers kommt ggf. noch hinzu. (vgl. hierzu auch Kapitel 4.4. zur Executive Order).

Nun könnte man meinen, die allseits diskutierte Abschaltung der „Insights-Funktion" könnte die Lösung für all diese Probleme sein. Verantwortliche Stellen, privat wie öffentlich, führen immer wieder an, die Abschaltung der Insights – so sie denn möglich ist – befreie sie aus der gemeinsamen Verantwortlichkeit und damit aus den datenschutzrechtlichen Fallstricke beim Betrieb einer Fanpage. Und das lässt sich durchaus hören. Zwar könnte grundsätzlich argumentiert werden, die gemeinsame Bestimmung von Zwecken und Mitteln folge auch ohne die Verarbeitung von Insights bereits daraus, dass die öffentlichen Stellen durch den Betrieb der Fanpage und die verbundene Datenverarbeitung im eigenen Interesse die Reichweite gegenüber den Bürger_innen erhöhen und sich den Netzwerk-Effekt des sozialen Netzwerks zunutze machen, welches wiederum von den Nutzenden-Daten für das eigene Geschäftsmodell profitiert.

Allerdings darf nicht übersehen werden, dass der Europäische Gerichtshof in seinem Urteil Wirtschaftsakademie (Rn. 33 ff.) eben ganz entschieden auf die Parametrierung abstellt, sprich die den eigenen Zielen entsprechende Verarbeitung der vom sozialen Netzwerk ausgewerteten Daten durch

dessen Einbindung – und zwar im Rahmen der Verarbeitung der Insights. Ob die Verfügung einer Aufsichtsbehörde an eine öffentliche (oder auch private) Stelle, ihre Fanpage abzuschalten, trotz Deaktivierung der Insights-Funktion Bestand haben und dem Verhältnismäßigkeitsprinzip gerecht werden kann, bleibt demnach abzuwarten. Wir werden hierzu die zu erwartende Rechtsprechung aufmerksam verfolgen.

Als Folge der hier dargestellten Problematik entschieden wir uns bekanntermaßen selbst bereits Anfang 2020 dazu, aus Twitter auszusteigen und den öffentlichen Account dort zu löschen. Das Zauberwort für uns lautet: Alternativkanäle! Auf diese setzen wir sowohl im eigenen Doing als auch in unserer Beratungspraxis. Entsprechend beraten wir die Landesregierung sowie sonstige öffentliche Stellen des Landes Baden-Württemberg zum Aufbau datenschutzkonformer Angebote in Alternative zu den kommerziellen sozialen Netzwerken. Datenschutzkonforme Kommunikationsplattformen wie Mastodon oder PeerTube ermöglichen einen regen digitalen Austausch mit den Menschen, ohne ihre Daten in die Hand kommerzieller Unternehmen zu geben. Und die Plattformen erfreuen sich aktuell über viele und immer mehr neue Nutzende.

Öffentliche Stellen müssen gemeinsam ein Zeichen setzen und mit gutem Beispiel vorangehen, den kommerziellen Anbietern entgegentreten, es besser machen. Sie müssen ihre staatlichen Informationen in einem ersten Schritt auch über alternative Kanäle zur Verfügung stellen. Und je mehr öffentliche Stellen dies tun, desto mehr erreichen wir die wünschenswerte Reichweite der öffentlichen Verwaltung über dezentrale soziale Netzwerke – ganz im Sinne der Nachhaltigkeit, indem Datenschutz und Digitalisierung zusammen gedacht und gemacht werden.

☛ Mehr Informationen:

Executive Order (Durchführungsverordnung) des US-Präsidenten vom 7.10.22:
www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities

Das Thema ist und bleibt aktuell. So wurde die Nutzung von Social Media durch öffentliche Stellen auch dieses Jahr wieder mit den Datenschutzbeauftragten der Ministerien erörtert, mit denen wir an zwei Terminen im Jahr in einem „Arbeitskreis Datenschutz“ einen regen und sehr fruchtbaren Austausch zu den aktuellen Datenschutz-Themen pflegen.

4.4 Internationaler Datentransfer – Die neue Executive Order der USA

Das letzte Quartal 2022 stand noch einmal ganz besonders im Zeichen des Drittstaatentransfers. Bereits am 16. Juli 2020 hatte der Europäische Gerichtshof in seinem sogenannten „Schrems II“-Urteil (Rs. C-311/18) das EU-US Privacy Shield für ungültig erklärt, weil dieses kein mit der EU vergleichbares Datenschutz-Niveau gewährleiste. Das Gericht stellte dabei zum einen auf den weitreichenden Zugriff durch US-Behörden, insbesondere des Nachrichtendienstes, auf Daten von Wirtschaftsunternehmen ab, die personenbezogene Daten von EU-Bürger_innen verarbeiten. Die pauschale und undifferenzierte Massenerhebung personenbezogener Daten verstößt dabei nach Ansicht des Gerichtshofs gegen das Verhältnismäßigkeitsprinzip aus Artikel 52 Grundrechtecharta. Zum anderen mangelt es nach Einschätzung des Gerichtshofs an einem ausreichenden Rechtsschutz für EU-Bürger_innen, da ihnen als Nicht-Amerikaner_innen keine Beschwerdemöglichkeit gegen den Zugriff auf die eigenen Daten und kein Zugang zu unabhängigen Gerichten offensteht. Datenübermittlungen in die USA können mithin nicht mehr auf das Privacy Shield gestützt werden. Im März dieses Jahres verkündeten die Europäische Kommission und US-Präsident Biden, eine grundsätzliche Einigung über einen neuen EU-US-Datenschutzrahmen erzielt zu haben. In den folgenden Monaten erfolgte die Arbeit an der endgültigen Festlegung und Umsetzung dieser Vereinbarung.

Nun hat US-Präsident Biden am 7. Oktober 2022 eine Executive Order (Durchführungsverordnung) erlassen, welche die angekündigte Grundsatzvereinbarung in US-Recht umsetzen soll. Die darin enthaltenen Vorgaben beschränken nunmehr den Zugriff auf personenbezogene Daten von EU-Bürger_innen aufgrund nachrichtendienstlicher Tätigkeiten auf erforderliche („necessary“) und angemessene („pro-

portionate“) Fälle. Die USA implementieren damit Beschränkungen im Sinne des europäischen Verhältnismäßigkeitsprinzips (Artikel 52 Grundrechtecharta). Zudem enthält die Executive Order Regelungen zu einem zweistufigen Beschwerde- beziehungsweise Rechtsbehelfsverfahren, die durch eine Verordnung des Department of Justice ergänzt wird. Als erste Ebene wird ein Civil Liberties Protection Officer im Office of the Director of National Intelligence (CLPO) eingerichtet, der als unabhängige Stelle Beschwerden über bestimmte Verstöße im Zusammenhang mit den Aktivitäten des US-Nachrichtendienstes unter Abwägung der beiderseitigen Interessen untersuchen und gegebenenfalls Maßnahmen treffen soll. Auf der zweiten Stufe wird ein Data Protection Review Court (Datenschutzprüfungsgericht) installiert, das die Entscheidungen des CLPO auf Antrag überprüfen soll.

Wir begrüßen diese neuesten Entwicklungen grundsätzlich. Dass die US-Regierung im Hinblick auf das Datentransfer-Abkommen aktiv wird, ist ein wichtiger und guter Schritt in die richtige Richtung. Er könnte insbesondere ein Weg aus der inakzep-tablen Rechtsunsicherheit sein, in welcher sich unsere Unternehmen infolge der Entscheidung des EuGH befinden. Um Europa langfristig nicht als wichtigen Handelsund Unternehmenspartner zu verlieren, müssen sich die USA auf die Europäische Kommission und die europäischen Datenschutzgrundsätze zubewegen.

Die Regelungen der Executive Order werfen jedoch auch Zweifel auf und lassen noch erhebliche Defizite erkennen. Es stellt sich schon die Frage, inwieweit eine Executive Order überhaupt ein wirksames Instrument zur Umsetzung der Anforderungen sein kann, da sie als interne Anweisung an Regierung und nachgeordnete Behörden (nur) so lange in Kraft bleibt, bis sie durch den jeweils amtierenden Präsidenten abgeändert oder zurückgenommen wird. Ohne ein parlamentarisch verabschiedetes Gesetz kann also nicht die erforderliche Rechtssicherheit für alle Beteiligten eintreten. Eine bloße Executive Order ist für EU-Bürger_innen nicht einklagbar. Es ist auch nicht klar, wie sie sich zu anderen bestehenden US-Regulierungen wie insbesondere dem Cloud Act verhält.

Zudem wirken die jetzt enthaltenen Beschränkungen von Datenverarbeitungen auf erforderliche und angemessene Fälle zwar wie ein Zugeständnis im Sinne des europäischen Verhältnismäßigkeitsprinzips. Jedoch ist die Auslegung des Rechtsbegriffs der Verhältnismäßigkeit in Europa und den USA unterschiedlich. Wann ist aus Sicht der USA ein Zugriff für die nationale Sicherheit erforderlich und angemessen? Wird das die Überwachungspraxis seitens der USA wesentlich beeinflussen, wo doch eine Änderung der Sicherheitsgesetze nicht zu erwarten steht? Die Executive Order lässt Massenüberwachung („bulk surveillance“) gerade nach wie vor ausdrücklich zu. Der Europäische Gerichtshof hat jedoch nicht nur Rechtsbehelfe gegen ein staatliches Ausspähen verlangt, sondern die Beendigung dieser anlasslosen Überwachung selbst. Dieser vom EuGH geforderte Systemwechsel ist bislang nicht erkennbar.

Bezüglich der Rechtsschutzmaßnahmen ist beachtlich, dass an die Einreichung einer Beschwerde beim CLPO erhebliche Anforderungen gestellt werden. Es werden Mindestangaben aufgezählt, die erfüllt sein müssen, sodass von einem Aussieben „ungeliebter“ Beschwerden auszugehen ist. Außerdem muss die Beschwerde über eine Aufsichtsbehörde in einem „qualifying state“ eingereicht werden, wobei diese „qualifying states“ vom US-Justizminister bestimmt werden und ggf. auch geändert werden können. Rechtsschutz wird also lediglich mittelbar gewährt. Da das Data Protection Review Court innerhalb des Justizministeriums eingerichtet wird, dürfte es der Exekutive zuzurechnen sein, was auch einer richterlichen Unabhängigkeit entgegensteht.

Beschwerdeführer werden außerdem nach der Executive Order ausdrücklich nicht darüber informiert, ob sie Gegenstand von nachrichtendienstlichen Aktivitäten waren, sondern erhalten eine standardisierte Mitteilung, die besagt, dass die Überprüfung ihrer Beschwerde abgeschlossen ist und entweder keine Verstöße festgestellt wurden oder dass Abhilfemaßnahmen für erforderlich gehalten werden. Derselbe Wortlaut ist für Entscheidungen des „Gerichts“ vorgegeben. Effektiver Rechtsschutz sieht anders aus.

Es ist nun an der Europäischen Kommission, zu entscheiden, ob ein „der Sache nach gleichwertiger Schutz“ der personenbezogenen Daten in den USA gegeben ist. Sie muss sich also fragen, ob sie allein auf Grundlage der Executive Order überhaupt ernsthaft in der Lage ist, das Datenschutzniveau in den USA neu zu bewerten und einen Angemessenheitsbeschluss zu erlassen. Der EuGH wird nur eine hin-

reichende Vertrauensbasis für den Datentransfer in die USA akzeptieren können – für EU-Bürger_innen wie auch für datenexportierende Unternehmen.

4.5 Neues von der EU Kommission I: Entwurf zu CSAM (Child Sexual Abuse Material)

Ohne Zweifel gehört der Missbrauch von Kindern zu den Straftaten, denen konsequent nachgegangen werden muss. Die in einem neuen Verordnungs-Entwurf der EU-Kommission angelegte lokale Erkennung von Missbrauchsfotos von Kindern (CSAM) auf Smartphones und der hierzu vorgesehene Eingriff in die verschlüsselte Kommunikation (Chatkontrolle) müssen aber dennoch kritisch beobachtet werden. Die geplante Umsetzung schränkt die Grundrechte auf Privatsphäre und Datenschutz empfindlich ein. Dabei bestehen erhebliche Zweifel sowohl an ihrer Eignung als auch an ihrer Verhältnismäßigkeit.

Zur Kommunikation im beruflichen und privaten Umfeld wird immer mehr auf Smartphones und darauf installierte Kommunikations-Software zurückgegriffen. Die Kommunikation ist inzwischen häufig Ende-zu-Ende verschlüsselt, d.h. nur Sendende und Empfangende von Nachrichten können diese im Klartext lesen, während Dritte, auch die Anbieter_innen der Kommunikations-Software und die Hersteller_innen der Smartphones, die Nachrichten und deren Inhalte nicht (mit)lesen können. Dies ermöglicht eine vertrauliche und sichere Kommunikation – ein Grundpfeiler des Datenschutzes und der Informationssicherheit.

Am 11. Mai 2022 hat die EU Kommission einen Vorschlag für eine Verordnung zur Festlegung von Vorschriften zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern vorgelegt. Der Vorschlag sieht Verpflichtungen für Anbietende von Hosting-Diensten, interpersonellen Kommunikationsdiensten und anderen Diensten vor, die der Aufdeckung, Meldung und Entfernung von Online-Materialien zum sexuellen Missbrauch von Kindern sowie der Verhinderung von gezielter Ansprache von Kindern dienen sollen. Unter anderem soll sogar die verschlüsselte Kommunikation aufgebrochen werden, damit Anbietende solcher Dienste missbräuchliches Material erkennen können. Auch Maßnahmen zur Erkennung von bis dahin unbekannter Kinderpornografie sollen umgesetzt werden, wobei gerade hier die Gefahr besteht, aufgrund des wahrscheinlichkeitsbehafteten Charakters entsprechender Algorithmen unbegründet in Verdacht zu geraten. Dies kann mit einem erheblichen Eingriff in die Grundrechte aller Bürger_innen verbunden sein. Auch der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte (EDSB) haben den Vorschlag der EU Kommission in einer gemeinsamen Stellungnahme vom 28. Juli 2022 daher scharf kritisiert.

Eine anlasslose und umfassende Durchforstung unserer Kommunikation lässt erhebliche Zweifel an der Verhältnismäßigkeit des Vorschlags der EU Kommission zur Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern aufkommen. Die EU Kommission muss stattdessen einen sinnvollen Vorschlag machen, wie der offensichtliche Konflikt mit dem Schutz privater Kommunikation sinnvoll gelöst werden kann.

4.6 Neues von der EU Kommission II: Entwürfe zur KI-Haftung und Cyber-Resilienz

Die EU Kommission hat unter dem 15. September 2022 den Entwurf einer Verordnung zur Cyber-Resilienz und unter dem 28. September 2022 den Entwurf einer Richtlinie zur Anpassung der Vorschriften über die außervertragliche zivilrechtliche Haftung für künstliche Intelligenz vorgelegt. Beide Entwürfe stärken die Rechte und Daten von natürlichen Personen und sorgen für eine Festigung der Informations- und Datensicherheit. Wesentliche Grundsätze wie Security by Design und die Bereitstellung von Sicherheitsupdates sollen für Hersteller_innen und Händler_innen von digitalen Produkten zukünftig verpflichtend werden.

4.6.1 Verordnungsentwurf zur Cyber-Resilienz

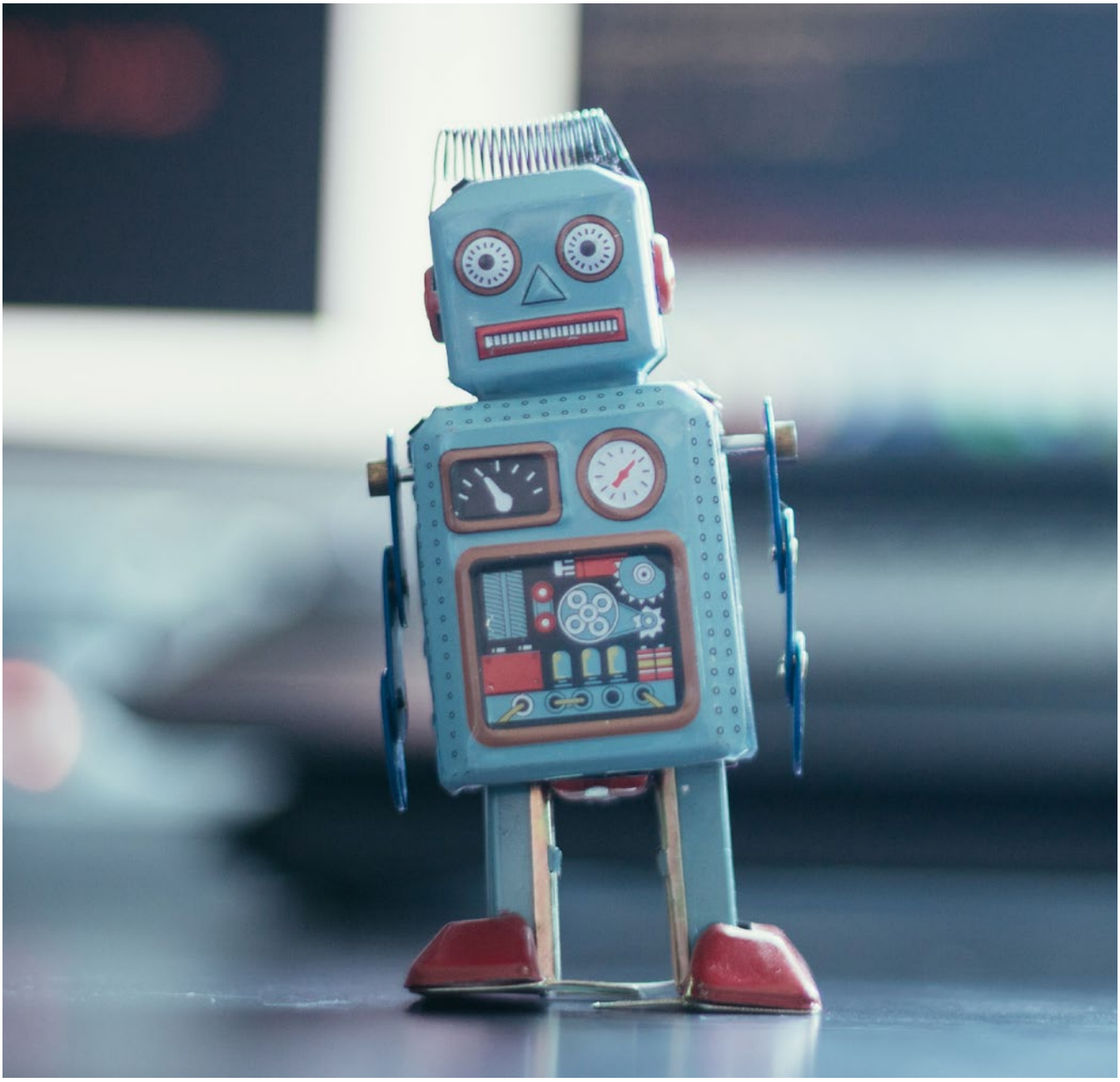
Der Verordnungsentwurf zur Cyber-Resilienz vom 15. September 2022 schließt eine große Regulierungslücke in der Informationssicherheit. Während

☛ Mehr Informationen:

Pressemitteilung der EU Kommission – Fragen und Antworten: Richtlinie über KI-Haftung, zuletzt aufgerufen am 3.11.22: ec.europa.eu/commission/presscorner/detail/de/QANDA_22_5793

bereits die Digitale-Inhalte-Richtlinie Verbraucherverträge zwischen Hersteller_innen und Endverbraucher_innen regelt (über die mit der nationalen Umsetzung u.a. in den §§ 327 ff. BGB), adressiert die Cyber-Resilienz-Verordnung direkt die Hersteller_innen von vernetzten Produkten. Sie gilt für alle vernetzten Produkte mit digitalen Elementen. Das schließt Hard- und Software-Produkte ein und umfasst neben den Hersteller_innen auch Importierende und Händler_innen solcher Produkte. Kernpunkte sind unter anderem, dass Security by Design im gesamten Lebenszyklus eines Produkts, von der Entwicklung bis zur Außerbetriebnahme, umgesetzt werden muss. Aktiv ausgenutzte Schwachstellen und Vorfälle müssen an die zuständige Aufsichtsbehörde gemeldet werden. Die Aufsichtsbehörde übernimmt die Funktion einer Marktüberwachungsbehörde und kann Kontrollen durchführen sowie Sanktionen verhängen. Und last but – very much – not least müssen Hersteller_innen Sicherheitsupdates über einen Zeitraum von fünf Jahren beziehungsweise für die erwartete Lebensdauer des Produkts zur Verfügung stellen.

Auch wenn dies alles mit weiteren Anforderungen und Aufwand für Hersteller_innen und Händler_in-



Wer haftet, wenn durch Künstliche Intelligenz Schaden entsteht? Die EU hat einen Entwurf dazu vorgelegt.

nen digitaler Produkte verbunden ist, so dürfte die bisher fehlende Haftung für Hersteller_innen digitaler Produkte oft als Grund für Vorfälle in der Cybersicherheit und damit auch für Datenpannen sein. Zudem fallen Hersteller_innen und Händler_innen von digitalen Produkten häufig nicht unter den Anwendungsbereich der DS-GVO, da sie nicht für die Verarbeitung personenbezogener Daten ihrer Kundschaft verantwortlich sind. Die in der Cyber-Resilienz-Verordnung vorgesehenen Sanktionen werden bei manchem Hersteller_innen für ein wünschenswertes Umdenken in der Produktsicherheit sorgen. Das Schließen der derzeit bestehenden Regulierungslücken durch den Verordnungsentwurf zur Cyber-Resilienz bedeutet eine große Stärkung der Informationssicherheit – und damit auch des Datenschutzes.

4.6.2 Richtlinien-Entwurf zur KI-Haftung

Der Richtlinien-Entwurf zur KI-Haftung vom 28. September 2022 stärkt die Position von betroffenen Personen in zwei wesentlichen Punkten: Erstens wird es betroffenen Personen erleichtert, einen durch eine KI verursachten Schaden nachzuweisen. Die Richtlinie zur KI-Haftung führt dazu eine „Kausalitätsvermutung" ein. Kann eine betroffene Person nachweisen, dass für einen erlittenen Schaden ein ursächlicher Zusammenhang mit der KI wahrscheinlich ist, können auch die Gerichte davon ausgehen, dass die KI den Schaden verursacht hat. Andererseits kann die haftbare Person oder Institution diese Vermutung widerlegen, muss dazu aber nachweisen, dass der Schaden eine andere Ursache hatte. Durch die Kausalitätsvermutung wird der betroffenen Person die Erlangung eines Schadensersatzes deutlich erleichtert.

Zweitens wird die Richtlinie zur KI-Haftung betroffenen Personen helfen, Zugang zu einschlägigen Beweismitteln zu erhalten. Dazu können betroffene Personen bei Gericht beantragen, die Offenlegung von Informationen über Hochrisiko-KI-Systeme anzuordnen. Damit erhalten betroffene Personen Zugang zu (sensiblen) Informationen, welche für sie ansonsten nicht zugänglich wären, beispielsweise aufgrund von Geschäftsgeheimnissen.

Kritisch ist zu sehen, dass bereits der wahrscheinliche Zusammenhang mit einem von einer KI verursachten Schaden nur schwer nachweisbar sein dürfte. Es wird sich in der Praxis deshalb zeigen müssen, ob hiermit wirklich die wünschenswerte Erleichterung für betroffene Personen einhergeht.

Eine Stärkung der Rechte von natürlichen Personen ist bei dem Ungleichgewicht, das häufig zwischen ihnen und Software- und KI- Hersteller_innen herrscht, von erheblicher Bedeutung. Daher sind die beiden Regelungsentwürfe sehr zu begrüßen, auch wenn sie für Unternehmen und Behörden ein Mehr an Aufwand und Haftungsrisiken bedeuten. Insbesondere die Update-Pflicht für Software Hersteller_innen und Vorgaben für Security by Design sind längst überfällig – sind sie doch das Fundament für Cybersicherheit und Datensicherheit.

4.7 Der Digitale Euro – oder wie sich die EZB monetär digitalisieren will

Bereits im Oktober 2020 hatte die Europäische Zentralbank (EZB) den „Report on a digital Euro" veröffentlicht, ein Papier zur möglichen Umsetzung und Gestaltung einer digitalen Währung im Eurosystem. Ausgangspunkt der Betrachtung war dabei der signifikante Rückgang der Akzeptanz von Bargeld als Zahlungsmittel. Ein digitaler Euro wäre eine Banknote in digitaler Form. Er soll das Bargeld nicht ersetzen, wie man vielleicht meinen könnte, sondern als weitere Bezahlmöglichkeit zur Auswahl stehen. Er würde als digitales Geld von der EZB und den nationalen Zentralbanken des Euroraums ausgegeben und könnte von Privatpersonen und Unternehmen als digitales Zahlungsmittel genutzt werden, soll aber nicht als Geldanlage dienen. Wichtige Prämisse war dabei, das Vertrauen in die digitale Währung sowohl bei der Einführung als auch über Zeit zu gewährleisten. Die öffentliche Konsultation zu den Wünschen und Anforderungen an den digitalen Euro lief vom 12. Oktober 2020 biszum 12. Januar 2021: Mehr als 8.200 Rückmeldungen von Bürger_innen und Unternehmen gingen ein – Rekord für ein öffentliches Konsultationsverfahren!

☛ Mehr Informationen:

Zeitplan der EZB zum Digitalen Euro, siehe Übersicht auf Seite 2:
www.ecb.europa.eu/paym/digital_euro/investigation/governance/shared/files/ecb.degov220929.en.pdf

Die Ergebnisse in Kürze: 94% der Rückmeldungen kamen von Privatpersonen. Die meisten Antworten aus Deutschland (47%), Italien (15%) und Frankreich (11%). Die zentralen Forderungen waren Datenschutz (43%), Sicherheit (18%), Zahlungsmöglichkeit innerhalb von ganz Europa (11%), keine zusätzlichen Kosten (9%) und Offline-Nutzbarkeit (8%).

Der EDSA und die Financial Matters Subgroup (FM ESG) waren von Anfang an in die datenschutzrechtlichen Fragestellungen eingebunden und die EZB berichtet seither regelmäßig in den Subgroup-Sitzungen. Die EZB muss sich beispielsweise Fragen des materiell-rechtlichen Geltungsbereich, der Datenminimierung, des Zugangs zur Plattform und deren Interoperabiltität, der Anonymisierung und zu privacy by design stellen.

Soweit so gut. Dass die Digitalisierung von Bargeld alles andere als einfach ist, lässt sich schnell feststellen, wenn man sich die vielen unterschiedlichen Bezahlsysteme allein auf Bankenebene und innerhalb der Länder einmal anschaut. Und das hat auch die EZB in ihrer neuesten Studie festgestellt und kündigt weitere Untersuchungen an.

Noch ist die Einführung des digitalen Euros keine beschlossene Sache, das Vorhaben wird bis Oktober 2023 intensiv unter Einbeziehung von relevanten Stakeholdern geprüft. Erst dann wollen die Europäische Kommission und die EZB entscheiden. Laut Zeitplan der EZB sollen bis Ende 2022 die Fragen zu Online-/offline-Verfügbarkeit, Datenschutzgarantien und Transfermechanismus gelöst sein.

In der jüngsten Stellungnahme setzte sich der EDSA deshalb kritisch mit den Plänen der EZB auseinander, eine Online-Variante unter Einschaltung eines Dienstleisters (Intermediär) zu favorisieren. Der EDSA bevorzugt nach wir vor eine Variante, die einer Cash-Lösung, und damit dem ursprünglichen Zweck der digitalen Euros, nähersteht und damit datenschutzfreundlicher gestaltet werden kann. Besonders in Bezug auf die Einführung eines E-Commerce-Prototypen empfiehlt der EDSA, sicherzustellen, dass dieser vollumfänglich mit der „Schrems II"-Entscheidung des EuGH sowie anderen Datenschutzgesetzen in Einklang steht. Der EDSA hat angekündigt, weiterhin an den Themen dranzubleiben.

4.8 Sie sind da: Unsere Datenschutz-Icons!

Wer personenbezogene Daten verarbeitet, muss immer auch erklären, wofür und auf welcher Rechtsgrundlage dies geschieht und wer für die Verarbeitung verantwortlich ist. Datenschutzhinweise sind aber häufig lang, oftmals schwer verständlich und auch unübersichtlich. Nutzer_innen, die diese Erklärungen lesen, verlieren nicht selten dabei am Ende den Überblick.

Bereits im Tätigkeitsbericht des letzten Jahres berichteten wir von unserem Wettbewerb „Icons entwerfen und Datenschutz mitgestalten". Von Juli bis September 2021 waren alle Kreativen aufgefordert, beim Wettbewerb „Datenschutz-Icons" mitzumachen und Vorschläge einzureichen. Ziel war es, die Datenschutzinformationen mithilfe von Icons, Symbolen oder anderen grafischen Elementen einfacher, klarer und intuitiv verständlich zu machen. Denn nur wer versteht, worum es geht, kann seine Rechte informiert ausüben und beispielsweise die Einwilligung in den Newsletterversand widerrufen, Betroffenenrechte geltend machen oder Privatsphäreneinstellungen am Browser vornehmen.

An dem Wettbewerb nahmen sowohl Profis der Grafikgestaltung als auch Laien teil. Nachdem die Gewinner_innen des Wettbewerbs prämiert wurden, ging es anschließend noch an die grafische Überarbeitung und Vereinheitlichung der Datenschutz-Icons. Die fertigen Icons wurden bereits auf der diesjährigen BvD-Herbstkonferenz in Stuttgart einem breiten Fachpublikum vorgestellt.

Nun sind sie also da, unsere Datenschutz-Icons! Und sie stehen ab sofort auf unserer Homepage zum Download bereit. Unsere Hoffnung ist, dass sich solche Icons etablieren. Sie können den Menschen nützen, sich im Informationsdschungel besser zurechtzufinden. Hierzu werden sie auch dem Europäischen Datenschutzausschuss präsentiert werden, um eine möglichst breite Verwendung in Europa zu erreichen.

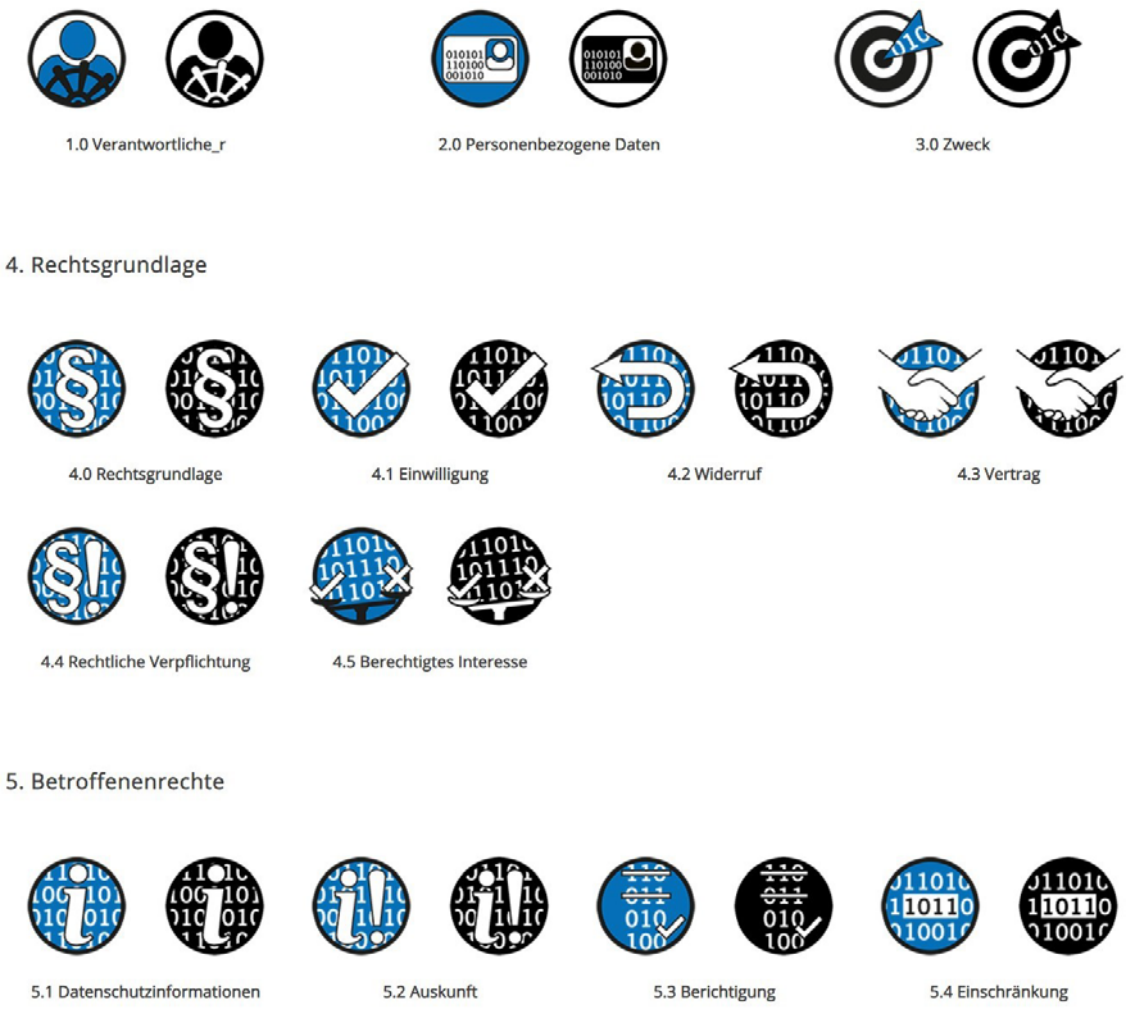
☛ Mehr Informationen:

Die Datenschutz-Icons stehen auf unser Homepage zum Download bereit: www.baden-wuerttemberg.datenschutz.de/datenschutz-icons

Die vielen Einreichungen zu unserem Wettbewerb und die positive Resonanz auf die Veröffentlichung unserer Icons senden ein tolles Signal: Die Bereitschaft, Datenschutz mitzugestalten ist groß! Weitere Wettbewerbe dieser Art sind in Planung und tragen hoffentlich dazu bei, dass immer mehr Menschen wissen: Hier geht's lang in Sachen Datenschutz!

4.9 Schulungen der Stabsstelle Deutsche und Europäische Zusammenarbeit

Zur fortlaufenden Fortbildung des Hauses hat die Stabsstelle Deutsche und Europäische Zusammenarbeit auch im Jahr 2022 wieder stetig Inhouse-Schulungen für alle Mitarbeitenden angeboten, die u.a. aufgrund der Pandemiesituation weiterhin im Online-Format veranstaltet wurden. Die insgesamt 24 Schulungen gaben den Beschäftigten Einblicke in die aktuelle Arbeit der verschiedenen Abteilungen des LfDI und erfreuten sich eines großen Interesses in der Dienststelle, glücklicherweise auch bei vielen der neu hinzugekommenen Beschäftigten. Daneben halten die Referent_innen der Stabsstelle Deutsche und Europäische Zusammenarbeit regelmäßig Vorträge im Rahmen des Programms des Bildungszentrums BIDIB, beispielsweise zu unserem Tool „DS-GVO.clever" und weiteren aktuellen Themen. Es freut uns, dass die Schulungen im BIDIB mittlerweile häufig auch im hybriden Format möglich sind und einen direkten Austausch mit den Teilnehmenden ermöglichen. Das von der Stabsstelle entworfene Format der Online-Schulungen soll auch erweitert werden, um in Zukunft noch mehr datenschutzinteressierte Personen unterstützen und begeistern zu können.



Mit Icons können Datenschutzhinweise leicht verständlich und übersichtlich gestaltet werden.

5. Bildungszentrum

Das Veranstaltungsangebot des Bildungszentrums Datenschutz und Informationsfreiheit Baden-Württemberg (BIDIB) wird vielfältiger und erfreut sich nachhaltig großer Beliebtheit. Das Angebot konnte im Jahr 2022 weiter ausgebaut und diversifiziert werden. Die Nachfrage nach unseren Veranstaltungen ist groß, neue Bildungsangebote werden tendenziell sehr gut angenommen. Insgesamt konnten alles im allem rund 120 Veranstaltungen durchgeführt werden, zu denen es über 3.200 Anmeldungen gab. Die deutliche Erhöhung sowohl bei den durchgeführten Veranstaltungen als auch bei den Anmeldungen im Vergleich zum Vorjahr ist insbesondere auf das Projekt Schule digital zurückzuführen, das auf breites Interesse stößt.

Im Gegensatz zum Vorjahr wurden vermehrt Veranstaltungen mit Teilnahmemöglichkeiten vor Ort im Bildungszentrum angeboten (sowohl hybride als auch reine Präsenz-Veranstaltungen), soweit die Pandemie-Lage dies zuließ. Viele Interessierte freuten sich über diese Möglichkeit. Es gab jedoch auch Stimmen, die sich bei reinen Präsenz-Veranstaltungen nach digitalen Teilnahmemöglichkeiten erkundigten. Dies dürfte zum einem an Corona liegen, aber auch an den für die Interessierten anfallenden Wegezeiten bei Präsenz-Teilnahmen. Deshalb werden wir versuchen, unser hybrides Angebot mit der Möglichkeit, wahlweise vor Ort in Präsenz oder Online teilzunehmen, weiter auszubauen.

5.1 Erfolgreiches Programm 2022

Für die interessierte Öffentlichkeit haben wir die Reihe „Digitale Selbstverteidigung“ etabliert. In loser Folge bieten wir hier Veranstaltungen an, die aufzeigen, wie es möglich ist, datensparsam in der digitalen Welt unterwegs zu sein sowie Gefahren und Risiken für die eigenen Daten zu reduzieren. 2022 organisierten wir drei Veranstaltungen: „Eine Reise durch den Messenger-Dschungel“, „Horch! Was kommt von drinnen raus? Über die Kommunikationsfreudigkeit mobiler Endgeräte“ jeweils mit einem Referenten aus unserem Haus sowie „Digital souverän bleiben, aber wie?“ mit dem bekannten und renommierten IT-Sicherheitsexperten Manuel Atug, im Internet auch unter dem Namen „HonkHase“ bekannt. Die Reihe setzen wir im Jahr 2023 fort.

Für klein- und mittelständische Unternehmen haben wir unter anderem eine vierteilige Veranstaltungsreihe „Datenschutz durch Technikgestaltung“ in Präsenz angeboten, die rasch ausgebucht war. Die Veranstaltungsreihe vermittelte einen grundlegenden Überblick über datenschutzrechtliche Anforderungen bei der Technikgestaltung. Inhaltlich wurde schrittweise auf den risikobasierten Ansatz der DS-GVO und die maßgeblichen Erwägungen hierzu eingegangen, die eine verantwortliche Stelle beziehungsweise der Hersteller von Produkten treffen sollte. Aufgrund der großen Nachfrage planen wir für das Jahr 2023 Wiederholungsveranstaltungen.

Es gab für Unternehmen eine Veranstaltung zum Themenfeld „IT-Sicherheitsmanagement“. Dieses Thema gewinnt immer mehr an Bedeutung. Die Veranstaltung stand auch der Landes- und Kommunalverwaltung offen. Alleine an diesem hybrid ausgestalteten Vortrag haben über 100 Personen teilgenommen.

Der Themenbereich Videoüberwachung ist ein Dauerbrenner mit fortlaufend großer Nachfrage von verantwortlichen Stellen. Vor diesem Hintergrund haben wir spezielle Veranstaltungen für Gewerbeämter und Polizeibehörden („Videoüberwachung durch nicht öffentliche Stellen“) sowie für Schul- und Kommunalverwaltungen („Videoüberwachung an Schulen durch Kommunen“) durchgeführt.

Fortbildungsangebot Schule digital

Um den Datenschutz an den Schulen zu stärken, hat uns der Landtag Ende 2021 dankenswerterweise für die Zeit bis Ende 2024 weitere Stellen bewilligt, um Schulungen für Lehrkräfte, Schulleitungen, Datenschutzbeauftragte, Eltern und Schülervertretungen anzubieten. Leider gestaltete sich die Besetzung der zeitlich begrenzten Stellen sehr schwierig, sodass wir bis Ende 2022 noch nicht alle besetzen konnten. Trotzdem nahmen 2022 an 60 Veranstaltungen fast 1200 Interessierte an unseren Fortbildungen teil.

In der Zwischenzeit steht eine Kooperation mit dem Zentrum für Schulentwicklung und Lehrerbildung des Landes Baden-Württemberg (ZSL) und dem Kultusministerium Baden-Württemberg kurz vor dem Abschluss. In dieser Kooperation ist geplant, dass wir unsere datenschutzrechtlichen Kompetenzen in die Lehrerfortbildungen des ZSL zum Datenschutz einbringen. Dadurch können wir noch stärker in der Fläche an den Schulen wirken und Schulleitungen, Lehrkräfte oder für den Datenschutz an Schulen Zuständige noch besser erreichen.

© ake1150 - stock.adobe.com

„Schule digital" war ein voller Erfolg.

Neben dieser Kooperation bieten wir aber auch Fortbildungen für weitere Gruppen im Schulumfeld an. So sind bereits Fortbildungen für Mitarbeitende in den Schulsekretariaten, für Kindertagesstätten oder für Schüler_innen an den Schulen erfolgt. Die Fortbildungen für Schüler_innen erfolgen in Kooperation mit „Datenschutz geht zur Schule" des Bundesverbands der Datenschutzbeauftragten Deutschland e.V. (BvD). Hierzu gehen Mitarbeiter des Landesbeauftragten direkt an den Schulen in die Klassen um sie beispielsweise für einen sichereren Umgang in den sozialen Netzwerken zu sensibilisieren.

Ende des Jahres 2022 erfolgten außerdem die ersten Fortbildungen zum Datenschutz für Elternvertretungen. Veranstaltungen für weitere Zielgruppen, beispielsweise für IT-Verantwortliche an Schulen oder für Verantwortliche für Schulen bei den Kommunen, sind darüber hinaus geplant.

☛ Mehr Informationen:

Das aktuelle Programm zu „Schule digital" steht hier: www.baden-wuerttemberg.datenschutz.de/bidib-schule-digital

Datenschutz geht zur Schule: www.bvdnet.de/datenschutz-geht-zur-schule

Medienbereich

Der Medienbereich des Bildungszentrums beschäftigt sich seit dessen Gründung mit der Konzeption, Entwicklung und Umsetzung digitaler Bildungsformate und unterstützt dabei unsere gesamte Dienststelle. Dies schließt die Begleitung von Veranstaltungen in medientechnischer Hinsicht ein. So haben wir erstmals bei der KI-Woche im Juli die Veranstaltungen allesamt live auf PeerTube gestreamt. Die Geräteausstattung im Bereich Medientechnik konnte im Jahr 2022 ergänzt werden, so dass nunmehr die Beschaffung der technischen Grundausstattung abgeschlossen ist.

Das Spektrum der Medienproduktion für unsere Dienststelle reicht von Erklärvideos über Podcasts bis hin zu Hörspielen. Die Videos und Audios sind auf unserer Homepage zu finden, zugleich nutzen wir immer intensiver die Videoplattform PeerTube.

Wir erreichen mit unseren Medienproduktionen Bürger_innen und verantwortliche Stellen gleichermaßen und wollen unser Wissen, welches hier im

Haus vorhanden ist, so einfach, direkt und ansprechend wie möglich zur Verfügung stellen.

5.2 Bildungsportal

Um unser Angebot weiter zu optimieren, arbeiten wir seit Herbst 2022 am Aufbau eines Bildungsportals. Bereits in der Vergangenheit haben wir Beiträge zu verschiedenen Themen, die Datenschutz und Informationsfreiheit betreffen, in unterschiedlichen Formaten online zur Verfügung gestellt. Die Resonanz hierzu war sehr positiv. Deshalb bauen wir dieses Angebot weiter aus.

Das künftige Bildungsportal soll das Angebot des Bildungszentrums einfach, klar strukturiert und nach verschiedenen Detailierungsgraden abgestuft an einer Stelle in unserem Internetauftritt vereinen. Interessierte und Suchende werden künftig im Bildungsportal durch einzelne Themenbereiche geführt und können selbst entscheiden, wie vertieft sie sich mit einem Thema befassen wollen. Jeder Themenbereich soll ein Einführungsvideo bekommen, auf das dann, sofern angebracht, Vertiefungsvideos folgen und mit Handreichungen, weiteren Veröffentlichungen und FAQs verknüpft werden.

Auf dem Bildungsportal wollen wir künftig umfassend ein Angebot bereithalten, das unabhängig von einzelnen Veranstaltungen genutzt werden kann – die Interessierten entscheiden selbst, wann und von wo aus sie sich informieren wollen. Unser Beratungsangebot wird so um eine entscheidende Facette erweitert.

Der Aufbau des Bildungsportals ist ein längerfristiges Projekt. Eine erste Version wollen wir möglichst noch im Laufe des Jahrs 2023 online stellen.

Bildungszentrum für Datenschutz und Informationsfreiheit (BIDIB)

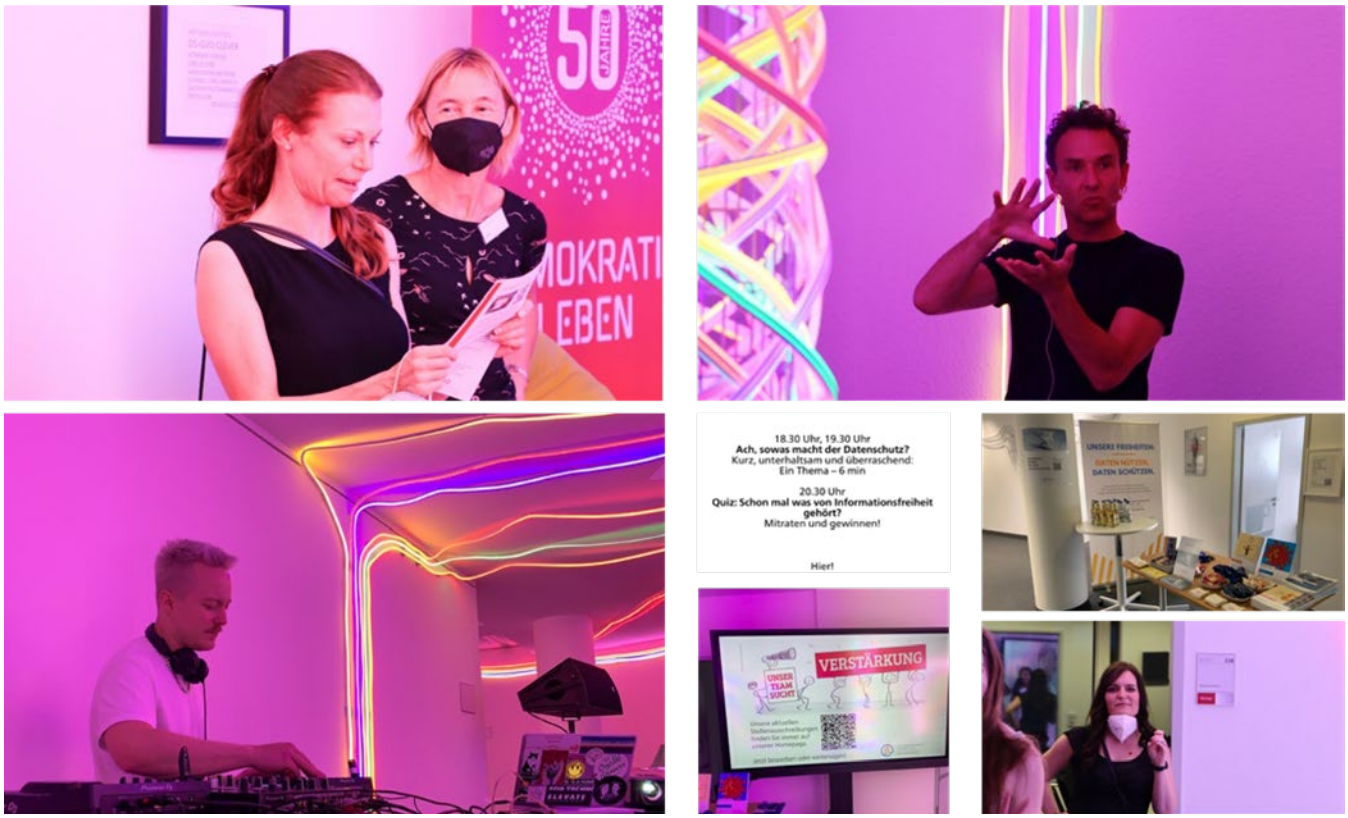
Scannen Sie den QR-Code und informieren Sie sich
über unser aktuelles Angebot im Bildungszentrum!

6. Veranstaltungen

6.1 Die Lange Nacht der Museen (und des LfDI BW) am 21. Mai 2022

Eine unserer Kernaufgaben ist es, Bürger_innen zu ermächtigen, ihre informationelle Selbstbestimmung in einer digitalisierten Gesellschaft selbst in die Hand nehmen zu können. Eine Herausforderung hierbei ist jedoch, dass viele Menschen keinen Zugang zum Datenschutz finden oder diesen womöglich gar als lästige Auflage empfinden. Einem Großteil der Bürger_innen ist nicht bekannt, dass die informationelle Selbstbestimmung ein Bürgerrecht ist, das ihre individuelle Autonomie stärkt – und wie stark Fragen des Datenschutzes durch die Nutzung vernetzter Technologien auch Fragen danach sind, wie man ganz persönlich in der digitalen Gesellschaft leben will. Daher gehen wir schon seit vielen Jahren unter dem Stichwort „Datenschutz als Kulturaufgabe“ neue Wege, um Bürger_innen zu erreichen und ihnen die Bedeutung des Datenschutzes für sie ganz persönlich nahezubringen – auf neue und kreative Art und Weise.

Die vielseitig beachtete Lichtkunst in unseren Räumlichkeiten, das Werk „Data to Light“ des Künstlers Florian Mehnert, diente in diesem Jahr als Türöffner, um für den Datenschutz auch Menschen zu sensibilisieren, die sich noch gar nicht mit diesem Thema befasst hatten und häufig auch nicht wussten, was wir überhaupt machen. Flankiert von einem facettenreichen Programm an Datenschutz-Kurzvorträgen, Quizrunden, Datenschutz-Give-aways und Einführungen in das Werk „Data to Light“ durch Florian Mehnert selbst konnte die begehbare Lichtinstallation begleitet von elektronischer Musik an dem Abend über 3.000 Besucher_innen in die Landesbehörde



Oben links: Kollegin Sabine Grullini und Sabine Keitel (Landeszentrale für politische Bildung) stellen gemeinsame Projekte vor; oben rechts: Künstler Florian Mehnert spricht über seine Lichtinstallation „Data to Light“; unten links: DJ Sample Samurai sorgt für passende Musik, unten Mitte: Programmhinweise für Impulsvorträge und Hinweis zu unseren Stellenausschreibungen; unten rechts: Tätigkeitsberichte, Veranstaltungshinweise und Give-Aways sowie unsere Kollegin Clarissa Henning, die bei der Langen Nacht alles im Griff hat.

locken. Warteschlangen vor dem Eingang – das war für uns tatsächlich eine neue Erfahrung. Die eigens von Florian Mehnert für den Abend zusätzlich konzipierte Projektion, die Datenspuren auf die Außenwand unseres Gebäudes warf, machte den Datenschutz weiträumig sichtbar. Dies war nur durch das großzügige Entgegenkommen des Ministeriums für Kultus, Jugend und Sport Baden-Württemberg möglich, die ihre Räumlichkeiten für das Projektionsgerät zur Verfügung stellten. An dieser Stelle sei hierfür noch einmal herzlich gedankt.

Als einen besonderen Erfolg der Veranstaltung sehen wir es an, dass wir eine Altersgruppe ansprechen konnten, von der man vielfach sagt, wir alle redeten über sie, aber nicht mit ihnen: die sogenannten Twens. Datenschutz als erfahrbares Bürgerrecht – dieser Abend hat hierzu beigetragen.

Unser Projektteam hat tolle Arbeit geleistet. Bitte vormerken – am 25. März 2023 sind wir wieder mit einem vielfältigen Programm bei der Langen Nacht der Museen dabei.

6.2 BvD-Herbstkonferenz und Behördentag 2022

Vom 26. bis 28.10.2022 fand zum sechsten Mal die jährliche Datenschutzkonferenz des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V. zum Thema „DSGVO im 5. Jahr: Wie hat Europa den Datenschutz verändert?“ statt, die regelmäßig neben dem LfDI BW in Kooperation mit dem Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) und dem Bayerischen Beauftragten für den Datenschutz (Bay LfD) durchgeführt wird. Gastgeber war in diesem Jahr der LfDI BW und durfte zirka 230 Konferenzteilnehmer_innen aus ganz Deutschland im Steigenberger Hotel Graf Zeppelin in Stuttgart begrüßen. Schon am Vorabend luden wir die Konferenzteilnehmenden in die Räumlichkeiten des LfDI ein, um die Landesbehörde sowie die Fachabteilungen kennenzulernen. Diese Einladung fand großen Anklang. Die Möglichkeit, mit der Aufsichtsbehörde „face-to-face“ in Kontakt kommen zu können und einen Einblick in die Aufsichtspraxis zu erhalten, stieß auf sehr positiven Zuspruch.

Fachlicher Input und Austausch: Die BvD-Herbstkonferenz und der Behördentag fand in Stuttgart statt. Der Leitende Beamte Jan Wacke vertrat den LfDI in diesem Jahr. Das Team des LfDI lieferte dem Fachpublikum aus Behörden und Unternehmen datenschutzrechlichen Input und diskutierte mit ihnen. Auf dem Bild v.l.n.r.: Clarissa Henning, Frank Feucht, Walter Kicherer, Johanna Krieger, Jan Wacke, Peter Nägele, Thuy Nga Thrin, Alvar Feude, Kristof Meding.

Die Konferenz selbst wurde am folgenden Tag mit einer Keynote von Renate Nikolay (Kabinettschefin, EU-Kommission) eröffnet, die den Teilnehmer_innen einen Blick auf wichtige europäische Gesetzgebungsprozesse wie den Data Act oder die E-Privacy-Verordnung gewährte und offene Fragen ausräumte. Neben Themen wie Whistleblowing und Drittstaatentransfer widmeten sich weitere Vorträge auch dem Themenkomplex Cybersicherheit, unter anderem ein Vortrag von Ralf Rosanowski, Präsidenten Cybersicherheitsagentur BW. Ein besonderer Schwerpunkt der Konferenz lag dieses Mal auf der Gesundheitsdatennutzung und -forschung. Hierzu berichtete unter anderem Professor Kindervater (BIOPRO) über das Forum Gesundheitsstandort BW und diskutierte mit weiteren Referent_innen, Unternehmensvertreter_innen und Behördenvertreter_innen über die datenschutzrechtlichen Herausforderungen bei der Datennutzung von Gesundheitstechnologien.

Der letzte Tag der Veranstaltung ist traditionellerweise speziell auf behördliche Datenschutzthemen ausgerichtet – so auch in diesem Jahr. Ein dezidierter Blick wurde auf die kommenden Herausforderungen und Chancen durch den Einsatz von Künstlicher Intelligenz (KI) im behördlichen Arbeitsalltag geworfen, z. B. im Kontext der in Abstimmung befindlichen EU-KI-Verordnung oder bezüglich Betroffenenrechten. Von besonderem Interesse für die Teilnehmer_innen war auch die Frage nach möglichen Schadenersatzforderungen nach Art. 82 DSGVO gegenüber Behörden.

Ein Highlight, sowohl für behördliche wie auch Unternehmens-Datenschutzbeauftragte, stellt jedes Jahr die Möglichkeit dar, in einem eigens dafür vorgesehenen Slot, Fragen an die Leiter der Aufsichtsbehörden stellen zu können – was auch in diesem Jahr rege genutzt wurde.

6.3 KI-Themenwoche

Die KI-Woche vom 7. bis zum 14 Juli bot schließlich gebündeltes Wissen für Fachleute und Laien, die sich mit dem Thema der Künstlichen Intelligenz befassen wollten. Hierzu verweisen wir auf die ausführliche Darstellung in Kapitel 1.5.

Lange Nacht der Museen: Der LfDI ist hier – unser Logo strahlt vom Gebäude des Kultusministeriums auf das Gebäude, wo wir unsere Büros haben.

7. Datenschutz als Kulturaufgabe – Kulturtechniken des Digitalen

Der Umgang mit den eigenen persönlichen Daten im Digitalzeitalter ist eine verhältnismäßig junge Kulturtechnik. Sie hat sich deutlich langsamer als die ökonomische Technik der Verwertung von personenbezogenen Daten entwickelt. Je weiter die Digitalisierung voranschreitet – und infolge der Coronapandemie hat sie in vielen Lebens-, Arbeits- und Gesellschaftsbereichen einen enormen Schub bekommen – umso stärker hat sich der Datenschutz genau auf diesem Gebiet zu bewähren; er verändert wie die Gesellschaft insgesamt rasant sein Gesicht.

Gleichzeitig leben wir in einer stark durchästhetisierten Gesellschaft. Die Möglichkeiten, sich in digitalen Medien zu inszenieren, sind enorm und werden virtuos genutzt – und sie gehorchen ästhetischen Regeln. Jede_r Einzelne kann Erzählungen von sich, kann Bildstrecken und Videos mit hoher Reichweite veröffentlichen. Die Strategien dazu sind an künstlerisch-narrativen Techniken orientiert – doch oft ohne um diese Techniken, ihre Potenziale, Regeln und Risiken gewusst wird. Auch hier setzen Kulturtechniken des Digitalen an: Gibt es im übertragenen Sinn „Grammatiken" für die neuen Kommunikationsformen, mit denen sich jede_r, die oder der sie selbstbestimmt nutzen möchte, beschäftigen sollte – sei es als Datenkonsument oder Produzent?

Ein weiterer Gedanke gilt einem merkwürdigen Paradox. Einerseits scheinen wir in einer Gegenwart zu leben, die auf den ersten Blick stark an Sachlichkeit und technischen Paradigmen orientiert ist: in einer Wissensgesellschaft, in der Informationen und Informationsverarbeitung zählen. Auf der anderen Seite sind aber Informationen, news, sehr stark in einer narrativen und ästhetisierten Form aufbereitet, sie sollen – Stichwort Aufmerksamkeitsökonomie – Emotionen ansprechen und so zu einem bestimmten Netzverhalten animieren. Digitale Logiken sind für diesen Trend zum Treiber geworden. Wie das handwerklich genau gemacht wird, dafür sind wiederum Künstler_innen und Kulturschaffende Spezialisten und gute Ratgeber – um Dinge einzuordnen, und um die Strategien, wie sie hergestellt werden, zu verstehen: Was genau steckt drin an gestalterischem und dramaturgischen know-how in den timelines von Social Media und Co.?

Kunst und Kultur können Praktiken vermitteln, mithilfe derer wir uns als Gesellschaft mit den neuen Formen digitaler Wirklichkeitsherstellung selbstbewusst, aufgeklärt und selbstbestimmt erproben können.

Wenn Kunst der Ort ist, an welchem sich Gesellschaften mit sich selbst beschäftigen, Grundlagen der „harten Fakten" auf den Prüfstand stellen und Zukunftsentwürfe einmal „folgenlos" durchspielen, so bringen uns Kunst und Kultur zum scheinbar Selbstverständlichen und Unhinterfragbaren produktiv auf Distanz und lassen unseren Möglichkeitssinn tanzen. Und das gilt besonders angesichts der oft als alternativlos wirkenden Wirklichkeiten des Digitalen.

Wer aber hat überhaupt Zugang zu den neuen Kommunikations- und Informationsmöglichkeiten des Digitalen, und zu welchem Preis? Was in privaten gesellschaftlichen und privatwirtschaftlichen Initiativen frei, offen und bunt spätestens ab Mitte der 70er Jahre in den berühmten Garagen-Start-ups seinen Ausgang genommen hat, ist längst zu einer Art zweitem öffentlichen Raum von globaler Reichweite geworden. Über die Zugangsregeln zu diesem Raum bestimmen allerdings – nachdem auf die Phase des freien Experimentierens rasch ein starker Ökonomisierungs- und Monopolisierungsprozess gefolgt war – einige wenige Tech-Firmen. Die Spielregeln auf dem Marktplatz der Meinungen, Debatten und Informationen, um eigene Sichtbarkeit herzustellen, sich zu vernetzen und nicht zuletzt ziemlich weltumspannend zu kommunizieren, unterstehen kurzum den AGBs dieser Player. Meistens, und hier wird es für den Datenschutz interessant, „bezahlen" wir den Zutritt zur Infrastruktur der besuchten Plattformen mit unseren eigenen Daten, und teilweise auch mit den Daten unseres „Netzwerkes". Ein öffentlicher Raum sollte, so wiederum die Überzeugung vieler und immer lauter werdender Stimmen, von denen, die ihn benutzen, auch in seinem Regelwerk mitgestaltet werden. Hier wird ein Spannungsverhältnis sichtbar.

Die Frage, wie wir unsere digitale Zukunft gestalten, sollte gesellschaftlich beantwortet werden, wenn es eine nachhaltige Antwort sein will, bei der Digitalisierung und Bürgerrechte miteinander verbunden sind. Wir Bürger_innen können uns dieser Zukunft aktiv widmen: Welche Möglichkeiten und Freiräume wünschen und erstreiten wir uns – und unter welchen Spielregeln? Wie lässt sich unser Bedürfnis nach Freiheit und Sicherheit so ausbalancieren, dass Bürgerrechte gewahrt bleiben? Und wie lernen die Jüngsten, für die eine Trennung von analog und digital längst obsolet scheint, mit den medialen Mechaniken nicht nur technisch versiert, sondern selbst-bestimmt und mit Abstandsvermögen umzugehen?

Künstliche Intelligenz: Maßgebliche Entwicklungen im Blick

Wir arbeiten an Fragen zum Digitalen, zur Informationsgesellschaft und zu den gesellschaftlichen Herausforderungen, so wie es Artikel 57 der DS-GVO von uns erwartet. Wir informieren die Öffentlichkeit, sensibilisieren und klären auf. Wir verfolgen maßgebliche Entwicklungen, soweit sie sich auf den Schutz personenbezogener Daten auswirken.

Vom 7. bis zum 14. Juli fand in den Räumen unserer Behörde inmitten der Kunstinstallation von Florian Mehnert und entwickelt aus den Abteilungen der Behörde heraus und vom Kulturbereich unterstützt die bereits erwähnte Veranstaltungsreihe zur Künstlichen Intelligenz (KI) statt: KI und Datenschutz: Was heißt hier Selbstbestimmung? Eingeladen waren Vortragende sowohl mit anwendungsbezogener, eher technischer Perspektive – mit den denkbaren Implikationen, welche diese für die rechtliche Seite des Datenschutzes hat – als auch vor einem abstrakteren philosophischen Hintergrund.

Neben Impulsvorträgen standen Diskussionsformate mit Akteur_innen aus Wissenschaft, Wirtschaft, Verwaltung, Kultur und Politik. Neben der Information der Öffentlichkeit über bereits verfügbare und zukünftig mögliche Anwendungsfelder für KI ging es um die Vernetzung der Beteiligten untereinander, aber auch darum, unsere eigene Rolle als konstruktiver Akteurin und kritischer Begleiterin bei der Entwicklung und Anwendung von KI zu definieren.

Der Bereich Datenschutz als Kulturaufgabe hat sich bei der Programmgestaltung mit einer allgemeiner gehaltenen kulturgeschichtlichen, technikphilosophischen und gesellschaftlichen Perspektive auf das Thema eingebracht (siehe dazu auch Kapitel 1). Dieses Themenfeld wird uns sicher noch intensiv beschäftigen.

☛ Mehr Informationen:

Zu den Aufgaben einer Aufsichtsbehörde gehört es nach Artikel 57 der DS-GVO (dsgvo-gesetz.de/art-57-dsgvo) unter anderem, die Einhaltung der gesetzlichen Regelungen zum Datenschutz zu überwachen und durchzusetzen, eingehende Beschwerden zu bearbeiten. Gleichzeitig gehört dazu auch, die Öffentlichkeit zu beraten, zu informieren, zu sensibilisieren und aufzuklären. Der Gesetzgeber fordert hierfür außerdem spezifische Maßnahmen für Kinder.

Hieraus leitet sich für uns auch der Auftrag ab, Datenschutz als Kulturaufgabe zu verstehen: Wir sensibilisieren und klären auf, entwickeln spezifische Programme für Kinder und Jugendliche und arbeiten dabei auch mit Methoden der Kunst und der kulturellen Bildung.Ein weiteres wichtiges Thema, das der Gesetzgeber den Aufsichtsbehörden im Artikel 57 aufgetragen hat: „maßgebliche Entwicklungen verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken." Genau hier haken wir ein, wenn wir uns diskursiv mit den gesellschaftlichen Fragestellungen auseinandersetzen, die durch die Digitalisierung oder durch die Verbreitung intelligenter künstlicher Systeme die gegenwärtigen und zukünftigen Lebenswirklichkeiten sehr prägend bestimmen, mit dem Ziel, uns als Gesellschaft darüber aufzuklären, was sich daraus für den Schutz personenbezogener Daten und damit für unsere Bürgerrechte im digitalen Zeitalter ergibt.

Netzausbau

Weiter arbeitet der Bereich Datenschutz als Kulturaufgabe an der Schnittstelle Kunst/Technik/Wissenschaft/Gesellschaft am Ausbau eines Kulturnetzwerkes mit dem Ziel, die Themen der Behörde im Kultur- und Wissenschaftsdiskurs weiter zu verankern und umgekehrt Einflüsse aus diesen Diskursen für die Vermittlungsarbeit der Dienststelle fruchtbar zu machen, beispielsweise durch die Konzeption und Planung gemeinsamer Veranstaltungen. Hier soll an der guten Zusammenarbeit während der KI-Woche angeknüpft werden mit Partnern wie dem ITAS/KIT oder der Uni Tübingen.

Anlässlich der Zweiten Stuttgarter Zukunftsrede am 18. Januar 2023 hat sich unsere Dienststelle auch mit dem Literaturhaus Stuttgart und dem Zentrum für Kultur und Technikforschung der Uni Stuttgart verknüpft.

Voller Erfolg: Die Lange Nacht der Museen

Nach der erfolgreichen Teilnahme unserer Behörde an der Langen Nacht der Museen 2022 (siehe ausführlich Kapitel 6) planen wir nunmehr die Fortsetzung im Jahr 2023: Für die nächste Lange Nacht der Museen am 25. März 2023 programmieren wir aktuell die speziell für die Veranstaltung konzipierte Leseperformance „Art of Being … Observed" – Überwachungsphantasien quer durch die jüngere Literaturgeschichte – mit zwei Autoren aus der freien Szene Freiburgs und nehmen so auch Kooperationen landesweit auf. Wieder dabei sein werden Künstler Florian Mehnert, dessen Lichtinstallation zu sehen sein wird, sowie die Malerin Christiane Schauder, deren Bilder in unseren Räumen hängen.

☛ Mehr Informationen:

2. Stuttgarter Zukunftsrede: www.literaturhaus-stuttgart.de/reihe/stuttgarter-zukunftsrede-179.html

Gesprächsreihe „B. sucht Freiheit":
tube.xn--baw-joa.social/c/lfdi_bsuchtfreiheit/videos?s=1

Für junge Menschen: Portal „Young Data"

Die Datenschutzkonferenz der Länder und des Bundes hat das für Jugendliche konzipierte behördenübergreifende Internetprojekt Young Data ein Relaunch vorgesehen. Hier wird sich der Bereich Datenschutz als Kulturaufgabe gerade für die junge Zielgruppe durch redaktionelle Mitarbeit am Online-Auftritt Datenschutz in Baden-Württemberg weiter

© LfDI BW

Ein Highlight aus der Reihe „B. sucht Freiheit": Das Gespräch mit dem Plakatkünstler Klaus Staeck in seinen Arbeitsräumen in Heidelberg. Seine Plakate sorgen seit Jahrzehnten für Aufsehen, so auch die zu Big-Tech und zur Volkszählung.

engagieren. Jugend- und Medienbildung nimmt eine besondere Rolle bei der Vermittlungsarbeit ein.

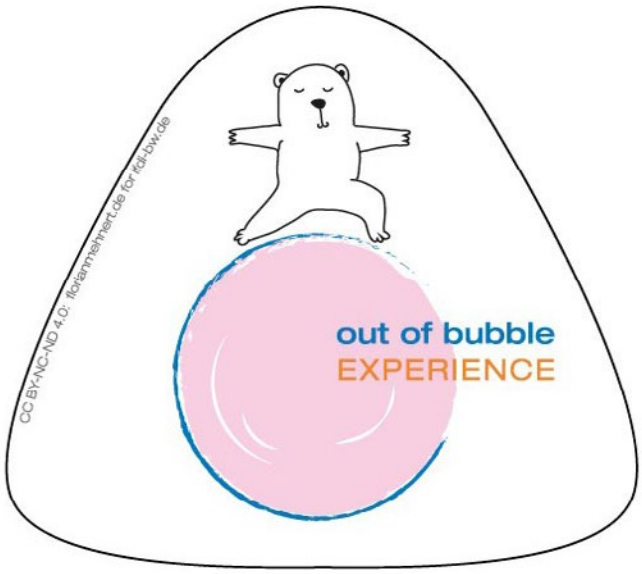
Gespräche über die Freiheit

In unserer Videoreihe „B. sucht Freiheit“ trafen wir regelmäßig Persönlichkeiten, die sich intensiv und nachdrücklich mit Fragen des Datenschutzes und der Informationsfreiheit auseinandergesetzt haben. Zu dem bereits etablierten Videoformat hat der Bereich Kultur im Jahr 2022 zur Vorbereitung und Durchführung weiterer Folgen beigetragen. Das Videoformat bietet etwa einen auf unserem PeerTube Kanal vielbeachteten Diskussionsbeitrag zu Themen im technischen Setting von Big Data und KI. So hat unlängst der Psychiater und Philosoph Thomas Fuchs (Verteidigung des Menschen 2021), der im Jahr 2023 den Erich-Fromm-Preis erhält, mit uns darüber gesprochen, wie sich die Künstliche Intelligenz in der psychiatrischen Behandlung entfaltet und Ärzt_innen assistieren soll, wie Chatbots das persönliche direkte Gespräch imitieren und wie eine permanente Gegenwart zwar das Vergangene stets abrufbar hält, aber eben nicht im eigentlichen Sinne erinnert. Und wir sprachen mit Thomas Fuch darüber, welche Selbst- und Fremdbilder der beispielsweise Jugendliche „produzieren“, wenn sie in den Sozialen Medien aktiv sind.

Auch unsere Gesprächsrunden etwa mit dem Bundesverfassungsrichter Heinrich Amadeus Wolff, dem Plakatkünstler Klaus Staeck und dem Journalisten Philip Banse interessierten viele Menschen. Wir erreichen durch die Vielfalt und unterschiedlichen Fachdisziplinen, in denen unsere Gesprächsgäste herausragend sind, neue Personengruppen, die wir anders nur schwerlich ansprechen könnten. Der interdisziplinäre Austausch mit Persönlichkeiten und Organisationen, die sich intensiv mit Datenschutz- und Fragen der Informationsfreiheit beschäftigen, bleibt für uns bedeutsam. So strecken wir unsere Fühler noch stärker in die Kulturszene und die Institute an den Universitäten aus, um hier unser Denken und Wissen einzubringen und zugleich Neues für uns als Dienststelle anzunehmen.

Ausblick

Wir nehmen uns auch für die Zukunft Kooperationen vor und Gespräche, Bildungsformate und: Kunst. Denn so sagte es Marshall McLuhan, ein Medientheoretiker, der aktueller nicht sein könnte, vor einem halben Jahrhundert: Kunst sei in der Lage „zukünftige soziale und technologische Entwicklungen zu antizipieren“, ein „Frühwarnsystem“; sie übernehme „als Radar die Funktion eines unverzichtbaren Wahrnehmungstrainings“. (Zitiert nach Hans Ulrich Obrist: Das Unsichtbare sichtbar machen: Kunst trifft auf KI / New Experiments in Arts and Technology, Vorlesung an der Saas Fee Academy 2018.)



Unsere Laptop-Sticker „out of bubble experience“ – einfach mal aus der Filterblase heraus treten und neue Erfahrungen machen. Die Sticker sind auch beliebt auf Kühlschränken in Studi-WGs.

8. Aktuelles aus der Bußgeldstelle

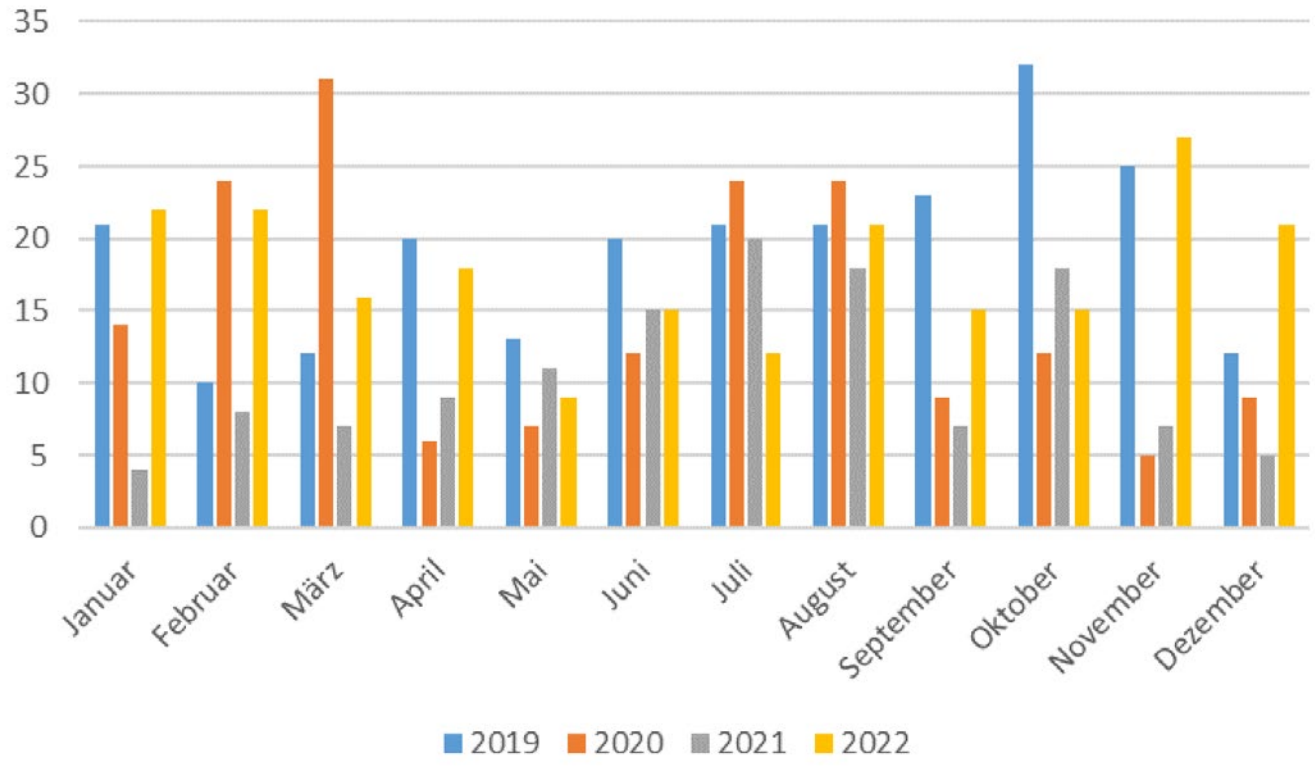
Vom 1. Januar bis 31. Dezember 2022 wurden bei der Bußgeldstelle insgesamt 213 neue Verfahren anhängig. Die Zahl der Neueingänge lag damit signifikant über dem der letzten beiden Jahre und erreichte wieder das Niveau der „Vor-Corona"-Jahre.

Im Berichtszeitraum hat die Bußgeldstelle 19 Bußgeldbescheide erlassen, von denen 18 rechtskräftig wurden. Sie richteten sich sowohl gegen Unternehmen als auch nicht-unternehmerisch tätige natürliche Personen. Während bei den Verfahren gegen Unternehmen die Verstöße vielfältiger Art waren, stand bei den Verfahren gegen nicht-unternehmerisch tätige natürliche Personen – wie im letzten Berichtszeitraum – die zweckwidrige Verwendung von personenbezogenen Daten zu privaten Zwecken, insbesondere durch Beschäftigte der Polizei, im Zentrum der Vorwürfe. Geldbußen wurden aber auch wegen heimlicher Videoüberwachung von Nachbar_innen oder dem wegen heimlichen GPS-Trackings von früheren Partner_innen oder flüchtigen Bekanntschaften verhängt. Insgesamt setzen wir Bußgelder in einer Höhe von 145.950,00 Euro und Gebühren in Höhe von 7.386,80 Euro fest. 151 weitere Verfahren wurden in sonstiger Weise erledigt, insbesondere durch Einstellung, wenn nach Ermittlungen durch die Bußgeldstelle ein Datenschutzverstoß nicht festgestellt oder nachgewiesen werden konnte oder wenn die Verhängung einer Geldbuße aus Verhältnismäßigkeitsgesichtspunkten nicht geboten erschien.

Umgang mit Gesundheitsdaten

Unsere Bußgeldstelle erhält regelmäßig Hinweise zu Datenschutzverstößen direkt aus der Bevölkerung. So machen uns betroffene Personen oder aufmerksame Bürger_innen auf unzulässige Videoüberwachungssysteme, die zweckwidrige Verwendung von zu Zwecken der Pandemiebekämpfung erhobenen Kontaktdaten oder auch unsachgemäß entsorgte Unterlagen aufmerksam.

Durch einen solchen Hinweis aus der Bevölkerung ergab sich auch der Verdacht, dass eine Apotheke bei der Entsorgung ihrer Unterlagen mit personenbezogenen Daten der besonderen Kategorie nicht die gesetzlichen Vorschriften einhält und darüber hinaus eine unzulässige Videoüberwachung betreibt.



Da sich aus dem Hinweis der Verdacht einer nicht unerheblichen unzulässigen Datenverarbeitung ergab, erwirkte die Bußgeldstelle – wie im letzten Tätigkeitsbericht dargestellt – einen Durchsuchungsbeschluss beim zuständigen Amtsgericht und führte auf dieser Grundlage eine Durchsuchung bei der betroffenen Apotheke durch.

Im Rahmen der Durchsuchung konnte vor Ort eine Vielzahl von Unterlagen mit personenbezogenen Daten der besonderen Kategorie in einem Müllraum, welcher für eine größere Gruppe nichtberechtigter Personen z. B. für andere Mietparteien zugänglich war, in insgesamt sechs großen Müllbehältnissen aufgefunden werden. Neben Ergebnissen aus Corona-Testungen stellte die Bußgeldstelle vor allem Rezepte mit Diagnosen und Kassenbelege, aber auch sonstige Korrespondenz sicher, aus denen sich regelmäßig neben Vor- und Zunamen die Anschrift, Telefonnummer und die gekauften Medikamente und damit die jeweiligen Erkrankungen entnehmen ließen. Zwar hatte die Apotheke auf Grund einer vorhergehenden Beschwerde an den einzelnen Arbeitsplätzen Aktenvernichter und diverse Behältnisse angebracht, welche zur Sortierung der zu entsorgenden Unterlagen dienten. Trotz dieser Vorkehrungen konnte eine hohe Anzahl an intakten oder nur unsachgemäß zerrissenen Unterlagen in den Müllbehältnissen aufgefunden werden.

Die Apotheke verstieß damit in einem nicht unerheblichen Maß gegen Artikel 5 Absatz 1 Buchstabe f DS-GVO, der von Verantwortlichen eine Verarbeitung personenbezogener Daten fordert, die eine angemessene Sicherheit der personenbezogenen Daten und den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen gewährleistet.

Darüber hinaus wurde im Rahmen der Durchsuchung festgestellt, dass die Apotheke eine Videoüberwachungsanlage in Betrieb hatte, welche den gesamten Geschäftsraum inklusive der Bedienplätze und damit auch die Mitarbeitenden der Apotheke, auch während der Öffnungszeiten, aufzeichnete. Ein Hinweis auf eine Videoüberwachung fehlte gänzlich.

Da die Geschäftsleitung bereits während der Durchsuchung an der Aufklärung des Sachverhaltes mitwirkte und auch während des Verfahrens umfassend kooperierte, zudem ihre technischen und organisatorischen Maßnahmen insoweit verbesserte, sahen wir in Bezug auf die unsachgemäße Entsorgung der Unterlagen trotz des Umfangs und der besonderen Sensibilität der betroffenen Daten eine Geldbuße in Höhe von 6.500,- Euro als verhältnismäßig an, die von der Betroffenen akzeptiert wurde. Nachdem die Betroffene zudem die Vorgaben der Aufsichtsbehörde zum datenschutzkonformen Betrieb der Videoüberwachungsanlage umgesetzt hatte, wurde in Bezug auf diesen Vorwurf unter entsprechender Anwendung des § 154 Absatz 1 Nummer 1 StPO von der Verhängung einer Geldbuße abgesehen, da eine solche im Vergleich zu der wegen der unsachgemäßen Entsorgung von Unterlagen verhängten Geldbuße nicht beträchtlich ins Gewicht gefallen wäre.

Aber nicht nur Unternehmen der Gesundheitsbranche gehen regelmäßig mit besonders schutzwürdigen Gesundheitsdaten um, auch Arbeitgeber können solche Daten in Bezug auf ihre Beschäftigten verarbeiten. Dies galt ganz besonders zu Zeiten der Corona-Pandemie, als auch Arbeitgeber damit konfrontiert waren, wie sie mit Informationen zu Corona-Erkrankungen oder dem Impfstatus umzugehen hatten.

Einen offensichtlich falschen Weg wählte hierbei ein Unternehmen, welches im Sommer letzten Jahres Informationen zum Impfstatus ihrer Beschäftigten zusammentrug und diese Informationen in einen Bürobelegungsplan einfließen ließ. Bei der Information gegenüber den Mitarbeitenden hinsichtlich der neuen Bürobelegung wurde ein Plan mitübersandt, bei dem den einzelnen Mitarbeitenden eine Farbe (grün, gelb oder rot) abhängig von ihrem Impfstatus zugewiesen war. Auch ohne große detektivische Begabung war es in Kombination mit den sonstigen Informationen ein Leichtes, den Impfstatus der Kolleg_innen zu ermitteln. Da es sich hierbei um einen grob fehlerhaften Umgang mit besonders schutzwürdigen Informationen handelt, wurde das Verfahren von der Fachabteilung an die Bußgeldstelle abgegeben, nachdem sichergestellt war, dass die Impfdaten gelöscht worden waren. Die Bußgeldstelle verhängte am Ende eine Geldbuße in Höhe von 20.000,- Euro. Bei der Zumessung wurde zu Gunsten des Unternehmens insbesondere dessen aktuelle schwierige wirtschaftliche Lage berücksichtigt.

In einem weiteren Fall, welcher zwar nicht den Umgang mit Gesundheitsdaten betraf, der aber wie der zuvor beschriebene eng mit der Corona-Pandemie zusammenhing, wurden wir bzw. die Polizei durch einen Hinweis aus der Bevölkerung darauf aufmerksam, dass ein Gastronom einen ganzen Beutel mit Corona-Kontaktzetteln kurzerhand im Wald entsorgt hatte. Zwar waren die entsprechenden Kontaktzettel auf Grund gesetzlicher Vorgaben nach vier Wochen zu löschen. Die hierbei gewählte Verfahrensweise war offensichtlich aber nicht sachgemäß. Während in anderen – weniger schwerwiegenden – Fällen des sachwidrigen Umgangs mit Kundendaten, z. B. bei offenen Kontaktlisten in Restaurants und Kneipen, Betroffene Geldbußen verhindern konnten, wenn sie aufzeigen konnten, dass zukünftig ein datenschutzwidriges Verhalten nicht zu erwarten ist, war in diesem Fall auf Grund der Vielzahl von betroffenen Personen und des sehr fahrlässigen Umgangs mit Kundendaten die Verhängung einer Geldbuße erforderlich. Diese betrug allein wegen der wirtschaftlichen Verhältnisse des Unternehmens lediglich 500,- Euro.

Wettbewerbsvorteil Datenschutzverstoß? Wettbewerbsvorteil Datenschutz!

Immer mehr Unternehmen sehen die DS-GVO, insbesondere wenn von Anfang an mitgedacht, als einen Wettbewerbsvorteil. Einige wenige versuchen dagegen, sich durch das Hinwegsetzen über datenschutzrechtliche Vorgaben einen Wettbewerbsvorteil gegenüber der Konkurrenz zu verschaffen. Im Berichtszeitraum gab es zwei solcher Vorfälle, bei denen konsequenterweise am Ende ein Bußgeld verhängt wurde, damit sich Datenschutzverstöße nicht lohnen.

In einem Fall hatte ein Grundstückseigentümer in einem Neubaugebiet ein Schreiben eines Bauträgers erhalten, in dem ihm ein Kaufpreisangebot für sein Grundstück unterbreitet wurde. Die Kenntnis

Mal hat man gute Ideen, mal schlechte, mal besonders schlechte: Corona-Kontaktzettel im Wald zu entsorgen gehört nicht nur aus Umweltschutzgründen zu den ganz schlechten Ideen.

von der Eigentümerstellung war aber keine allgemein bekannte Information, der Betroffene hatte seinen Wohnsitz sogar in einer anderen Gemeinde. Eine Information über die Herkunft seiner Daten enthielt das Schreiben nicht, auch auf Nachfrage wurde dem Adressaten nicht mitgeteilt, woher der Bauträger dessen Daten hatte, insbesondere die Kenntnis von dessen Eigentümerstellung.

Die Bußgeldstelle beim Landesbeauftragten ermittelte anschließend, dass ein Vermessungsingenieur von seiner Befugnis zur Einsichtnahme in das elektronische Grundbuch im automatisierten Abrufverfahren Gebrauch gemacht und in zwei Fällen mehrere Hundert Grundstückseigentümer_innen ohne deren Kenntnis identifiziert und die entsprechenden Informationen an einen Bauträger weitergegeben hatte. Dieser wiederum schrieb die so ermittelten Eigentümer mit einem Kaufpreisangebot für deren Grundstücke an, ohne die notwendigen Informationen nach Artikel 14 DS-GVO zu erteilen, insbesondere ohne über die Herkunft der Daten zu informieren.

Dieses Vorgehen stellt einerseits einen Verstoß gegen Artikel 6 Absatz 1 DS-GVO dar. So ist bei der Interessenabwägung im Rahmen des Artikels 6 Absatz 1 Buchstabe f DS-GVO zu berücksichtigen, dass zwischen den Grundstückseigentümern und dem Bauträger keine vorherige Geschäftsbeziehung bestand und die Eigentümer nicht davon ausgehen mussten, dass ihre Daten im Grundbuch für werbliche Ansprachen zur Verfügung stehen. Hierbei kommt besondere Bedeutung der Tatsache zu, dass Grundstückseigentümer weder der Eintragung im Grundbuch noch der Datenübermittlung widersprechen können, vielmehr werden ihre Daten auf Grund einer gesetzlichen Pflicht erhoben und im Grundbuch eingetragen. Diese gesetzliche Pflicht dient aber nicht der werblichen Ansprache, sondern der Rechtssicherheit bei Grundstücksgeschäften. Dementsprechend ist für das grundbuchrechtliche Einsichtsrecht auch allgemein anerkannt, dass ein alleiniges Erwerbsinteresse nicht zur Einsichtnahme berechtigt, es vielmehr bereits der konkreten Vertragsverhandlungen bedarf.

Zudem lag auch ein Verstoß gegen Artikel 14 DS-GVO vor, indem den Eigentümern – auch bei Kontaktaufnahme – keine Informationen zur Datenverarbeitung zur Verfügung gestellt wurden. Diese Informationen sind aber wesentliche Voraussetzung für betroffene Personen, um ihre Betroffenenrechte nach den Artikel 15 ff. DS-GVO geltend machen zu können. Ein Ausschlussgrund war hier nicht gegeben, insbesondere stellt § 12 Grundbuchordnung (GBO) keine Rechtsvorschrift im Sinne des Artikel 14 Absatz 5 Buchstabe c DS-GVO dar, da für betroffene Personen bei Einsichtnahme durch Dritte aus § 12 GBO weder die datenerhebende Stelle noch Umfang, Zweck oder Dauer der Datenerhebung ersichtlich sind.

Als Konsequenz hat unsere Bußgeldstelle Geldbußen gegen das Bauträgerunternehmen und den Vermessungsingenieur in Höhe von 50.000 Euro respektive 5.000 Euro verhängt. Bei der Zumessung der Geldbuße wurde neben der Anzahl der betroffenen Personen, der Art der betroffenen Daten und der Bedeutung der verletzten Vorschriften vor allem die Kooperation der verantwortlichen Stellen im Bußgeldverfahren berücksichtigt.

In einem anderen Fall erhielt ein Inkassounternehmen von dem Beschäftigten eines insolventen Unternehmens eine Aufstellung mit Anlegerinformationen ohne Kenntnis oder Zustimmung der betroffenen Personen. Diese Informationen verwendete das Inkassounternehmen gezielt, um den Anlegern seine Dienste, konkret die Anmeldung der Insolvenzforderung sowie die Begleitung des Verfahrens, anzubieten, ohne diesen aber die Quelle der Daten offen zu legen.

Dies sahen wir als einen Verstoß gegen Artikel 6 Absatz 1 DS-GVO i. V. m. Artikel 14 Absatz 1, 2 DS-GVO an. Bei der Beurteilung, ob das Unternehmen sich auf Artikel 6 Absatz 1 Buchstabe f DS-GVO stützen konnte, war einerseits zu berücksichtigen, dass der offensichtliche Datenmissbrauch durch den Mitarbeitenden des insolventen Unternehmens bei der Weitergabe der Daten auf die Frage der Berechtigung des Interesses an der Weiterverarbeitung dieser Daten durchschlägt. Zudem kann die entsprechende Datenverarbeitung auch nicht als erforderlich angesehen werden, hier wäre als datensparsameres Mittel auch der Hinweis auf die angebotene Dienstleistung durch das insolvente Unternehmen selbst möglich gewesen. Zuletzt stehen der Datenverarbeitung auch überwiegende schutzwürdige Interessen der betroffenen Personen entgegen.

Bei der im Rahmen des Artikels 6 Absatz 1 Buchstabe f DS-GVO notwendigen Interessenabwägung sind insbesondere die vernünftige Erwartungshaltung der betroffenen Person (reasonable expectations) bzw. die Absehbarkeit (Branchenüblichkeit) der Verarbeitung (vgl. Erwägungsgrund 47 Satz 1 Halbsatz 2 und Satz 3) sowie die bestehenden Beziehungen zu dem Verantwortlichen (Erwägungsgrund 47 Satz 2) zu berücksichtigen. In dem von uns zu beurteilenden Fall bestand indes keine rechtliche oder wirtschaftliche Beziehung zwischen dem Inkassounternehmen und den Anlegern. Die betroffenen Personen mussten darüber hinaus vernünftigerweise nicht damit rechnen, dass das insolvente Unternehmen bzw. ein für dieses tätiger Mitarbeitender ihre Daten an ein drittes Unternehmen für (Werbe-)Angebote weitergibt und dieses ihnen unter Ausnutzung der Kenntnis ihrer Betroffenheit von dem Insolvenzverfahren (Werbe-)Angebote zusendet, die ihre Stellung als Gläubiger betreffen.

Als einen wesentlichen Aspekt der Zumessung ermittelte die Bußgeldstelle schätzungsweise, welchen Umsatz das Inkassounternehmen letztlich mit dem datenschutzwidrigen Werbeangebot generieren konnte. Dies floss dann in die Festsetzung der Geldbuße ein, so dass die Bußgeldhöhe mindestens den Tatertrag abschöpfte. Das Bußgeld ist mittlerweile rechtskräftig.

Vorgaben aus Europa zur Zumessung von Geldbußen

Die DS-GVO ermöglicht es den europäischen Aufsichtsbehörden nicht nur, bei Datenschutzverstößen eigenständig und mit vergleichbaren Befugnissen wie eine Staatsanwaltschaft zu ermitteln – die Aufsichtsbehörden haben auch die Befugnis, Verstöße wirksam zu sanktionieren. Bei gravierenden Fällen kann die Aufsichtsbehörde auch Bußgelder erlassen. Bußgelder können erheblich sein und bis zu 20 Millionen Euro oder bei Unternehmen 4 Prozent des weltweiten Jahresumsatzes betragen.

Um mehr Transparenz bei Bußgeldern herzustellen hat die Datenschutzkonferenz (DSK) unter unserer federführenden Mitwirkung im Oktober 2019 ein eigenes Konzept zur Bußgeldzumessung erstellt. Nun hat der Europäische Datenschutzausschuss (EDSA) in seiner Sitzung vom 12. Mai Leitlinien zur Bußgeldbemessung („Guidelines on the calculation of fines“) angenommen. (Siehe auch Kapitel 4.1.4)

Wesentliches Ziel der Leitlinien ist eine weitere Harmonisierung der europäischen Bußgeldpraxis. Neben Regelungen zur maximalen Bußgeldhöhe ist Kernelement der Leitlinien – ähnlich wie im Bußgeldkonzept der DSK – die Festlegung eines Grundbetrags („starting point“) für die Zumessung. Dieser

Ein weiterer Schritt in Richtung einheitlicher Vollzug: Europaweite einheitliche Regeln für die Zumessung Bußgelder sorgen für Klarheit und Nachvollziehbarkeit.

bestimmt sich aus drei Größen: der Einordnung der Tat anhand der verletzten Norm, der Schwere der konkreten Tat sowie des Unternehmensumsatzes. So ist beispielsweise der Grundbetrag, welcher bei mittelschweren Verstößen bis zu 20 Prozent der gesetzlichen Bußgeldgrenze betragen kann, bei Kleinstunternehmen mit einem Umsatz von höchstens 2 Millionen Euro auf 0,2 Prozent dieses Betrags zu reduzieren. Der EDSA macht damit deutlich, dass der Unternehmensumsatz auch für die konkrete Bußgeldberechnung eine maßgebliche Größe ist, Bußgelder umgekehrt die Unternehmen auch nicht überfordern dürfen. Entgegen der teilweise geäußerten Befürchtungen geht diese Konzeption nicht zu Lasten von umsatzstarken Unternehmen, vielmehr haben die Leitlinien gerade umgekehrt umsatz- und finanzschwächere Unternehmen im Blick.

Die vom EDSA vorgelegten Leitlinien stellen einen wichtigen Baustein zur einheitlichen Anwendung der DS-GVO dar. Hierdurch wird in Europa mehr Transparenz in der Bußgeldpraxis geschaffen und für Rechtsklarheit in zentralen Fragen der Bußgeldbemessung gesorgt. Die Leitlinien sind allerdings kein „Bußgeldrechner", vielmehr bedarf eine wirksame, verhältnismäßige und abschreckende Sanktionierung nach wie vor einer konkreten Abwägung im Einzelfall. Als Leitlinien haben sich diese bereits in der Praxis durch die Bußgeldstelle bewährt.

Informationszugang zu Bußgeldbescheiden

Bei besonders öffentlichkeitswirksamen Bußgeldverfahren, deren Entscheidung über den Einzelfall hinaus von öffentlichem Interesse ist, berichten wir nach Abschluss des Bußgeldverfahrens hierüber in Erfüllung unseres gesetzlichen Auftrags zur Sensibilisierung der Öffentlichkeit gem. Artikel 57 Absatz 1 Buchstabe b und d DS-GVO i. V. m. Artikel 58 Absatz 3 Buchstabe b DS-GVO. Dies weckt regelmäßig das Interesse von Bürger_innen, welche auf Grundlage des Landesinformationsfreiheitsgesetzes (LIFG) Zugang zu Informationen in dem Bußgeldbescheid – in anonymisierter – Form begehren.

In einem besonders gelagerten Fall hatten wir, da es bereits entsprechende Presseartikel und -anfragen unter Nennung des betroffenen Unternehmens gab, in identifizierender Weise über einen Bußgeldbescheid gegen die AOK Baden-Württemberg berichtet. Da die AOK in der Folge auf verschiedene IFG-Anträge hin nicht mit der Zurverfügungstellung des Bußgeldbescheids, auch nach Schwärzung aller personenbezogenen Daten sowie Betriebs- und Geschäftsgeheimnisse, einverstanden war, schloss sich an das Bußgeldverfahren ein Gerichtsverfahren zu der Frage an, inwieweit Bußgeldbescheide wegen Verstößen gegen die DS-GVO dem Informationszugang nach dem Landesinformationsfreiheitsgesetz unterliegen. Ein solcher Informationszugang besteht grundsätzlich nur insoweit, wie die Verwaltung auch als Verwaltung handelt (in Abgrenzung zur Judikative und Legislative). Hierbei vertraten wir die Position, dass die DS-GVO Geldbußen als Abhilfemaßnahmen einordnet, dementsprechend diese nicht repressiver Natur sind und damit letztlich Verwaltungshandeln darstellen. Das Gericht konnte dieser Argumentation aber nicht folgen und ordnete auch verwaltungsrechtliche Sanktionen nach der DS-GVO– zumindest für die Frage der Anwendbarkeit des Landesinformationsfreiheitsgesetzes – dem Handeln von Strafverfolgungsbehörden zu. Zudem sah das Gericht die Informationszugangsregelungen für Bußgeld- und Strafverfahren auch im vorliegenden Fall für abschließend an, obwohl nach unserer Auffassung einerseits grundsätzlich dieser Ausschluss für datenschutzrechtliche Bußgeldverfahren wegen der Einordnung von Geldbußen als Abhilfemaßnahmen sowie der Aufgabe der Datenschutzbehörden zur Sensibilisierung der Öffentlichkeit gem. Artikel 57 Absatz 1 Buchstabe b und d DS-GVO i. V. m. Artikel 58 Absatz 3 Buchstabe b DS-GVO nicht zwingend ist, andererseits im konkreten Fall der Schutzzweck dieser spezialgesetzlichen Zugangsregelungen – das Recht auf informationelle Selbstbestimmung der von einem Straf- oder Bußgeldverfahren betroffenen Personen – nicht berührt war, da es sich bei der AOK um eine Körperschaft des öffentlichen Rechtes handelt.

Durch die Entscheidung des VG Stuttgart haben wir in dieser für uns sehr praxisrelevanten Rechtsfrage nunmehr insoweit Klarheit, dass das Landesinformationsfreiheitsgesetz nicht als Grundlage für den Zugang zu Bußgeldbescheiden dienen kann. Der Zugang zu Informationen dem Bußgeldbescheid richtet sich vielmehr ausschließlich nach anderen Vorschriften, namentlich nach den Regelungen des § 4 LPresseG und des § 475 Absatz 1 Strafprozessordnung (i. V. m. § 46 Absatz 1 Ordnungswidrigkeitengesetz), so dass er nur noch bestimmten Personen beziehungsweise in besonderen Konstellationen zu gewähren ist.

Forensik

Mit der fortschreitenden Digitalisierung ändern sich auch die Anforderungen an den Umgang und die Auswertung von Beweismitteln in Bußgeldverfahren. Da die Datensätze von Unternehmen in der Regel in elektronischer Form vorliegen, handelt es sich bei den meisten Beweismitteln in datenschutzrechtlichen Bußgeldverfahren als Konsequenz hieraus um elektronische Datenträger. Diese müssen gesichert, aufbereitet und ausgewertet werden. Abhängig von den Speichermedien, der Art der zu untersuchenden Datensätzen, dem Ziel der Untersuchung sowie dem Umfang der Daten handelt es sich hierbei um komplexe Verfahren, die spezieller Software bedürfen. Um hierfür die notwendige Expertise im Haus zu haben und sich zudem von Dritten unabhängig zu machen, hat unsere Bußgeldstelle im Berichtszeitraum mit Unterstützung von Forensikern des Landeskriminalamt eine eigene IT- und Multimedia-Forensik aufgebaut, wodurch eine weitere Professionalisierung bei der Bearbeitung von Bußgeldverfahren erreicht wird.

Besser ausgestattet als Old-School Detektive: Die Bußgeldstelle hat zwar auch Lupen, aber zudem noch leistungsfähige Technik, um ihre Prüfungen sorgfältig und professionell durchzuführen.

Unsere Expert_innen im Haus kümmern sich um Eingaben und bieten zudem Unterstützung mit Vorträgen, Schulungen und Fortbildungen in unserem Bildungszentrum. Einfach den QR-Code scannen und die passende Veranstaltung finden!

9. Datenschutz-Vielfalt, veranschaulicht von Fall zu Fall

© Frank Gärtner – stock.adobe.com

Flughafen Stuttgart: Automatisierte Kennzeicherfassung im Parkbereich ist möglich.

9.1 Neues aus dem Amt: Innere Sicherheit, Justiz, Kommunalwesen

9.1.1 Einsicht in das Handelsregister – kostenfrei und ohne Registrierung

Seit dem 1. August 2022 sind Abrufe aus dem Handelsregister und anderen von den Registergerichten geführten Registern nicht mehr kostenpflichtig. Auch eine Nutzerregistrierung ist nicht mehr vorgesehen. Diese vereinfachte und kostenfreie Zugangsmöglichkeit hat bei zahlreichen Betroffenen die Sorge um einen Missbrauch ihrer Daten ausgelöst. Dies gilt vor allem für Fälle, in denen in den abrufbaren Dokumenten die vollständigen Wohnanschriften oder bildliche Wiedergaben von Unterschriften enthalten sind. Die bei uns hierzu eingegangenen Anfragen und Beschwerden bezogen sich sämtlich auf das Handelsregister.

Die genannten Änderungen beruhen auf dem Gesetz zur Umsetzung der Digitalisierungsrichtlinie. Dass der Abruf der personenbezogenen Daten aus dem Handelsregister sowie aus den zum Handelsregister eingereichten Dokumenten jeder Person zu Informationszwecken gestattet ist, war dagegen bereits vor dem 1. August 2022 gesetzlich vorgeschrieben und dient vor allem der Transparenz im Rechtsverkehr. In Bezug auf die zu veröffentlichenden Daten ist ebenfalls keine Änderung der Rechtslage eingetreten.

Während die Bereitstellung der Informationen zum Abruf durch die Allgemeinheit über das gemeinsame Registerportal der Länder erfolgt, das vom Ministerium der Justiz des Landes Nordrhein-Westfalen im Auftrag der Länder betrieben wird, werden die Eintragungen in das Register, die Erstellung der Abdrucke und das Einstellen der Dokumente vom jeweils zuständigen Registergericht vorgenommen.

Aufgrund gesetzlicher Pflichten, die sich aus verschiedensten bereichsspezifischen Normen ergeben, ist die Eintragung und Veröffentlichung einer großen Zahl personenbezogener Daten im Handelsregister zulässig. Ob eine durch ein ba-

den-württembergisches Registergericht erfolgte Registereintragung beziehungsweise die Aufnahme von Dokumenten zur unbeschränkten Einsicht im Einzelfall rechtmäßig ist, können wir jedoch nicht überprüfen. Denn hierbei handelt es sich um eine justizielle Tätigkeit, die der Zuständigkeit der datenschutzrechtlichen Aufsichtsbehörden entzogen ist (vgl. Artikel 55 Abs. 3 DS-GVO). Die Personen, die sich bei uns über den einfachen und kostenfreien Abruf sie betreffender personenbezogener Daten aus dem Handelsregister beschwert hatten, konnten wir daher lediglich allgemein über die Rechtslage informieren.

Am 23. Dezember 2022 ist eine Änderung der Handelsregisterverordnung (HRV) in Kraft getreten, die hoffentlich dazu beiträgt, dass sich die Einsicht künftig auf für den Rechtsverkehr notwendige Unterlagen beschränkt.

In § 9 Absatz 1 HRV wurden zum einen klarstellende Regelungen dazu aufgenommen, welche zum Handelsregister eingereichten Dokumente das Registergericht zur unbeschränkten Einsicht in den Registerordner aufnehmen soll. Zum anderen ist nun in § 9 Absatz 7 HRV klargestellt, unter welchen Voraussetzungen der nachträgliche Austausch von zur Einsicht eingestellten Dokumenten möglich ist und wie hierbei zu verfahren ist.

Darüber hinaus gibt es auch Bestrebungen, die Dienstordnung für Notare dahingehend zu ändern, dass die Wohnanschrift (hier ist der Straßenname und die Hausnummer, nicht jedoch der Wohnort gemeint) in bestimmtem Fällen bereits nicht zum Urkundeninhalt gemacht werden soll beziehungsweise, dass bei Dokumenten, die elektronisch in öffentlich beglaubigter Form an das Handelsregister übermittelt werden, Wohnanschrift und Unterschriftszug in der Regel nicht aufgenommen oder unkenntlich gemacht werden sollen.

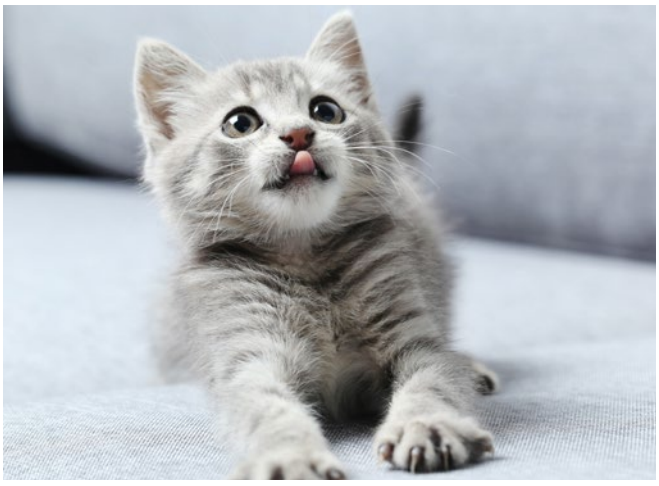
Wir werden den Fortgang der Änderungsbestrebungen bzw. die Auswirkungen der bereits in Kraft getretenen Änderung der Handelsregisterverordnung weiterverfolgen.

9.1.2 Alle Jahre wieder: die Hundebestandsaufnahme

Bereits mehrfach haben wir uns in der Vergangenheit mit dem Thema „Hundebestandsaufnahme" beschäftigt. Nach wie vor ist es nicht zulässig, zum Zwecke der Hundesteuerfahndung sämtliche Einwohner_innen einer Gemeinde „auf freiwilliger Basis" dazu zu befragen, ob ein Hund gehalten wird (vgl. dazu schon unseren 30. Tätigkeitsbericht, S. 116 f.).

Ist eine Hundesteuer durch kommunale Satzung festgelegt, ist es selbstverständlich Aufgabe der Gemeinde, für deren gleichmäßige Erhebung zu sorgen. Die Frage ist nur, mit welchen Mitteln sie diese gleichmäßige Erhebung erwirken kann und darf. Bereits in der Vergangenheit haben wir uns mit der sogenannten „Hundebestandsaufnahme" beschäftigt. Gemeint ist das Vorgehen einer Gemeinde, entweder selbst oder durch Beauftragung Dritter sämtliche Haushalte der Gemeinde dahingehend zu überprüfen, ob ein Hund gehalten wird. Dazu wird an jeder Haus- oder Wohnungstür geklingelt. Faktisch findet damit letztlich eine Rasterfahndung statt, für die die einschlägigen Gesetze keine Rechtsgrundlage bieten. Zwar ist eine Auskunftspflicht auf Nachfrage der zuständigen Behörde sogar als verpflichtend im Gesetz geregelt – allerdings nur dann, wenn sich diese Auskunft auf einen konkreten Sachverhalt bezieht und nicht dazu dienen soll, ohne konkrete Veranlassung „ins Blaue hinein" auszuforschen, ob überhaupt ein steuerlich erheblicher Sachverhalt vorliegt.

Nun soll es in dem von uns zu beurteilenden Fall zwar nicht so sein, dass eine Pflicht zur Auskunft besteht, was die Gemeinden auch regelmäßig be-



Ob Katzen die Hundebestandsaufnahme aufregend finden, wissen wir nicht. Beim LfDI sind wir aufgrund der jährlich wiederkehrenden Thematik Expert_innen auf dem Gebiet.

tonen. Vielmehr soll freiwillig eine Angabe dazu gemacht werden, ob ein Hund gehalten wird oder nicht, ob also ein steuerlich erheblicher Sachverhalt vorliegt oder nicht. Diese Freiwilligkeit sehen wir jedoch nicht. So handeln die beauftragten Kontrolleure letztlich für die Gemeinde im Rahmen eines Über-Unterordnungsverhältnisses zum_r befragten Bürger_in, nämlich zum Zwecke der Durchsetzung einer Steuer. In diesem Bereich scheidet ein freiwilliges Handeln von vornherein aus. Spätestens aber, wenn nach dem Öffnen der Wohnungstür eine feuchte Schnauze die Füße beschnuppert, ist eine Wahlmöglichkeit für die Kontrollierten ohnehin nicht mehr vorhanden. Solche Erkenntnisse werden von den Kontrolleuren auch protokolliert und später bei der Steuererhebung herangezogen. Hier wird außerdem deutlich, dass – auch wenn die Wohnungen nicht betreten werden – jedenfalls die häusliche Sphäre betroffen ist, die besonderen Schutz genießt.

Wesentlich ist im Übrigen, dass die gewählte Ermittlungsmaßnahme vor allem Personen betrifft, die keinen Hund halten oder zwar einen Hund halten, aber ihre Steuer bereits entrichten – die mithin keinen Anlass dafür geboten haben, dass sie von einer staatlichen Maßnahme betroffen werden. Die Werteordnung des Grundgesetzes und auch der baden-württembergischen Verfassung gibt vor, dass eine Sachverhaltsaufklärung nicht um jeden Preis erfolgen darf. Vor dem Hintergrund des Rechtsstaatsgebots ist es mindestens geboten, den von der Maßnahme betroffenen Personenkreis mittels sachgerechter Kriterien einzugrenzen. Eine Totalerfassung ist demgegenüber unzulässig.

Selbstverständlich dürfen und müssen die zuständigen Behörden im Sinne der Steuergerechtigkeit nach nicht bezahlten Steuern fahnden. Für derartige Ermittlungsmaßnahmen gibt es auch vom Gesetzgeber vorgesehene Möglichkeiten. Diese haben allerdings auch Grenzen. Eine (faktische) Rasterfahndung ist dort nicht vorgesehen.

9.1.3 Ein Prüfverfahren schlägt Wellen

Neben den bekannten Aufgaben und Befugnissen als datenschutzrechtliche Aufsichtsbehörde gemäß den Artikeln 57 und 58 DS-GVO und § 25 Landesdatenschutzgesetz (LDSG) kommt uns als dem Landesbeauftragten für den Datenschutz eine weitere Aufgabe zu: So sind gemäß § 21 Abs. 3 LDSG die Abgeordneten des Landtags berechtigt, Anfragen an uns zu stellen und wir sind umgekehrt verpflichtet, diese zu beantworten. Hieraus erwächst alleine eine Verpflichtung gegenüber den anfragenden Abgeordneten beziehungsweise dem Parlament, eine Beteiligung anderer Stellen – insbesondere eine Anhörung – ist, anders als in sonstigen Verfahren des LfDI weder vorgesehen noch ohne weiteres statthaft.

Mit einem besonderen Fall der parlamentarischen Anfrage hatten wir es im Mai 2022 zu tun: Wir wurden von der baden-württembergischen SPD-Fraktion um eine datenschutzrechtliche Bewertung eines Vorgangs im Innenministerium gebeten. Ausgangspunkt waren ursprünglich Vorwürfe gegen den Inspekteur der Polizei, welche in ein Disziplinarverfahren mündeten. Im Rahmen dieses laufenden Disziplinarverfahrens hatte dessen Anwalt dem Innenministerium den Wunsch zu einem persönlichen Gespräch unterbreitet. Dieses Schreiben war in der Folge durch das Innenministerium an einen einzelnen Journalisten weitergegeben worden. Nach einer öffentlichen Stellungnahme des Innenministers diente diese Weitergabe der Transparenz, um den Anschein einer „Mauschelei“ zu verhindern.

In unserer Prüfung auf Grundlage der uns seinerzeit vorliegenden Informationen, insbesondere der öffentlichen Stellungnahme des Innenministers, konnten wir keine Rechtsgrundlage für die Weitergabe des Anwaltsschreibens erkennen. Nach unserer Einschätzung wurden vielmehr durch die Weitergabe des Schreibens personenbezogene Daten eines Landesbeamten an einen Dritten ohne Einwilligung der betroffenen Person oder Vorliegen einer spezifischen gesetzlichen Legitimation übermittelt – und sodann veröffentlicht.

Die Übermittlung von Daten aus der Personalakte beziehungsweise einem Disziplinarverfahren ist wegen ihrer besonderen Schutzwürdigkeit nur unter ganz engen Voraussetzungen zulässig, insbesondere wenn sie gegenüber am Verfahren unbeteiligten Dritten erfolgen. Hier gilt grundsätzlich die Vertraulichkeit der Personalakte und des Disziplinarverfahrens, mit der Herausgabe des Anwaltsschreibens war diese in Bezug auf den sich daraus ergebenden Inhalt aufgehoben. Beamte, die sich in solch einem Verfahren befinden, müssen sicher sein und darauf vertrauen können, dass keine persönli-

chen Informationen nach außen dringen. Sie haben einen Anspruch auf die Fürsorge ihres Dienstherrn – gerade in einem Disziplinarverfahren, in dem ja die Unschuldsvermutung gilt. Dementsprechend käme eine Datenübermittlung nur zur Abwehr einer erheblichen Beeinträchtigung des Gemeinwohls oder zum Schutz rechtlich höherrangiger Interessen des jeweiligen Adressaten in Betracht.

In der Unterbreitung eines Gesprächsangebots eines Beamten im Rahmen eines Disziplinarverfahrens konnten wir keine solche erhebliche Beeinträchtigung des Gemeinwohls erkennen, die es abzuwehren gegolten hätte. So wurde unserer Auffassung nach durch ein solches Gesprächsangebot – auch im konkreten Fall – keineswegs bei unbefangenen Dritten der Anschein erweckt, es solle „gemauschelt" oder „unter den Teppich gekehrt" werden. Vielmehr entsprach nach unseren Erkenntnissen das Anwaltsschreiben und die darin geäußerte Gesprächsofferte den üblichen Gepflogenheiten im Rahmen einer rechtlichen Auseinandersetzung, wonach die anwaltliche Vertretung regelmäßig den Versuch einer einvernehmlichen Konfliktlösung mit dem Dienstherrn unternimmt.

Transparenz und Nachvollziehbarkeit von Verwaltungshandeln finden Ausdruck und zugleich Grenze in den gesetzlichen Regelungen zur Datenübermittlung. Darüberhinausgehend gibt es für Transparenzerwägungen schon grundsätzlich keinen Raum, erst recht nicht unter Berücksichtigung der besonderen Geheimhaltungsinteressen eines Beamten in einem laufenden Disziplinarverfahren.

Auf Grund dieser Bewertung haben wir – nach pflichtgemäßer Beantwortung der Anfrage der SPD-Fraktion – schließlich ein aufsichtsbehördliches Verfahren nach Artikel 58 DS-GVO eingeleitet, welches mit Rücksicht auf die staatsanwaltschaftlichen Ermittlungen zum gleichen Sachverhalt bis zum förmlichen Abschluss dieser Ermittlungen zurückgestellt wurde. Bei Wiederaufnahme des Verfahrens werden wir dann selbstverständlich zunächst das Innenministerium anhören, bevor wir ggf. zu einer endgültigen Bewertung der Sach- und Rechtslage kommen.

9.1.4 Mehr Beratungen und Kooperationen – neu mit dabei: Die Cybersicherheitsagentur des Landes Baden-Württemberg

Der Landesbeauftragte baut seine Beratung und Kooperation mit anderen öffentlichen Stellen aus, auch im Sicherheitsbereich. Von deren Gründung an haben wir auch mit der Cybersicherheitsagentur zusammengearbeitet und unsere Expertise angeboten.

Auf der Datenautobahn ist viel los. Cybersichersicherheit hilft, die Bürgerrechte auch in der digitalen Welt zu wahren.

Datenschutz ist ebenso wie die Informationssicherheit eine Querschnittsmaterie, die fast bei jeglicher Aufgabenerfüllung öffentlicher Stellen relevant ist. Auch gibt es jede Menge Schnittstellen der beiden Bereiche, da mit der immer schneller werdenden Digitalisierung auch Cybersicherheit sowie Cybercrime und damit einhergehend die Frage des Datenschutzes immer relevanter wird. Mit dem gemeinsamen Ziel vor Augen, die Grundrechte der Bürger_innen im Zeitalter der Digitalisierung adäquat zu schützen, ergeben sich Synergieeffekte mit anderen Stellen. Wir freuen uns also sehr über die verschiedenen Beratungen oder Kooperationen in diesem Bereich, seit ihrer Gründung auch mit der Cybersicherheitsagentur. Beispielsweise erarbeiten wir derzeit eine gemeinsame Informationsbroschüre, damit für Bürger_innen auf einen Blick nachvollziehbar ist, wer im Bereich Cybersicherheit und Cybercrime wie helfen kann. Ziel der Kooperation ist es, für die Bürger_innen herauszuarbeiten, dass in vielen Bereichen der Digitalisierung staatliche Akteure für die Sicherheit der digitalen Infrastruktur sorgen können und es hierfür klare Ansprechpersonen gibt. Auch wenn die jeweilige staatliche Institution unterschiedliche Aufgaben wahrnimmt, so steht sie doch stets im Dienste der Bürgerschaft und wirkt dabei mit, dass Bürger_innen, Vereine, Behörden und Unternehmen in Baden-Württemberg bestmöglich geschützt sind. Die Publikation soll im Frühjahr 2023 erscheinen – weitere Kooperationen nicht ausgeschlossen!

Auch zukünftig wollen wir zu datenschutzrechtlichen Themen mit den anderen öffentlichen Stellen kooperieren. Insbesondere wegen der Schnittstelle Datenschutz/Informationssicherheit freuen wir uns auf die Zusammenarbeit mit der Cybersicherheitsagentur.

9.1.5 Gratulationen zu Jubiläen im Amtsblatt

Immer wieder erreichen uns Anfragen dazu, ob man Einwohner_innen im gemeindlichen Amtsblatt zu Jubiläen gratulieren könne. Wir haben uns daher mit dieser Fragestellung befasst, und sind zu dem Ergebnis gekommen, dass dies mittlerweile nur noch mit Einwilligung des_der Glückwunschempfänger_in zulässig ist.

Die Veröffentlichung von runden Geburtstagen oder goldenen Hochzeiten im Amtsblatt hat in Baden-Württemberg eine gewisse Tradition. Datenschutzrechtlich handelt es sich dabei um eine Verarbeitung personenbezogener Daten, die einer Rechtsgrundlage bedarf — in besonderem Maße, wenn das Amtsblatt im Internet abrufbar ist. Bis zur bundesweiten Vereinheitlichung des Melderechts im Jahr 2015 erlaubte das baden-württembergische Landesrecht explizit eine Veröffentlichung von Jubiläen, siehe § 34 Absatz 2 des Meldegesetzes Baden-Württemberg alte Fassung: „Die Meldebehörde darf Namen, Doktorgrad, Anschriften, Tag und Art des Jubiläums von Alters- und Ehejubilaren veröffentlichen und an Presse und Rundfunk zum Zwecke der Veröffentlichung übermitteln."

In unserem Tätigkeitsbericht von 2010/2011 hatten wir uns bereits mit diesem Thema beschäftigt, als nach und nach die bis dato nur in Druckform erscheinenden Amtsblätter auch ins Internet wanderten. Zwar erlaubte die damalige Norm die Veröffentlichung, allerdings nicht diejenige zum weltweiten Abruf im Internet (siehe S. 121 im Tätigkeitsbericht 2010/2011).

Im Jahr 2015 trat bundeseinheitlich das Bundesmeldegesetz (BMG) in Kraft und löste damit die oben genannte baden-württembergische (Landes-) Regelung ab. Das Bundesmeldegesetz sieht nunmehr in seinem § 50 Absatz 2 vor: „Verlangen Mandatsträger, Presse oder Rundfunk Auskunft aus dem Melderegister über Alters- oder Ehejubiläen von Einwohnern, darf die Meldebehörde Auskunft erteilen […]". Diese neue gesetzliche Regelung greift indes die Möglichkeit einer Veröffentlichung in seinem Wortlaut nicht mehr auf. Sie stellt folglich eine Befugnis dar, die entsprechenden Daten zum Zwecke der Gratulation zu übermitteln, sie erlaubt jedoch keine Veröffentlichung. Für bedürfte es folglich einer anderen Rechtsgrundlage.

Auch außerhalb des Melderechts ist uns keine gesetzliche Rechtsgrundlage bekannt, welche die öffentliche Gratulation zu Jubiläen erlauben würde. Teilweise wurde vertreten, dass eine Veröffentlichung auf die Generalnorm des § 4 Landesdatenschutzgesetz gestützt werden könne. Diese Norm, welche von vornherein nur zur Anwendung gelangen könnte, wenn § 50 Absatz 2 BMG keine abschließende Regelung darstellt, setzt jedoch voraus, dass es eine öffentliche Aufgabe gibt, für die die in Rede stehende Datenverarbeitung erforder-

lich ist. Eine öffentliche Aufgabe ist zwar unbedingt auch die Öffentlichkeitsarbeit von Gemeinden, wie sie beispielsweise im Amtsblatt stattfindet. Es ist jedoch nicht ersichtlich, weshalb die Veröffentlichung privater Informationen, unter Umständen weltweit durch Publikation im Internet, für diesen Zweck erforderlich sein sollten. Auch sprechen die damit einhergehenden Risiken wie beispielsweise sogenannte „Enkeltricks" oder „Schockanrufe" bei älteren Mitbürger_innen gegen eine solche Veröffentlichung.

Nach sorgfältiger Prüfung mussten wir feststellen, dass keine gesetzliche Rechtsgrundlage für die – gedruckte oder digitale – Veröffentlichung existiert. Demnach bedarf die Veröffentlichung einer Einwilligung durch die betroffenen Personen.

Zulässig ist es allerdings, die Informationen über ein anstehendes Jubiläum zu verwenden um mit den Jubilaren in Kontakt zu treten, ihnen beispielsweise postalisch zu gratulieren und zu erfragen, ob die jeweilige Person mit einer Veröffentlichung einverstanden wäre. Mit § 50 Absatz 2 BMG hat der Gesetzgeber jedenfalls ein legitimes Interesse an einer Gratulation anerkannt. Wegen der oben genannten Gefahren empfehlen wir allerdings, auch bei Einwilligung in die Veröffentlichung weder die Anschrift noch das genaue Geburtsdatum mitzuveröffentlichen.

Eine gesetzliche Grundlage für die Veröffentlichung von Jubiläen im Amtsblatt gibt es also nicht mehr. Es ist jedoch dennoch möglich, auf diese Art und Weise öffentlich zu gratulieren, wenn die betroffene Person sich einverstanden erklärt. Es ist zulässig, dass der_die Bürgermeister_in die Daten aus dem Melderegister verwendet um zu gratulieren und nachzufragen, ob eine Veröffentlichung im Amtsblatt gewünscht ist.

9.1.6 Volkszählung / Zensus 2022

Mit einem Jahr Verzögerung aufgrund der Covid-19-Pandemie wird im Jahr 2022 wieder eine Volkszählung durchgeführt. Hierzu erreichten uns zahlreiche Beratungsanfragen von Bürger_innen, welche sich unsicher waren, ob sie überhaupt zur Auskunft verpflichtet sind oder welche Auskünfte sie ggf. erteilen müssen. Auch sind wir einigen konkreten Beschwerden nachgegangen und konnten diese überwiegend bereits abschließend klären. Wenige Erhebungsstellen mussten uns Datenpannen insbesondere im Zusammenhang mit der Arbeit der Erhebungsbeauftragten melden.

Die EU-Verordnung 763/2008 verpflichtet die Mitgliedstaaten, alle 10 Jahre eine Zählung der Bevölkerung durchzuführen, den sogenannten Zensus. Die letzte Volkszählung in Deutschland fand im Jahr 2011 statt. Wie schon bereits beim Zensus 2011 wird das Prinzip einer registergestützten Zählung für den Zensus 2022 beibehalten. Die Verfassungskonformität der registergestützten Erhebung wurde mit Urteil des Bundesverfassungsgerichts vom 19. September 2018 bestätigt. Stichtag für den Zensus 2022 war der 15. Mai. An diesem Tag wurde mit den Befragungen begonnen. Der Zensus wird vom Statistischen Bundesamt und den Statistischen Ämtern der Länder durchgeführt. Die Daten des Zensus unterliegen der statistischen Geheimhaltungspflicht. Für den Zensus 2022 hat der Gesetzgeber eine Auskunftspflicht festgelegt. Bei statistischen Erhebungen werden die Angaben nach den sogenannten Hilfs- und Erhebungsmerkmalen getrennt. Bei den Hilfsmerkmalen handelt es sich um diejenigen Angaben, die der Durchführung der Erhebung dienen (beispielsweise Name, Adresse), die Erhebungsmerkmale sind die Antworten zu den gestellten Fragen. Die Hilfsmerkmale sind von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren. Sie sind zu löschen, sobald die Überprüfung auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist. Eingeschränkt können im Rahmen des Zensus auch die Betroffenenrechte nach der DS-GVO beim Statistischen Landesamt Baden-Württemberg oder der jeweiligen Erhebungsstelle geltend gemacht werden.

Insgesamt können wir aus datenschutzrechtlicher Sicht ein positives Fazit zum Zensus 2022 in Baden-Württemberg ziehen, derzeit gibt es keinen Grund für datenschutzrechtliche Beanstandungen.

9.1.7 Viel Wirbel um Bodenrichtwertinformationssystem Baden-Württemberg (BORIS-BW) im Zuge der Grundsteuerreform

Die Grundsteuerreform bewegte im Jahr 2022 die Gemüter. Mit der Website www.grundsteuer-bw.de beabsichtigte die Finanzverwaltung eigentlich, den

Bürger_innen auf einfachste Weise die für die Erfüllung der Erklärungs- und Anzeigepflichten benötigten flurstücksbezogenen Daten in verschiedenen Portalen zur Verfügung zu stellen. Das Portal BORIS-BW sorgte jedoch bei etlichen Grundsteuerpflichtigen für Unmut, da über dieses Portal nicht nur die jeweiligen Grundstückseigentümer_innen Daten abrufen können, sondern für jedes Flurstück in Baden-Württemberg grundstücksbezogene Daten frei abrufbar, also ohne Einschränkung zugänglich sind. Uns erreichte daraufhin eine Beschwerdewelle.

Laut Finanzverwaltung soll es den Steuerpflichtigen ermöglicht werden, ohne den Gang aufs Amt ihre Steuererklärungen vollständig auszufüllen und elektronisch abzugeben. Dadurch sollen die örtlich zuständigen Finanz- und Vermessungsbehörden sowie die Gutachterausschüsse vor einer Vielzahl von Einzelanfragen der Steuerpflichtigen bewahrt werden.

Die Finanzverwaltung hatte uns in die Konzeption des Portals zur Veröffentlichung flurstücksbezogener Daten in beratender Funktion eingebunden. Bei BORIS-BW finden sich maßstabsgetreue grafische Darstellungen sämtlicher Flurstücke des Landes sowie deren Bebauung. Gibt man in die Suchmaske beispielsweise eine Adresse ein, so erscheint die Darstellung des entsprechenden Grundstücks und seiner näheren Umgebung. Die nunmehr eingegangenen Beschwerden bezogen sich ganz überwiegend darauf, dass darüber hinaus auch der für das Grundstück geltende Bodenrichtwert und die Fläche der Grundstücke auf den Quadratmeter genau öffentlich abrufbar sind.

Mit § 61 Absatz 3 Satz 1 des Landesgrundsteuergesetzes (LGrStG) wurde eine Rechtsgrundlage im Sinne von Artikel 6 Absatz 1 Buchstabe e, Absatz 2 und Absatz 3 der DS-GVO geschaffen, die die Finanzbehörden dazu ermächtigt, die für die Erklärungs- und Anzeigepflicht notwendigen flurstücksbezogenen Daten nach § 23 Absatz 1, § 31 sowie § 38 Absatz 2 LGrStG den Steuerpflichtigen elektronisch und öffentlich abrufbar bereitzustellen. Sowohl der Bodenrichtwert als auch die Grundstücksfläche sind für die Ermittlung der Grundsteuer erforderlich (vgl. § 38 Absatz 1 LGrStG). Unsere Prüfung hat ergeben, dass § 61 Absatz 3 Satz 1 LGrStG beide Werte umfasst.

Im Amtlichen Liegenschaftskatasterinformationssystem (ALKIS), das Bestandteil des von den unteren Vermessungsbehörden geführten Liegenschaftskatasters ist, sind die Flurstücke mit der Flurstücksfläche zu führen, die auf den Quadratmeter nachzuweisen ist. Die Flurstücksfläche wird den Vermessungsbehörden im Rahmen ihrer Vermessungsaufgaben und ihrer sonstigen im Vermessungsgesetz genannten Aufgaben bekannt. Bei der Flurstücksfläche handelt es sich um eine Geobasisinformation im Sinne von § 2 Absatz 1 Vermessungsgesetz (VermG). Aus § 2 Absatz 3 VermG ergibt sich, dass Geobasisinformationen auf Antrag übermittelt werden, soweit nicht eine Rechtsvorschrift eine Übermittlung oder Veröffentlichung von Amts wegen vorsieht. Lediglich für Angaben über die Grundstückseigentümer beziehungsweise Erbbauberechtigte ist die freie Zugänglichkeit von Geobasisinformationen eingeschränkt. § 23 Absatz 1 LGrStG sieht eine Übermittlung i. S. d. § 2 Absatz 3 VermG vor. Nach § 23 Absatz 1 LGrStG, auf den in § 61 Absatz 3 Satz 1 LGrStG Bezug genommen wird, haben die nach Bundes- oder Landesrecht zuständigen Behörden den Finanzbehörden die rechtlichen und tatsächlichen Umstände mitzuteilen, die ihnen im Rahmen ihrer Aufgabenerfüllung bekannt geworden sind und die für die Feststellung von Grundsteuerwerten oder für die Grundsteuer von Bedeutung sein können, was auf die Flurstücksfläche zutrifft (vgl. § 38 Absatz 1 LGrStG). Bei der Flurstücksfläche handelt es sich somit um ein für die Erklärungs- und Anzeigepflicht notwendiges flurstückbezogenes Datum, das den Steuerpflichtigen gemäß § 61 Absatz 3 Satz 1 LGrStG elektronisch und öffentlich abrufbar bereitgestellt werden kann.

Dass die gem. § 38 Absatz 2 LGrStG von den Gutachterausschüssen an die zuständigen Finanzbehörden zu übermittelnden Bodenrichtwerte ebenfalls von der Rechtsgrundlage erfasst werden, ergibt sich bereits unmittelbar aus der Verweisung auf § 38 Absatz 2 LGrStG in § 61 Absatz 3 Satz 1 LGrStG.

Die bei uns eingegangenen Beschwerden bezüglich BORIS-BW waren daher unbegründet. Aufsichtsrechtliche Maßnahmen, wie zum Teil von den Beschwerdeführenden gefordert, waren daher nicht angezeigt.

9.1.8 Zwischenbilanz für „Online-Petzportal" der Finanzverwaltung

Ein Jahr nach Einführung des Hinweisgeberportals der Oberfinanzdirektion Karlsruhe haben wir gemeinsam mit der Finanzverwaltung eine erste Bilanz aus datenschutzrechtlicher Sicht gezogen.

Im Sommer 2021 führte die Oberfinanzdirektion Karlsruhe das bundesweit erste anonyme Hinweisgebersystem für Finanzämter ein. Es soll Bürgerinnen und Bürgern einen „sicheren und anonymen Kommunikationsweg" bieten, „um Verstöße gegen Straf- und Steuergesetze anzuzeigen". Dank des anonymen Hinweisgebersystems könnten sie mit den baden-württembergischen Finanzämtern digital, sicher, diskret und anonym kommunizieren und Anzeigen von Steuerstraftaten oder sonstigen Verfehlungen gegen Steuergesetze melden. Zudem bestehe die Möglichkeit, über ein Postfach auch nach der Abgabe der Anzeige mit der zuständigen Steuerfahndungsstelle anonym zu kommunizieren (Ministerium für Finanzen Baden-Württemberg, Pressemitteilung vom 30.8.2021). Die Einführung wurde von der öffentlichen Debatte teilweise kritisch begleitet. So witterten manche Denunziantentum, während Steuerberater den Nutzen anzweifelten (FAZ vom 1.9.2021).

Im Rahmen des Austauschs mit Vertretern der Finanzverwaltung zu einer ersten Bilanz nach knapp einem Jahr Hinweisgebersystem haben wir erfahren, dass es zwar zunächst viele „Spaßhinweise" gegeben habe. Das habe sich aber zwischenzeitlich gelegt. Es würden etwa 200-250 Eingaben monatlich eingehen, was ungefähr der Anzahl der bisherigen Eingaben in Papierform entspreche. Inzwischen würden die Eingaben in Papierform deutlich abnehmen. Die strafrechtliche Verwertungsquote könne man aktuell noch nicht bewerten. Für die Speicherung würden Server des Landeszentrums für Datenverarbeitung bei der Oberfinanzdirektion Karlsruhe eingesetzt werden.

Da die Anonymität des Hinweisgebers gegenüber der Finanzverwaltung gewahrt werden und dennoch eine Kommunikation möglich sein soll, bedarf es besonderer technischer und organisatorischer Maßnahmen i. S. v. Artikel 32 der DS-GVO. Technische und organisatorische Maßnahmen sind unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu treffen, um ein angemessenes Schutzniveau im Hinblick auf die Sicherheit der Verarbeitung zu gewährleisten. Seitens der Finanzverwaltung wurden uns technische Dokumentationen, darunter eine Datenschutz-Folgenabschätzung (Artikel 35 DS-GVO) zur Prüfung vorgelegt. Während keine Mängel bezüglich der technischen und organisatorischen Maßnahmen festgestellt werden konnten, konnten wir im Hinblick auf die Dokumentation noch einige unterstützende Hinweise geben, die von der Finanzverwaltung dankbar aufgenommen wurden.

Ob das Hinweisgebersystem aus Sicht der Finanzverwaltung nun ein Erfolgsmodell oder einfach nur digital und damit zeitgemäß ist, können wir nicht bewerten. Probleme im Hinblick auf die Sicherheit der Verarbeitung, insbesondere die Wahrung der Anonymität der Hinweisgeber, bestehen aus unserer Sicht jedenfalls nicht.

9.2 Neues aus dem Amt: Gesundheits-, Sozial-und Bildungswesen

9.2.1 Die Bilddatei im Seniorenstift

Nicht nur Senior_innen fällt es manchmal schwer, sich Namen zu merken. Mit zunehmendem Alter lässt allerdings vielfach die Gedächtnisleistung nach, so dass es noch schwieriger werden kann, neue Inhalte zu erlernen und sie später zuverlässig wieder abzurufen. Vor diesem Hintergrund wandte sich ein Heimbewohner an uns mit der Frage, ob es gegen den Datenschutz verstoße, wenn in einem Seniorenheim eine Bilddatei angelegt werde, in die ein Foto der einzelnen Bewohner_innen zusammen mit Vor- und Nachname und die Appartement-Nr. aufgenommen werde. Eine solche Datei sollte dann allen Bewohner_innen zugänglich gemacht werden.

Wir verstanden die Frage zunächst so, dass das Seniorenstift diese Datei erstellen und verbreiten wolle. Deswegen wiesen wir darauf hin, dass dies mit einer ordentlichen Einwilligung der Abgebildeten datenschutzrechtlich zulässig sei. Mit der Einholung einer solchen Einwilligung für eine digitale Fotoanzeige oder eine Heimzeitung in der Verantwortung der

Heimleitung hatten wir uns beispielsweise schon im Zusammenhang mit unserem Beitrag „Datenschutz in der Pflege“ in unserem 34. Tätigkeitsbericht 2018 (S. 59 ff., insbesondere S. 61) und in unseren FAQ zum Datenschutz in der Pflege auseinandergesetzt.

Im weiteren Verlauf der Beratung stellte sich indes heraus, dass der anfragende Heimbewohner selbst diese Datei anlegen und die Fotos zugänglich machen wollte – möglicherweise, weil das Heim die Verantwortung zu übernehmen nicht bereit war. In dieser Konstellation stellte sich zunächst die Frage, ob für eine solche Betätigung überhaupt datenschutzrechtliche Anforderungen zu beachten sind, insbesondere ob eine solche Datenverarbeitung überhaupt unter die DS-GVO fällt.

Nach Artikel 2 Absatz 2 Buchstabe c DS-GVO findet die Verordnung nämlich keine Anwendung auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (auch sogenannten „Haushaltsausnahme“). Eine Definition der Begriffe „persönlich“ und „familiär“ enthält die DS-GVO hierzu nicht. Nach Erwägungsgrund 18 (der DS-GVO) gilt die Verordnung nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten und ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird. Von einer solchen rein familiären und privaten Verarbeitung konnten wir allerdings im konkreten Fall – unter anderem aufgrund der Größe des Seniorenstifts, in dem schon aufgrund der Vielzahl der Bewohner_innen mutmaßlich nicht alle untereinander Kontakt oder gar freundschaftliche Beziehungen pflegten – nicht mehr ausgehen.

Dies hatte aber nicht zur Folge, dass die geplante Datenverarbeitung nicht durchgeführt werden konnte. Als Rechtsgrundlage kommt auch bei Führung der Datei durch einen Mitbewohner des Heims hier eine Einwilligung der Bewohner_innen in Betracht. Allerdings hat diese den Anforderungen des Artikel 7 DS-GVO zu entsprechen. Insbesondere muss die Einwilligung auf freiwilliger Basis erfolgen, über das Widerrufsrecht informiert und der Widerruf gegebenenfalls auch tatsächlich ermöglicht werden. Besonders wichtig ist dabei in der der vorliegenden Konstellation, dass klargestellt wird, wer für die Verarbeitung der Daten (und damit beispielsweise auch für die Löschung im Falle des Widerrufs) verantwortlich ist, dass dies eben der betreffende Mitbewohner (und nicht etwa die Heimleitung) ist.

Die Frage, ob die Datenverarbeitung durch eine natürliche Person unter die DS-GVO fällt, ist nicht immer ganz einfach zu beantworten. Sofern dies zu bejahen ist, hat die Datenverarbeitung – zum Schutze der Personen, deren Daten verarbeitet werden – gewissen Anforderungen zu genügen. Hierbei beraten wir gern und geben Tipps.

Die DS-GVO sieht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person in Artikel 13 DS-GVO eine Informationspflicht vor. Ein für Vereine konzipiertes Muster dieser Informationspflicht (welches noch entsprechend anzupassen wäre) ist beispielsweise in unserem Praxisratgeber „Datenschutz im Verein nach der DS-GVO“ (auf unserer Internetseite abrufbar unter), Seite 12 ff., zu entnehmen. Darüber hinaus kann man sich auch durch unser Tool DS-GVO.clever unterstützten lassen, welches ebenfalls auf unserer Homepage steht. Auch sind wir unter anderem telefonisch, per E-Mail und über Mastodon erreichbar.

9.2.2 Datenpannen im Alltagsbetrieb

Die DS-GVO sieht in Artikel 33 eine Meldepflicht des Verantwortlichen vor. Danach hat der Verantwortliche eine „Verletzung des Schutzes personenbezogener Daten“ (also eine vielfach so bezeichnete „Datenpanne“) unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde zu melden. Unter einer Verletzung der Sicherheit des Schutzes von personenbezogenen Daten ist nach der Legaldefinition von Artikel 4 Nummer 12 DS-GVO eine Verletzung der Sicherheit zu verstehen, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Im Mittelpunkt einer Datenpanne steht also regelmäßig eine Verletzung der Datensicherheit.

Auch in diesem Jahr wurden uns zahlreiche Datenpannen gemeldet, die wir einer Überprüfung unterzogen haben. Dabei ist uns ein Verantwortlicher im Bereich

der Sozialversicherung besonders aufgefallen. Hier kam es in einem kurzen Zeitraum zu einer Häufung von gleichgelagerten Datenpannen. Hintergrund für das Vorliegen einer Datenpanne war dabei regelmäßig entweder ein Fehlversand von Dokumenten an einen falschen Empfänger oder ein Verlust von Dokumenten auf dem postalischen Versandweg. Hierbei besteht die Gefahr, dass ein unberechtigter Dritter eine Postsendung öffnet, personenbezogene Daten zur Kenntnis nimmt und diese etwa missbräuchlich verwendet. Diesen Umstand haben wir zum Anlass genommen, um von unseren aufsichtsrechtlichen Befugnissen nach Artikel 58 Absatz 1 Buchstabe b DS-GVO Gebrauch zu machen und eingehendere Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen. Im Zuge dessen haben wir uns an den Verantwortlichen gewandt und diesen zur Stellungnahme aufgefordert, um dadurch die internen Datenschutzprozesse im Bereich Postausgang und Versand genauer untersuchen zu können.

Denn nach Artikel 24 der DS-GVO trägt der Verantwortliche für die Verarbeitung von personenbezogenen Daten die Verantwortung.

Den Verantwortlichen trifft also nicht nur unter bestimmten Voraussetzungen eine Melde-, Benachrichtigungs- und Dokumentationspflicht nach Artikel 33 und 34 DS-GVO, sondern er hat darüber hinaus bei der Verarbeitung von personenbezogenen Daten präventiv die Umsetzung geeigneter technischer und organisatorischer Maßnahmen nach Artikel 24 und 25 DS-GVO sicherzustellen. Hierzu gehört auch, dass der Verantwortliche nach Artikel 32 DS-GVO die Datensicherheit, also vor allem den Schutz der Daten vor Verlust, Schädigung und Missbrauch, gewährleistet. Ob die Maßnahmen des Verantwortlichen allerdings geeignet sind, hängt vor allem neben der Art der Datenverarbeitung auch von dem jeweiligen Einzelfall ab. Es bedarf also grundsätzlich eines umfassenden Datenschutzmanagements, durch welches eine regelmäßige Überprüfung der Tauglichkeit der implementierten technisch-organisatorischen Maßnahmen gewährleistet werden kann.

Ein besonderes Augenmerk ist insbesondere auch dann auf die Einhaltung hoher Sicherheitsstandards zu legen, wenn es sich um Sendungen handelt, die besondere Kategorien von personenbezogenen Daten nach Artikel 9 Absatz 1 DS-GVO, beispielsweise Gesundheitsdaten, oder aber Sozialdaten gemäß § 67 Absatz 2 SGB X umfassen. In unserem Fall waren sowohl Gesundheits- als auch Sozialdaten als besonders geschützte Datenkategorien betroffen.

Mit Blick auf den Postausgang und den Versand ist regelmäßig vor allem darauf zu achten, dass mit einem hinreichenden Postausgangsmanagement sowie angemessener Verpackung alle spezifischen Maßnahmen ergriffen werden, um eine Verarbeitung im Sinne der DS-GVO sicherzustellen. Dies beinhaltet neben

Impftermine können jetzt auch online gebucht werden.

der ordnungsgemäßen Sortierung von ausgedruckten Dokumenten, z. B. durch farbige Trennblätter, insbesondere auch die Sicherstellung der korrekten Zuordnung der Dokumente zu einem adressierten Kuvert. Hierfür sind turnusmäßige Stichproben beispielsweise durch Kontrollwägungen vorzunehmen. Auch die stetige Sensibilisierung der Mitarbeitenden im Bereich des Postversands ist unabdingbar.

Für den Verlust auf dem Postweg selbst ist bei Auswahl eines vertrauenswürdigen Dienstleisters eine Verantwortlichkeit im Sinne der DS-GVO zwar regelmäßig nicht gegeben. Denn der Dienstleister wird bei der Beförderung von Postsendungen regelmäßig nicht als Auftragsverarbeiter im Sinne von Artikel 28 DS-GVO eingesetzt, sondern handelt als selbstständig Verantwortlicher. Dies entlässt einen Versender von Dokumenten mit sensiblen Inhalten jedoch nicht aus der bereits oben aufgezeigten Verantwortung, bis zur Übergabe der Sendungen angemessene Maßnahmen zu ergreifen. Des Weiteren kann es durchaus angebracht sein, auch Maßnahmen zu ergreifen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind. In diesem Fall kann beispielsweise die Inanspruchnahme einer Sendungsverfolgung angezeigt sein.

Insgesamt ist festzuhalten, dass der Schutz von betroffenen Personen vor einer beeinträchtigenden Datenverarbeitung – z. B. in Form von Datenpannen – nur dann sichergestellt werden kann, wenn die Anforderungen der DS-GVO eingehalten und umgesetzt werden. Demzufolge hat der Verantwortliche auch den Nachweis dafür zu erbringen, dass er alles Erforderliche unternommen hat, um dieses Ziel zu erreichen, vgl. Artikel 24 Absatz 1 Satz 1 DS-GVO. Der Fall zeigt, dass es einer stetigen Überprüfung der eingehenden Datenpannenmeldungen nicht nur im Einzelfall bedarf. Vielmehr müssen darüber hinaus frühzeitig Regelmäßigkeiten und Zusammenhänge erkannt werden, um so etwaige systematische Fehler im Datenschutzmanagement aufzeigen zu können. Gerade dafür ist aber wichtig, dass uns auch scheinbar alltägliche Datenpannen wie ein Fehlversand von personenbezogenen Daten gemeldet werden. Denn nur dann können wir derartige Häufungen feststellen, die einen Hinweis auf zugrundeliegende systematische Fehler darstellen könnten.

Auch zukünftig wird es daher neben der Beratung von Verantwortlichen unsere Aufgabe sein, Datenpannenmeldungen zu analysieren und ggf. etwa bei auffälligen Häufungen Datenschutzüberprüfungen im Einzelfall durchzuführen.

9.2.3 Terminvergabetool Impfen

Im August 2022 legte uns das Sozialministerium Baden-Württemberg seine Vorstellung dar, dass im Land ab dem 1. September 2022 die Termine für eine Corona-Schutzimpfung bei allen Leistungserbringern i.S.v. § 3 Abs. 1 S. 1 CoronaImpfV über ein gemeinsames, durch das Ministerium für Soziales, Gesundheit und Integration bereitgestelltes Online-Terminvergabe-Tool buchbar sein sollen. Mit Hilfe des Online-Tools sollen, so das Ministerium, die für den Herbst 2022 prognostizierten 6,5 Millionen Impfungen, das heißt 810.000 Impfungen pro Woche, effizient und gerecht abgewickelt werden. Gleichzeitig intendiere das Ministerium, anhand des Tools ein landesweites Impfmonitoring zu etablieren, um Kapazitätsengpässe und eventuelle Handlungsbedarfe frühzeitig zu erkennen. Menschen, die keinen Zugang zum Internet haben, sollten weiter telefonisch Impftermine buchen können. Dabei sollte ein Produkt eines bestimmten E-Health Unternehmens genutzt werden.

Trotz der leider sehr späten Beteiligung unserer Behörde haben wir das Sozialministerium unter dem entsprechenden Zeitdruck zu den grundlegenden datenschutzrechtlichen Fragen beraten können. Wir machten deutlich, dass wir, anders als zunächst das Sozialministerium, keine datenschutzrechtliche Verantwortung dieses Ministeriums sehen und stattdessen die jeweiligen Leistungserbringer als datenschutzrechtlich Verantwortliche im Sinne des Artikels 4 Nummer 7 DS-GVO betrachten. Zudem konnten wir dem Ministerium noch Hinweise geben, so zum Beispiel zu der Frage ob die Leistungserbringer jeweils Auftragsverarbeitungsverträge mit dem ausgewählten E-Health-Unternehmen abschließen müssten oder ob sich das über die Kassenärztliche Vereinigung Baden-Württemberg und involvierte Verbände bündeln ließe. Unsere Antwort dazu: Die nach Artikel 28 DS-GVO gebotenen Verträge sollten in rechtlicher Hinsicht jeweils zwischen dem Leistungserbringer einerseits und der den Internetdienst betreibenden zustandekommen.

Bestimmte Möglichkeiten der Bündelung, etwa das Bereitstellen eines Vertragsmusters auf einer zentralen Plattform, verbunden unter anderem mit sachdienlichen Hinweisen für dessen Handhabung, etwa hinsichtlich der gebotenen Anpassung des Mustertexts an die jeweils relevanten Umstände, sind aber datenschutzrechtlich ohne weiteres möglich.

Darüber hinaus konnten wir noch empfehlen, dass bei allen beteiligtem Webseiten und Apps in jedem Fall unsere Tracking-FAQ beachtet werden sollte (siehe auch Kapitel 9.4.2), was am besten vertraglich festgehalten werden sollte.

Im Verlauf des September 2022 konnte das Impfportal schließlich gestartet werden. Es ist über den Link www.impftermin-bw.de/ nutzbar. Auch wenn wir eine frühere Einbeziehung durch das Sozialministerium für sinnvoll erachtet hätten und wir infolge der Kurzfristigkeit die Ausführung nicht ins Detail begleiten konnten, so gelang es uns doch dabei zu helfen, dieses digitale Angebot datenschutzrechtlich tragfähig zu gestalten.

☛ Mehr Informationen:

Unsere Tracking-FAQ: www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2

Zum Start des Impfportals für BW: sozialministerium.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/impfterminportal-fuer-baden-wuerttemberg-gestartet

„SORMAS: 2021 immer noch kein Erfolgsmodell", Beitrag aus unserem Tätigkeitsbericht 2021: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2022/02/22020225_Taetigkeitsbericht_TB-Datenschutz_2021_V1.pdf

Zur länger zurückliegenden Vorgeschichte von SORMAS, Beitrag „Die Digitalisierung des (öffentlichen) Gesundheitswesens zur Pandemiebekämpfung" in unserem Tätigkeitsbericht 2020: www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Ta%CC%88tigkeitsbericht_2020_WEB.pdf

9.2.4 SORMAS

Das in unserem 37. Tätigkeitsbericht zum Datenschutz unter Nummer 1.3 und der Überschrift „1.3 SORMAS: 2021 immer noch kein Erfolgsmodell" recht kritisch beschriebene Verfahren hat 2022, jedenfalls aus Sicht der Datenschutzaufsichtsbehörden, ein letztlich dann noch zufriedenstellendes Ende gefunden. Unsere Behörde hat im Rahmen der sogenannten SORMAS-Arbeitsgruppe (AG SORMAS, ein Forum unter Beteiligung des Helmholtz-Zentrums für Infektionsforschung [HZI] und anderer Akteure auf Projektträgerseite, des Bundesministeriums für Gesundheit, des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie einiger, weniger Landesdatenschutzbehörden) die intensive Beratung des HZI zum elektronischen Verfahren SORMAS („Surveillance Outbreak Response Management and Analysis System"), das der Vereinfachung und Verbesserung der Kontaktnachverfolgung durch Gesundheitsämter dienen soll, abgeschlossen. Gravierende datenschutzrechtliche Probleme, die eine Anwendung von SORMAS zwingend gehindert hätten, können somit als nicht (mehr) vorhanden betrachtet werden.

Für das Ende der datenschutzrechtlichen Beratung durch die SORMAS AG war unter anderem von Bedeutung, dass die Förderung des (Forschungs-) Projektes SORMAS@DEMIS durch das Bundesministerium für Gesundheit zum 31. Dezember 2022 ausgelaufen ist. Die bereits im Sommer 2022 gegründete gemeinnützige SORMAS-Stiftung (SORMAS Foundation) soll ab Januar 2023 die Bereitstellung und Weiterentwicklung von SORMAS unterstützen soll, SORMAS künftig, jedenfalls ab Juli 2023, von einer GmbH (wohl als Auftragsverarbeiter i.S.d. Artikels 4 Nummer 8 DS-GVO) betrieben werden, welche, ebenso wie die SORMAS Foundation, der Datenschutzaufsicht der Landesbeauftragten für den Datenschutz Niedersachsen unterliegt.

Es bleibt nun abzuwarten, ob und gegebenenfalls welche baden-württembergischen Gesundheitsämter auf das ihnen unterbreitete Angebot der kostenpflichtigen Nutzung von SORMAS eingehen. Einer solchen (weiteren) Nutzung von SORMAS durch baden-württembergische Gesundheitsämter stehen, wie oben erwähnt, keine generellen datenschutzrechtlichen Hindernisse im Weg. Selbstverständlich müssen die mit einer solchen daten-

schutzrechtlichen Verantwortung verbundenen Pflichten erfüllt werden. Wir gehen bislang davon aus, dass dies gelingen kann, bei Bedarf etwa auch unter Nutzung des den Gesundheitsämtern in Gestalt der behördlichen Datenschutzbeauftragten eigenen Expertise. Selbstverständlich beraten auch wir bei Bedarf die Gesundheitsämter.

Bei eventuellen Entscheidung, SORMAS (weiter) zu nutzen oder nicht, sind baden-württembergische Gesundheitsämter inzwischen frei. Der Lenkungskreis Vereinbarung Digitales Gesundheitsamt (Vb. DiGA) hat in seiner Sitzung am 6. Oktober 2022 zu SORMAS unter anderem beschlossen:

„Der Lenkungskreis stellt fest, dass wichtige bidirektionale Schnittstellen weiterhin seitens des Bunds und des SORMAS@DEMIS-Konsortiums nicht geschaffen wurden und SORMAS somit derzeit noch keine technisch funktionssichere Anbindung zu den in den Gesundheitsämtern genutzten Meldesystemen und übrigen Fachanwendungen bietet. Der Beschluss des Lenkungskreises wird deswegen wie folgt modifiziert: die Verpflichtung der Gesundheitsämter in Baden-Württemberg, SORMAS technisch installiert zu haben, entfällt."

Das Sozialministerium hat nach eigener Darstellung die Erkenntnisse aus der Einführung von SORMAS aufgearbeitet und will diese ins Großprojekt „Digitalisierung des ÖGD BW" einfließen lassen. Dies ist sicher sinnvoll und kann dazu beitragen, dass künftige Digitalisierungsbemühungen schneller zum Erfolg führen. Wir fänden es sehr sinnvoll, wenn künftig Digitalisierung im Gesundheitswesen besser – nämlich zügiger und unter frühzeitiger Berücksichtigung datenschutzrechtlicher Aspekte einschließlich der Einhaltung der hierfür erforderlichen Dokumentationspflichten – läuft, als bei der SORMAS-Einführung unter der maßgeblichen Beteiligung des HZI und des Bundesgesundheitsministeriums. Wir werden das Sozialministerium bei seinen weiteren Digitalisierungsbestrebungen gerne mit unserer datenschutzrechtlichen Expertise unterstützen.

9.3 Neues aus dem Amt: Privatwirtschaft

9.3.1 Homeoffice in Drittstaaten

Die Corona Pandemie hat in den vergangenen drei Jahren für viele Beschäftigte – auch in unserer Dienststelle – Möglichkeiten eröffnet, von zu Hause und unterwegs aus zu arbeiten, von denen noch unmittelbar davor der Großteil der betroffenen Arbeitnehmer_innen nicht einmal zu träumen wagte. Allerdings führte dieser Umstand auch zu datenschutzrechtlichen Herausforderungen.

Mehrfach erreichten uns im Berichtszeitraum Beratungsanfragen dazu, welche datenschutzrechtlichen Vorgaben für Beschäftigte deutscher Unternehmen gelten, die im Homeoffice in einem Drittstaat außerhalb der EU und des europäischen Wirtschaftsraums (EWR) tätig sind.

Zum Teil wurde der Wunsch danach, die Arbeit von zu Hause aus in einen Drittstaat zu verlegen, damit begründet, auf diese Weise an der Betreuung von Angehörigen mitwirken zu können. Außerdem wurde darauf verwiesen, dass der Europäische Datenschutzausschuss (EDSA / EDPB) erst kürzlich den Fluss personenbezogener Daten innerhalb ein und desselben Verantwortlichen – also etwa den Fall, dass ein reisender Mitarbeiter Datenträger mit personenbezogenen Daten in ein Drittland mitnimmt oder von dort über einen Fernzugriff auf personenbezogene Daten in der EU zugreift – von den Regelungen des Kapitels 5 der DS-GVO ausgenommen habe. Dasselbe müsse gelten, wenn der Mitarbeiter im Rahmen einer im Drittstaat ausgeübten Homeoffice-Tätigkeit auf personenbezogene Daten in der EU zugreife, sodass auch in solchen Fällen die Vorgaben des Kapitels 5 der DS-GVO nicht zu beachten und die üblichen technischen und organisatorischen Maßnahmen wie beispielsweise eine Transportverschlüsselung und Sicherung von PCs durch Passwörter ausreichend seien.

Die Richtlinie 05/2021 des EDSA vom 18.11.2021 über das Zusammenspiel von Art. 3 und Kapitel 5 der DS-GVO unternimmt den Versuch, den Begriff des Transfers i.S.v. Art. 44 ff. DS-GVO näher einzugrenzen und enthält dabei unter anderem auch unter Randziffer 14 die Vorgabe, wonach ein Datenfluss aus Europa in einen Drittstaat keinen Transfer im Sinne des Kapitels 5 der DS-GVO darstellt, wenn Importeur und Exporteur Bestandteil desselben Verantwortlichen oder Auftragsverarbeiters sind.

Allerdings ist der Transferbegriff auch zwischen den Aufsichtsbehörden weiterhin in der Diskussion; die Arbeitsgruppe „Internationaler Datentransfer" des

EDSA arbeitet derzeit an einer neuen Definition des Transferbegriffs, die auch für Zweifelsfälle wie rechtlich unselbständige Niederlassungen eines Verantwortlichen oder Dienstreisen Rechtsklarheit bringen soll. Ein vollständiger Ausschluss aller Datenbewegungen innerhalb ein und desselben Verantwortlichen oder Auftragsverarbeiters von den Vorgaben über den Drittstaatentransfer wird zumindest von den deutschen Datenschutzaufsichtsbehörden mehrheitlich nicht geteilt, weil dies zur Folge hätte, dass personenbezogene Daten in Drittstaaten speziellen Risiken unterworfen werden könnten, ohne dass beispielsweise der Betroffene hierüber gemäß Artikel 13 beziehungsweise 14 DS-GVO ausreichend informiert werden müsste, so dass er faktisch keine Möglichkeit zum Widerspruch hätte.

Unterhält ein Verantwortlicher mit Sitz in der EU in einem Drittstaat eine rechtlich unselbstständige Niederlassung, in der personenbezogene Daten, die aus der EU stammen, verarbeitet werden, würden wir derzeit von einem Transfer personenbezogener Daten ausgehen. Gleiches gilt nach unserer Auffassung für mobiles Arbeiten, zumindest wenn dieses über einen längeren Zeitraum mit einer gewissen Regelmäßigkeit am selben Ort im Drittstaat erfolgt und sobald ein Zugriff auf personenbezogene Daten aus der EU durch den Mitarbeiter im Drittstaat tatsächlich stattfindet (beispielsweise durch Abruf / Fernzugriff) beziehungsweise wenn solche Daten auf Geräten im Drittstaat gespeichert sind oder in sonstiger Weise verarbeitet werden; das gilt unabhängig davon, ob es sich bei der datenverarbeitenden Stelle im Drittstaat um einen selbständigen Verantwortlichen, eine Niederlassung oder einen sonstigen unselbständigen Teil des Verantwortlichen mit Hauptsitz in der EU, der als Exporteur fungiert, handelt.

Das bedeutet, dass in solchen Fällen zusätzlich zu angemessenen technischen und organisatorischen Maßnahmen die Voraussetzungen eines Transferinstruments nach Kapitel 5 der DS-GVO erfüllt sein müssen. Bei einem Transfer innerhalb ein und desselben Verantwortlichen könnten zu diesem Zweck beispielsweise die Vorgaben der Standardvertragsklauseln der EU-Kommission für den Drittstaatentransfer durch eine einseitige Garantieerklärung des Verantwortlichen verbindlich gemacht und auf diese Weise Drittbegünstigtenrechte für die Betroffenen geschaffen werden. Ein solcher Transfer bedarf dann nicht der Genehmigung der Datenschutzaufsichtsbehörde. Allerdings ist zu beachten, dass nach dem Schrems II-Urteil des EuGH ein Transfer in Drittstaaten eine Analyse des Rechts des Drittstaats in Bezug auf den Zugriff auf personenbezogene Daten durch staatliche Stellen und den hiergegen möglichen Rechtsschutz Betroffener in der EU voraussetzt (vgl. näher hierzu die Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten des EDSA vom 18. Juni 2021 sowie die Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen des EDSA vom 10. November 2020). Ein solches sogenanntes „transfer impact assessment" ist danach auch in den Fällen des Homeoffice im Drittstaat zu verlangen, es sei denn, für den betroffenen Drittstaat existiert eine Angemessenheitsentscheidung der Europäischen Kommission. Das ist bislang für folgende Länder der Fall: Vereinigtes Königreich, Israel, Argentinien, Japan, Andorra, Guernsey, Isle of Man, Jersey, Kanada, Neuseeland, Schweiz, Färöer Inseln, Republik Korea (Südkorea) und Uruguay.

Homeoffice deutscher Arbeitnehmer in Drittstaaten außerhalb der EU wird durch das Datenschutzrecht nicht ausgeschlossen. Wenn die Tätigkeit mit einem Zugriff auf aus der EU stammende personenbezogene Daten einhergeht, sind allerdings – zusätzlich zu geeigneten technischen und organisatorischen Maßnahmen – die Vorgaben des Kapitels 5 der DS-GVO zu beachten. Mit Ausnahme derjenigen Länder, für die die Europäische Kommission ein im wesentlichen gleichwertiges Datenschutzniveau attestiert hat, ist damit ein auf den jeweiligen Einzelfall zugeschnittenes „transfer impact assessment" erforderlich, in dem die besonderen Risiken, denen die Daten außerhalb der EU ausgesetzt sind, untersucht werden.

9.3.2 Zwei Seiten einer Medaille: Aufbewahrungspflichten nach Handels- und Steuerrecht

Während Bürger_innen relativ häufig rügen, dass Unternehmen ihre personenbezogenen Daten zu lange speichern, kommt es doch auch zuweilen vor, dass betroffene Personen sich über die vorzeitige Löschung ihrer Daten beschweren. Beide Sachverhalte berühren den Datenschutz in unterschiedlicher Weise.

Ein Bankkunde stritt mit seiner Bank über mehrere Jahre über zurückliegende Sachverhalte aus seiner

Kontoverbindung. Er bestritt, einer angehörigen Person damals vorübergehend, wie von der Bank behauptet, eine Kontovollmacht erteilt zu haben und forderte von der Bank die Vorlage des Vollmachtsnachweises. Die Bank blieb diesen Nachweis schuldig, da die entsprechenden Unterlagen inzwischen wegen Zeitablaufs der Aufbewahrung entzogen und vernichtet worden waren. Daraufhin wandte sich der Bankkunde an uns und rügte, dass die Bank durch die Löschung des Vollmachtsnachweises ihre handels- und steuerrechtlichen Aufbewahrungspflichten verletzt habe.

Ungeachtet der Frage, wann die einschlägigen Aufbewahrungsfristen im konkreten Fall beginnen und enden, ist aus datenschutzrechtlicher Sicht zum Vorwurf einer Verletzung der Aufbewahrungspflichten Folgendes festzustellen: Angaben zu Kontovollmachten weisen u.a. einen Bezug zur_zum jeweiligen Kontoinhaber_in auf und sind daher personenbezogen. Sowohl bei der Speicherung als auch bei der Löschung dieser Daten handelt es sich mithin um eine Verarbeitung personenbezogener Daten i.S. der DS-GVO. Für beides bedarf es daher einer rechtlichen Grundlage gemäß Artikel 6 Absatz 1 DS-GVO. Wenn die Bank nicht nach Artikel 17 DS-GVO zur Löschung der Daten verpflichtet ist, kann als Rechtsgrundlage für eine (freiwillige) Löschung allenfalls Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO in Betracht kommen. Hiernach ist die Verarbeitung personenbezogener Daten (also auch deren Löschung) rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich sind, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen.

Ein berechtigtes Interesse an der Löschung dürfte für die Bank jedoch ausscheiden, wenn die Unterlagen, in denen die Daten enthalten sind, beispielsweise nach § 257 des Handelsgesetzbuchs und § 147 der Abgabenordnung aufbewahrungspflichtig und die in diesen Vorschriften normierten Aufbewahrungsfristen noch nicht abgelaufen sind. Unter diesen Voraussetzungen kann sich die Bank nach Artikel 17 Absatz 3 Buchstabe b DS-GVO erst recht nicht auf eine datenschutzrechtliche Löschpflicht berufen.

Folglich ist also weder die Über-, noch die Unterschreitung gesetzlicher Aufbewahrungsfristen mit der DS-GVO vereinbar. Was bedeutet das nun für die betroffene Person? Diese kann sich gem. Artikel 77 Absatz 1 DS-GVO bei einer Aufsichtsbehörde beschweren, wenn sie *„der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen (die DS-GVO) verstößt“*. Dieser dem Wortlaut nach sehr weite Anwendungsbereich erfährt eine signifikante Einschränkung durch Erwägungsgrund 141 Satz 1 Variante 1 zur DS-GVO. Danach sollte jede betroffene Person die Möglichkeit zur Einreichung einer Beschwerde haben *„wenn sie sich in ihren Rechten gemäß (der DS-GVO) verletzt sieht“*.

Maßgeblich dafür, ob die vorzeitige Löschung die betroffene Person in ihren Rechten verletzen kann, ist der Schutzzweck der gesetzlichen Aufbewahrungspflichten. Die diesbezüglichen handels- und steuerrechtlichen Bestimmungen dienen allerdings regelmäßig nicht den Beweisführungsinteressen der Kontoinhaberin oder des Kontoinhabers, sondern dem Schutz der ordnungsgemäßen Buchführung als Grundvoraussetzung jeder ordnungsgemäßen Wirtschaftsführung. Als Kaufmann im handelsrechtlichen Sinn ist die Bank nach § 238 Absatz 1 Satz 1 des Handelsgesetzbuchs verpflichtet, Bücher zu führen und in diesen ihre Handelsgeschäfte und die Lage ihres Vermögens nach den Grundsätzen ordnungsmäßiger Buchführung ersichtlich zu machen. Dies dient dem Schutz des Wirtschaftsverkehrs. Zudem soll die Aufbewahrung vom Unterlagen nach der Abgabenordnung eine ordnungsgemäße Besteuerung sicherstellen. Eine datenschutzrechtliche Rechtsverletzung der betroffenen Person ist daher bei einer vorzeitigen Datenlöschung zu verneinen.

Im Ergebnis steht einer betroffenen Person eine datenschutzrechtliche Beschwerdebefugnis nur gegen eine Überschreitung handels- und steuerrechtlicher Aufbewahrungspflichten, nicht aber gegen deren Unterschreitung zu. Unbeschadet dieser Rechtslage werden wir die Unternehmen im Land auch künftig bei der Einhaltung der gesetzlichen Aufbewahrungspflichten unterstützen.

9.3.3 Ein Funktionspostfach löst Probleme

Um mehr Bürgernähe zu ermöglichen und das Verwaltungshandeln transparenter zu gestalten, veröffentlichte ein Landrat die Namen, Vornamen und die Funktionsbezeichnung seiner Beschäftigten auf

der Internetseite seines Landratsamts. Die Bürger_innen des Landkreises sollten sich direkt an die Person wenden können, die im Internet als zuständige diensthabende Person benannt ist.

Grundsätzlich sind die Offenheit und Transparenz des Landratsamts sehr zu begrüßen, doch ging bei uns eine anonyme Beschwerde ein. Ergebnis unserer Prüfung: Wir mussten den Landrat darauf hinweisen, den Beschäftigtendatenschutz zu berücksichtigen und für die Mehrheit seiner Beschäftigten Funktionspostfächer einzurichten.

Für Beschäftigte des Landes gilt § 15 Abs. 1 S.1 Landesdatenschutzgesetz (LDSG):

„Personenbezogene Daten von…Beschäftigten dürfen verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des jeweiligen Dienst- oder Arbeitsverhältnisses erforderlich (…) ist."

Bei Veröffentlichungen im Internet ist stets zu bedenken, dass diese Daten weltweit einem unbeschränkten Personenkreis zur Verfügung gestellt werden. Moderne Informations- und Kommunikationstechniken bieten vielfältige Möglichkeiten, personenbezogene Daten zielgerichtet auszuwerten und zu verarbeiten. Durch eine Veröffentlichung im Internet kann das Recht auf informationelle Selbstbestimmung aus einer möglichen Verknüpfung von Angaben einzelner Personen mit Informationen aus anderen Datenbeständen stärker berührt werden. So können umfassende Persönlichkeitsprofile entstehen. Dies sollten öffentliche Stellen bei ihren Entscheidungen, Daten ihrer Beschäftigten im Internet zu veröffentlichen, stets berücksichtigen.

Eine Veröffentlichung von Personaldaten im Internet ist aus datenschutzrechtlicher Sicht somit nur zulässig, wenn die Betroffenen eingewilligt haben oder ohne Einwilligung der Betroffenen, wenn der Dienstverkehr es erfordert (§ 15 LDSG).

☛ Mehr Informationen:

Weitere Hinweise zum Beschäftigtendatenschutz:
www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/Ratgeber-Besch%C3%A4ftigten-datenschutz.pdf

Die Mitarbeitenden sind darauf hinzuweisen, dass sie ihre Einwilligung mit Wirkung für die Zukunft jederzeit widerrufen können. Unter Umständen ist auch der Personalrat zu beteiligen.

Die Veröffentlichung dieser Daten ist auch ohne Einwilligung zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegenden Aufgaben erforderlich ist und die Daten im Rahmen der in § 15 LDSG genannten Zweckbindung verarbeitet werden dürfen.

Die Veröffentlichung von personenbezogenen Daten im Internet kann als erforderlich angesehen werden bei Personen, deren Tätigkeit nach außen wirkt (beispielsweise Behördenleitung, Abteilungs- und Referatsleitungen, Pressesprecher_innen, Ansprechpersonen für Projekte mit Bürgerbeteiligung). Ohne deren Einwilligung können folgende Daten veröffentlicht werden: Name, Vorname (s. u.), Tätigkeitsbereich (Behördenbezeichnung, Organisationseinheit), Adresse der Dienststelle, dienstliche Telefon- und Telefaxnummer sowie dienstliche E-Mail-Adresse.

Ob der Dienstverkehr die Bekanntgabe von Namen und weiterer Daten sonstiger Mitarbeitenden im Internet erfordert, bedarf der Abwägung im Einzelfall. Derartige Entscheidungen sind aktenkundig zu machen. Bei der Verhältnismäßigkeitsprüfung sollten seitens des Dienstherrn folgende Aspekte berücksichtigt werden:

a. Durch die Angabe von Namen/Vornamen wird es Dritten erleichtert, unter Nutzung weiterer frei zugänglichen Datenbestände (z. B. Telefonbücher) Mitarbeitende zu identifizieren und diese eventuell zu belästigen oder zu bedrohen. So wird medial immer wieder über Stalking oder über Gewalttätigkeiten gegen Beschäftigte des öffentlichen Dienstes berichtet. Die für Organisationsangelegenheiten zuständigen Stellen sind gehalten, zwischen den Interessen der Öffentlichkeit an der namentlichen Nennung der einzelnen Bediensteten und der Fürsorgepflicht des Dienstherrn im Hinblick auf die Sicherheit der Bediensteten abzuwägen.

b. Die Zahl der in letzter Zeit rapide zugenommenen Spams an im Internet namentlich benannte Beschäftigten-Mail-Adressen kann ganze Serverbereiche zum Erliegen bringen.

Aus unserer Sicht sollte die Angabe der Namen und Vornamen von Mitarbeitenden, die nicht in den eben genannten Aufgabenbereichen mit Außenwirkung tätig sind, im Internet vermieden werden. Allgemein gehaltene Kontaktadressen, sogenannte Funktionsadressen wie beispielsweise „Bürgerbüro“, „Servicestelle“, „Poststelle“ oder „…amt“ oder die allgemeine Funktionsbezeichnung und die telefonische Durchwahlnummer der Bediensteten reichen für eine erste Kontaktaufnahme von Bürger_innen zur Verwaltung regelmäßig aus.

9.4 Neues aus dem Amt: Technisch-organisatorischer Datenschutz

9.4.1 Ransomware-Angriffe bleiben eine Bedrohung

Auch in diesem Jahr gab es zahlreiche Ransomware-Angriffe auf Unternehmen und öffentliche Einrichtungen. Bei Ransomware-Angriffen werden, nachdem Angreifer die Kontrolle über fremde Server übernommen haben, zumeist alle Daten auf Servern der Verantwortlichen zuerst von Kriminellen kopiert und anschließend auf den Servern der Verantwortlichen verschlüsselt. Ohne Information über den Schlüssel besteht dann kein Zugriff mehr. Zusätzlich kommt es zu einer Geldforderung für die Herausgabe des Schlüssels, außerdem wird bei Nichtbezahlung mit der Veröffentlichung der gekaperten Daten gedroht. Wir beobachten dabei eine stetige Professionalisierung der Erpresserbanden, beispielsweise haben einige Gruppen bereits seit längerem Franchisekonzepte eingeführt oder bieten Ransomware-as-a-Service als eine auch von Laien mietbare IT-Dienstleistung an. Nun wurde zusätzlich ein Bug-Bounty Programm, zum Finden von Schwachstellen in der eigenen Verschlüsselungssoftware aufgelegt, sodass Erpresserbanden eine Art Provision zahlen, wen ihnen und nicht anderen gesagt wird, wo eine Lücke in der Schadsoftware selbst ist.

Die Angriffe haben im Berichtszeitraum auch Kommunen in Baden-Württemberg getroffen. Gerade auch kleinere Kommunen standen, ob den Kriminellen bewusst oder unbewusst, im Fokus. Durch die drohende Veröffentlichung und den daraus entstehenden Schäden ist ein konzentriertes und fokussiertes Handeln von verantwortlichen Stellen nötig.

Im Beratungsalltag werden wir häufig nach dem richtigen Vorgehen gefragt, sofern personenbezogene Daten betroffen sind. Aus unserer Sicht ist in den meisten Fällen ein abgestuftes Verfahren sinnvoll. Grundsätzlich sieht die DS-GVO einen dreistufigen Aufbau von Prüfungen bei Datenpannen vor (siehe Art. 33, 34 DS-GVO): Prüfung ob eine Verletzung des Schutzes personenbezogener Daten vorliegt, anschließende Bewertung des Risikos für betroffene Personen und drittens die Entscheidung über die Meldung an die Aufsichtsbehörde und gegebenenfalls die Benachrichtigung betroffener Personen.

Zunächst ist die Verletzung des Schutzes von personenbezogenen Daten festzustellen. Eine Verletzung des Schutzes von personenbezogenen Daten ist in Artikel 4 Nr. 12 DS-GVO definiert. Nötig ist eine Verletzung der Sicherheit, die u. A., der unbefugten Zugang zu personenbezogenen Daten führt. Möglich ist aber auch der Verlust von Daten. Somit kann eine Verletzung des Schutzes von personenbezogenen Daten auch ohne eine unbefugte Offenlegung darin liegen, dass die Verfügbarkeit der Daten verloren geht – ein Punkt der häufig von Verantwortlichen übersehen wird.

Nach der Feststellung der Verletzung ist das Risiko für die Rechte und Freiheiten der betroffenen Personen ausführlich und vollumfassend zu bewerten. Diese Bewertung dient dazu, dass im Anschluss geeignete Maßnahmen getroffen werden können. Das Risiko ergibt sich dabei zumeist einerseits aus der Eintrittswahrscheinlichkeit des Schadens und andererseits aus der Schwere des Schadens. Beide Faktoren fließen in die Bewertung ein. Liegt gar kein Risiko für die Betroffenen vor, so ist in der ersten Stufe nur die Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 Abs. 5 DS-GVO intern zu dokumentieren. Eine Benachrichtigung der Aufsichtsbehörde oder der Betroffenen ist dann gerade nicht nötig.

In der zweiten und dritten Stufe ist zusätzlich die Meldung an die Aufsichtsbehörde sowie unter Umständen die Benachrichtigung der Betroffenen nötig, falls ein Risiko beziehungsweise ein hohes Risiko für die Rechte und Freiheiten der Person besteht.

Wir haben die Fälle zum Anlass genommen insbesondere bei öffentlichen Stellen bei Bedarf unsere Beratung zur Verfügung zu stellen. Wesentliche

Frage ist, wie die betroffenen Personen umfassend informiert werden können. Dies stellt regelmäßig eine Herausforderung für die Verantwortlichen dar. Die Information der Betroffenen ist umso wichtiger, da sich Verantwortliche gegebenenfalls schadensersatzpflichtig machen, wenn sie bei Datenpannen die Betroffenen unzureichend informieren. Dies gilt auch für öffentliche Stellen.

Weiterhin ist neben dem systematischen Vorgehen bei etwaigen Datenpannen die Verhinderung von Schäden durch Ransomware-Angriffe essentiell (siehe Kasten). Gerade bei kommunalen Stellen ist es wichtig, dass bei allen Beteiligten und insbesondere auch den externen Dienstleistern Bewusstsein für die etablierten IT-Sicherheitsstandard nach dem BSI-Grundschutz beziehungsweise ISO27001 herrscht. Zwar kann nicht immer jeder Angriff verhindert werden. Angriffe können jedoch so deutlich erschwert oder auf wenige Systeme beschränkt werden.

Für uns ist auch im Falle eines Angriffs ein guter Austausch mit allen Akteuren von Bedeutung, sodass schlussendlich die IT-Sicherheit und der Datenschutz öffentlicher und nicht-öffentlicher Stellen in Baden-Württemberg gestärkt wird.

9.4.2 FAQ Cookies und Tracking

Viele Anbieter von Telemediendiensten – also Webseitenbetreiber, Anbieter von Apps aber auch Hersteller von PC-Software, Betriebssystemen oder vernetzten Geräten wie Küchengeräten, Lampen, Steuergeräten für Heizungen, Alarmsystemen, Smart-TVs oder vernetzten Fahrzeugen – erheben und verarbeiten umfangreiche Daten über die Geräte, ihre Nutzer_innen und deren Verhalten. Sie erheben die Daten in der Regel zu eigenen Zwecken, übermitteln sie an verschiedene Dienstleister oder bieten diesen die Gelegenheit umfangreiche Daten zu erheben und weiterzuverarbeiten. Häufig werden diese Daten auch mit Offline-Bewegungsdaten oder Informationen über Konsumverhalten und ähnlichem verknüpft. Dieses Verhalten wird üblicherweise unter dem Begriff „Tracking“ zusammengefasst.

☛ Mehr Informationen:

Unsere wichtigsten Hinweise und Tipps gegen Ransomware-Angriffe:

- Mitarbeitende schulen, jegliche Remote-Zugänge schließen oder absichern
- Nur die tatsächlich für die Öffentlichkeit angebotenen Dienste sollten öffentlich (z. B. ohne VPN oder Client-Zertifikate) erreichbar sein
- Patch- und Update Management implementieren, regelmäßig Berechtigungen von Nutzenden und Administrator_innen überprüfen
- Die Ausführung von Software einschränken sowie E-Mail und Office Software besonders absichern, insbesondere Office Makros deaktivieren
- Sicheres Backup ist wichtig, insbesondere dürfen Angreifer_innen auch dann, wenn sie im Netzwerk Administrator_innen-Rechte erlangt haben, das Backup nicht zerstören können; bei wichtigen Daten 3-2-1 Backup-Regel einhalten (Mindestens drei Backups auf zwei verschiedenen Speichermedien und ein Backup an einem anderen offline Speicherort)
- Netzwerksegmentierung durchführen, um im Falle eines erfolgreichen Angriffs auf ein System die Auswirkungen auf andere Systeme zu beschränken

Ausführliche Informationen und Fallbeispiele befinden sich in den Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DS-GVO der Artikel-29-Datenschutzgruppe www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/03/Leitlinien-f%C3%BCr-die-Meldung-von-Verletzungen-des-Schutzes-personenbezogener-Daten-.pdf

Weitere umfangreiche Informationen finden Sie hier: www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/ransomware-angriffe_node.html

Die häufigste technische Basis für dieses Tracking sind Cookies, aber auch andere Techniken zum Auslesen und Abspeichern von Informationen auf den Endgeräten der Nutzer_innen. Beim Tracking fallen sehr viele und teils sehr sensible personenbezogene Daten an. Die Anbieter versuchen ihr Vorgehen oftmals mit sogenannten „Cookie-Bannern", mit denen eine Einwilligung der Nutzer_innen eingeholt werden soll, zu rechtfertigen. Denn sie müssen als Verantwortliche nach Artikel 4 Nr. 7 DS-GVO sicherstellen, dass bei der Verarbeitung personenbezogener Daten alle Vorgaben der DS-GVO eingehalten werden. Sie sind zugleich Anbieter von Telemediendiensten nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG, hier: § 2 Abs. 2 Nr. 1), welches die Nutzung von Cookies und ähnlichen Technologien zum Ablegen oder Auslesen von Informationen auf den Systemen regelt. Auch dessen Vorgaben müssen eingehalten werden.

Dabei fallen immer wieder zahlreiche und häufig gleichartige Fehler auf, die Verantwortliche begehen. Daher haben wir im März 2022 mit unserer FAQ zu Cookies und Tracking durch Betreiber von Webseiten, Anbieter von Smartphone-Apps und anderen Telemediendiensten eine umfangreiche Hilfestellung veröffentlicht. Diese steht online auf unserer Homepage unter www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2 zur Verfügung und gibt zahlreiche Hilfestellungen und beantwortet die wichtigsten Fragen rund um Cookie-Banner und den rechtlichen Anforderungen.

Cookies und Tracking haben das Internet und unsere Smartphones – früher mal Orte der Freiheit und Selbstbestimmung – inzwischen zu intensiv überwachten Räumen gemacht. Diese Überwachungsmaßnahmen werden heute häufig als gewöhnlich wahrgenommen – gerade so, als gäbe es keine Alternativen dazu und die Überwachung sei naturgegeben. Der Eingriff in die Bürgerrechte ist dabei teilweise so massiv, dass Menschen mit dem Wissen, das andere über sie haben, wirtschaftlich übervorteilt und sogar politisch manipuliert werden können. Die klaren Vorteile der Digitalisierung werden so in Zweifel gezogen, wenn sie nur noch um den Preis einer Aufgabe unserer Bürgerrechte zu haben sind. Digitalisierung lebt aber vom Vertrauen der Bürger_innen. Sie müssen sie sich darauf verlassen können, dass ihre zum Teil intimen Informationen nicht nebenbei und für sie völlig unklar zu Überwachung und Kontrolle genutzt werden. Die DS-GVO gibt den Rahmen für die Wahrung unserer Bürger_innenrechte in der digitalen Welt vor.

Wer Cookies und andere Tracking-Techniken einsetzt, personenbezogene Daten von Bürger_innen sammelt, verarbeitet, weitergibt und verkauft, muss die rechtlichen Vorgaben beachten. In der Regel ist für Tracking eine vorherige, informierte und freiwillige Einwilligung der Nutzer_innen nötig, die häufig über „Cookie-Banner" eingeholt werden soll. Die Anforderungen an diese gebotenen Hinweise sind hoch. An Behörden und andere öffentliche Stellen werden für die Einholung von Einwilligungen gesetzlich besonders hohe Hürden gestellt (vgl. Abschnitt A 4.2 der Tracking-FAQ). Nach dem Erwägungsgrund 43 der DS-GVO liegt im Regelfall eine Freiwilligkeit einer Einwilligung nicht vor, da im Verhältnis Bürger_in zu Behörde ein klares Ungleichgewicht vermutet wird. Behörden können daher grundsätzlich keine Einwilligung zum Tracking einholen.

Mit unseren FAQ knüpfen wir an die „Orientierungshilfe der Aufsichtsbehörden für die Anbieter_innen von Telemedien (OH Telemedien 2021)" der Datenschutzkonferenz der unabhängigen Aufsichtsbehörden der Länder und des Bundes (DSK) an. Sie benennt für die Praxis mögliche Risiken des Einsatzes von Überwachungstechniken und bietet konkrete Unterstützung wie etwa zur Reichweitenanalyse, die auch ohne den Einsatz von personenscharfen Kontrolltechniken möglich ist.

Tracking-Fälle in der Praxis

Wir helfen nicht nur den Verantwortlichen, ihre Pflichten zu erfüllen. Die Tracking-FAQ stellen auch unseren Prüfmaßstab bei der Prüfung von Webseiten, Apps und anderen Telemediendiensten dar. Die Prüfung kann dabei sowohl von Amts wegen als auch aufgrund von Beschwerden Betroffener erfolgen.

Solche Beschwerden erreichen uns in großen Zahlen. Daher entwickeln wir auch eigene Prüfwerkzeuge, um die technische Prüfung zu automatisieren und sowohl offene als auch versteckte Verarbeitungen zu erkennen. Wenn wir aktiv werden nehmen wir im ersten Schritt also eine technische Prüfung vor beziehungsweise analysieren das Datensendeverhalten der Website oder App. Die

Ergebnisse werden anschließend rechtlich bewertet und ein Anschreiben an die Verantwortlichen verfasst, das unter anderem die Sachlage erläutert, entdeckte Mängel aufführt, den Verantwortlichen zur Behebung der Mängel auffordert und für weitere Details auf die Tracking-FAQ verweist.

Zeitnahe Reaktion von Verantwortlichen

Die Verantwortlichen reagieren unterschiedlich auf unser Anschreiben beziehungsweise technische und rechtliche Bewertung. Positiv hervorheben möchten wir einen Anbieter für IT-Sicherheitslösungen, der von uns aufgrund der Einbindung von Tracking-Dienstleistern, Datenübermittlungen in Drittstaaten ohne Sicherheitsstandards wie die der europäischen DS-GVO und eines nicht datenschutzkonformen Einwilligungs-Banners innerhalb seiner App kontaktiert wurde. Um es mal greifbar zu machen: Ohne überhaupt eine Einwilligung beim Nutzer eingeholt zu haben, flossen Daten an Google-Dienste wie Firebase Analytics, Crashlytics und weitere Tracking-Anbieter ab. Während der App-Nutzung kamen dann noch weitere Tracking-Anbieter und sowie Facebook hinzu. Neben Geräteinformationen wurde unter anderem ebenfalls die Google-Advertising-ID an Facebook übermittelt – diese Information genügt im Grunde genommen, dass Facebook nun eine Verknüpfung zwischen Facebook-Nutzer und den übermittelten Daten herstellen kann. Der Grund: Auch die Facebook-App (sofern installiert) liest die Google-Advertising-ID aus. Damit hat Facebook anschließend einen Identifier, den sie einer Person exakt zuordnen können.

Die Reaktion auf unser Anschreiben fiel vorbildlich aus. Nahezu alle Beanstandungen, die wir im Anschreiben aufgeführt hatten, wurden beseitigt und in einem Antwortschreiben ausführlich Stellung bezogen. Aufgrund kleinerer Beanstandungen stehen wir mit dem Verantwortlichen zwar weiterhin in Kontakt – insgesamt gesehen freuen wir uns aber darüber, dass der Verantwortliche auf nahezu alle Beanstandungen zeitnah reagiert hat. Solch ein Vorgehen ist keinesfalls selbstverständlich.

Häufig integrieren Entwickler allerhand Tracking-Dienste in die Webseiten oder Apps, ohne sich über die rechtlichen Probleme bewusst zu sein. So stellen wir auf manchen Websites die Nutzung von unzähligen Tracking-Diensten fest, in einem Fall wurden 60 Cookies ohne Einwilligung gesetzt. Nach unserem Anschreiben hat der Verantwortliche bemerkt, dass diese (fast) alle nicht benötigt werden und hat sie entfernt.

Ausblick 2023

Auch in Zukunft planen wir, Verantwortliche umfangreich über ihre Pflichten zu informieren. So sind auch einige Schulungen in unserem hauseigenen Bildungszentrum BIDIB geplant. Weiter werden wir auch Prüfungen vornehmen und darauf hinwirken, datenschutzwidriges Tracking bei Verantwortlichen abzustellen. Zahlreiche Verantwortliche mussten im Jahr 2022 zudem feststellen, dass auch die betroffenen Personen zahlreiche Rechte haben und müssen vermehrt mit Schadenersatzforderungen nach Artikel 82 DS-GVO rechnen.

9.4.3 Updates: Vertrauen ist gut, Kontrolle des Abflusses ist besser

Das regelmäßige Einspielen von (Sicherheits-)Updates stellt eines der wichtigsten Maßnahmen gegen bekannte beziehungsweise bekanntgewordene Sicherheitslücken dar. Insbesondere weit verbreitete Softwareprodukte wie Betriebssysteme, Browser, und Standardsoftware wie PDF-Reader oder Textverarbeitungssoftware sind ein beliebtes Angriffsziel und ein häufiges Einfallstor für Schadsoftware (Viren, Würmer, Trojaner und so weiter), und dies ganz besonders dann, wenn keine aktuellen Patches beziehungsweise Updates eingespielt werden. Das bedeutet: Sowohl das Betriebssystem, als auch alle auf dem System installierten Anwendungen, Treiber, Browser-Erweiterungen et cetera sollten stets auf aktuellem Stand sein. Um den Anforderungen aus Artikel 32 DS-GVO gerecht zu werden, müssen Verantwortliche dafür Sorge tragen, dass Updates zügig installiert werden.

In großen Umgebungen werden solche (Sicherheits-)Updates meist über eine zentrale Softwareverteilung bereitgestellt und automatisiert auf die

☛ Mehr Informationen:

FAQ Cookies & Tracking: www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2

im Netzwerk befindlichen Rechner ausgeliefert. Freigegeben und verwaltet werden solche Updates im Normalfall über die IT-Administration beziehungsweise einen (externen) IT-Dienstleister. Und obwohl das zeitnahe Einspielen von (Sicherheits-) Updates konsequent, wichtig und sehr sinnvoll ist, gibt es auch Tücken dabei. Denn das regelmäßige Einspielen von (Sicherheits-)Updates schließt nicht nur bekanntgewordene Sicherheitslücken, sondern es werden auch Fehler beseitigt, die sich nicht unmittelbar auf die Sicherheit auswirken oder es werden neue Funktionen ausgeliefert. Insbesondere das Nachrüsten neuer Funktionen in bestehende (Standard-)Software kann sich negativ auf die Sicherheit und den Datenschutz der eigenen IT-Infrastruktur auswirken, wie das nachfolgende Beispiel demonstriert.

Als datenschutzrechtlich Verantwortliche untersuchen wir in Stichproben das Datensendeverhalten unseres Behörden-Arbeitsplatzes. Behördenintern können Mitarbeiter beim Landesbeauftragten zwischen dem Browser von Microsoft (Edge) und Mozilla (Firefox) wählen. Mit einem Update hat Microsoft dem Edge-Browser eine neue Funktion spendiert, die sich nicht zwangsläufig für den Einsatz im Unternehmens- beziehungsweise Behördenumfeld eignet. Nach dem Update war die Funktion „Shopping in Microsoft Edge" standardmäßig aktiv. Besuchte ein Nutzer nunmehr eine Shopping-Website, nimmt der Edge-Browser automatisch eine Verbindung zu Microsoft auf und ermittelt, ob für die Website Coupons beziehungsweise Vergünstigungen angeboten werden. Dabei werden zusätzlich einige Informationen an Microsoft übermittelt, unter anderem auch die vollständige URL der besuchten Webseite. Diese Übermittlung an Microsoft ist nicht von jedem Nutzer gewünscht und im Unternehmens- bzw. Behördenumfeld sogar fragwürdig, da das Unternehmen oder die Behörde für die Übermittlung dieser Daten an Microsoft verantwortlich ist. Zwar lässt sich die Funktion direkt im Browser (über Einstellungen → Datenschutz, Suche und Dienste → Dienste) beziehungsweise über die Gruppenrichtlinien für alle Mitarbeitenden deaktivieren. Allerdings müssen Arbeitgeber_innen als Verantwortliche für die Übermittlung dieser Daten an Microsoft nicht nur eine Rechtsgrundlage vorweisen, sondern auch die Anforderungen aus Artikel 25 Absatz 2 DS-GVO einhalten. Demnach sind Voreinstellungen zu wählen, die sicherstellen, dass nur solche Daten verarbeitet werden, die für den jeweiligen Zweck erforderlich sind. Für den Zweck der Darstellung der Webseite eines Online-Shops ist es aber nicht erforderlich, an den Browser-Anbieter die Information zu übermitteln, dass jemand bzw. wer diese Seite aufgerufen hat.

Umfangreicher Datenabfluss Ende 2022

Dass auch weitaus sensiblere Daten betroffen sein können, haben wir bei einer Folge-Untersuchung Ende 2022 kurz vor Redaktionsschluss dieses Tätigkeitsberichts festgestellt: Microsoft Edge in Version 107.0.1418.35 übermittelt alle Daten aus Eingabefeldern auf beliebigen Webseiten an einen Microsoft-Server (nleditor.osi.office.net). Die Übermittlung der Inhalte von Eingabefeldern an Microsoft fand auch im privaten Browsermodus statt. Nach unserer Beobachtung fand keine Übermittlung statt, wenn Eingabefelder als Passwort deklariert oder mit dem HTML Attribut „spellcheck=off" versehen waren oder wenn keine Buchstaben eingegeben wurden.

Im Rahmen der Untersuchung konnten wir zudem feststellen, dass für dieses Verhalten die Einstellung „Verwenden der Schreibunterstützung" (erreichbar über edge://settings/?search=editor) verantwortlich war, die der Hersteller in der Standardeinstellung aktiviert hat. In den Release Notes von Edge (Siehe learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-stable-channel) wurde darüber nicht informiert. Für Vorversionen, bei denen diese Funktion zwar vorhanden, aber nicht in der Standardeinstellung aktiviert war, gibt Microsoft nur an, dass Edge eine erweiterte Rechtschreib- und Grammatikprüfung anbiete. In späteren Versionen (z. B. 108.x.x.x) wurde die Standard-Einstellung nach unserer Beobachtung vom Hersteller wieder auf eine lokale Prüfung geändert.

Im Ergebnis wurden möglicherweise – soweit wir dies bislang mit den uns zur Verfügung stehenden Mitteln prüfen konnten – wochenlang grundsätzlich alle Daten aus Eingabefeldern bei der Nutzung des Edge-Browsers an Microsoft-Server übermittelt. Dies betraf nicht nur den LfDI, sondern alle Edge-Nutzer. Für den Standard-Arbeitsplatz der Landesverwaltung Baden-Württemberg konnte nach unserer Meldung an den Landesdienstleister BITBW der Datenabfluss schnell deaktiviert werden. Die übermittelten Daten können z. B. Suchbegriffe

im Intranet, komplette Inhalte von E-Mails bei der Verwendung eines Webmailers, sensible Daten bei der Nutzung von browserbasierten Fachverfahren oder auch beliebige Kontaktformulare auf Webseiten sein.

Kontrolle ist besser

Die Beispiele zeigen: Im Grunde muss jedes Update – und zwar nicht nur von Microsoft-Software – vor dem Ausrollen genau geprüft werden. Das beginnt beim Test auf Kompatibilität mit den im Unternehmen beziehungsweise Behörden etablierten Arbeitsprozessen und geht weiter mit der Prüfung des Datensendeverhaltens. Für die zuständige IT ist das eine Mammutaufgabe, die nur bewältigt werden kann, wenn genügend Personal für solche Aufgaben bereitgestellt wird. Aus Kostengründen oder etwa aufgrund fehlender Prozesse findet eine solche Prüfung vermutlich manchmal nur oberflächlich oder gar nicht statt, weshalb dann Funktionen Einzug halten, die sich negativ auf die Sicherheit und den Datenschutz der (eigenen) IT-Infrastruktur auswirken können.

Darüber hinaus hat solch ein „Funktionsupdate" übrigens nicht nur Ausstrahlwirkung in den Bereich der DS-GVO. Bei der Beschaffung der öffentlichen Hand sind die Ergänzenden Vertragsbedingungen für die Beschaffung von Informationstechnik (EVB-IT) zu beachten. Diese müssen grundsätzlich Vertragsbestandteil im Rahmen der Beschaffung sein. Demnach hat der Auftragnehmer zu gewährleisten, dass von ihm zu liefernde Standardsoftware frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit dieser Software, anderer Soft- und/oder Hardware oder von Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen. So sind unter anderem Funktionen zum unerwünschten Absetzen/Ausleiten von Daten oder unerwünschte Funktionserweiterungen unzulässig. Auftraggeber sollten darauf achten, dass sie Soft- und Hardware stets unter Einschluss der EVB-IT beschaffen und die Verträge auch durchsetzen. Die oben dargestellten Beispiele unterstreichen die Wichtigkeit und Praxisrelevanz dieser Klauseln.

Die Verantwortung nun gänzlich auf die jeweiligen IT- und Beschaffungs-Abteilungen abzuwälzen, greift allerdings zu kurz. Aus unserer Sicht sind die Hersteller ebenfalls in der Pflicht, ihre Produkte und Dienste so zu gestalten, dass sie und ihre Vertriebspartner ihre vertraglichen Verpflichtungen sowie ihre Kunden die rechtlichen Anforderungen der DS-GVO erfüllen können. Da die DS-GVO keine Herstellerhaftung kennt, können wir Hersteller selbst nicht aufsichtsrechtlich ansprechen. Gleichwohl kann es aber auch Hersteller für die Belange von Verantwortlichen sensibilisieren, wenn Kunden Sach- und Rechtsmängelansprüche geltend machen oder betroffene Personen Schadenersatz nach Artikel 82 DS-GVO einfordern oder ihre Auskunftsrechte nach Artikel 15 geltend machen.

Soweit Hersteller als datenschutzrechtlich Verantwortliche personenbezogene Daten verarbeiten, sind die jeweils federführenden Aufsichtsbehörden aufgerufen, die Rechtmäßigkeit solcher Verarbeitungen zu prüfen. Für den LfDI bedeutet dies, dass wir zukünftig in diesem Bereich verstärkt prüfen werden, ob die rechtlichen Vorgaben aus § 25 TTDSG eingehalten werden.

☛ Mehr Informationen:

Release Notes von Edge:
learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-stable-channel

Ältere Release Notes Edge:
learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote-archive-stable-channel

Handreichung zur „technischen no-spy-Klausel":
www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-bvb/basisvertraege/ueberlassung-typ-a/handreichung-no-spy-klausel.pdf

9.5 Alles mit V: Verkehr, Vereine, Videoüberwachung

9.5.1 Abschied auf Schwäbisch am Stuttgarter Flughafen

„Jezzd schnabb schoh dain Koffr ond raus aus'm Karra, sonscht koschd's meh noh äbbas!" Anzunehmen ist, dass sich zukünftig die Abschiedsszenen am Stuttgarter Flughafen aus Gründen der schwäbischen Sparsamkeit erheblich verkürzen werden.

In einer diesjährigen Presseerklärung vom 11.1.22 von Stuttgart Airport wurden die neue Regeln für die Zufahrt auf die Abflugebene direkt vor den Terminals kurz und knackig erklärt: *„Wer dort mit dem Auto vorfährt, um Fluggäste abzusetzen, darf sich dafür insgesamt acht Minuten Zeit lassen – bisher waren nur drei Minuten erlaubt. Bis 10 Minuten kosten dann fünf Euro. Wer bis zu 20 Minuten hält, zahlt 20 Euro, bei bis zu 30 Minuten werden 30 Euro fällig. Die Vorfahrt wird durch automatische Schranken geregelt. Bei Einfahrt und Ausfahrt registrieren Kameras vorübergehend das Autokennzeichen. An fünf Automaten entlang der Terminalvorfahrt kann bar oder elektronisch bezahlt werden. Dazu ist lediglich die Eingabe des Autokennzeichens erforderlich. Wer weniger als acht Minuten hält, kann direkt ausfahren und muss gar nicht erst zum Automaten. Sollte die Kamera einmal ausfallen, können bei der Einfahrt Tickets gezogen werden."*

Dass es sich hier um ein datenschutzrechtlich relevantes Verfahren handelt, hat auch der Betreiber erkannt und uns daher um einen Vorort- und Besprechungstermin gebeten. Vermutlich wurde bereits zu diesem Zeitpunkt bemerkt, dass nicht alle Kund_innen von dieser Maßnahme begeistert sind, was laut medialer Berichterstattung auch zu handfesten Auseinandersetzungen geführt haben soll.

Anzumerken ist, dass das System der Kennzeichenerfassungen auch an anderen Flughäfen in mehreren Bundesländern praktiziert wird. Videobasierte Kennzeichenerfassungssysteme sind uns aber nicht nur an Flughäfen, sondern auch aus Parkhäusern und gewerblichen Parkräumen bekannt geworden, auch wenn es hier immer wieder leichte technische Unterschiede gibt. So erreichten uns in der Vergangenheit wiederholt Anfragen von Bürgern vor allem zu verschiedenen Parkplatzbetreibern.

Neben dem datenschutzrechtlichen Aspekt geht es den Beschwerdeführer_innen oftmals auch darum, sich vertraglicher Ansprüche für die Nutzung der Parkflächen zu erwehren. Eine rechtliche Beratung zu möglichen zivilrechtlichen Auseinandersetzungen leisten wir allerdings nicht.

Eine automatisierte Kennzeichenerfassung an dem vorliegenden Bereich des Flughafens ist nach Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO zulässig, wenn sie zur Wahrnehmung eines berechtigten Interesses des Kamerabetreibers erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Indem das Kennzeichen eines jeden Fahrzeugs bei Ein- und Ausfahrt durch eine Kamera erfasst wird, erfolgt eine automatisierte Verarbeitung personenbezogener Daten. Gleiches gilt für die Eingabe des Kennzeichens im Rahmen des Bezahlvorgangs.

Neben dem nachzuweisenden berechtigten Interesse geht es für uns in erster Linie darum, dass sich die videobasierte Parkraumüberwachung und Kennzeichenerfassung als besondere Art der Datenverarbeitung an den datenschutzrechtlichen Grundsätzen gemäß Artikel 5 DS-GVO (z. B. Transparenz, Zweckbindung und Speicherbegrenzung) orientiert, insbesondere unter Beachtung der Erforderlichkeit.

Im konkreten Fall sah sich der Flughafenbetreiber seit Jahren dem Problem ausgesetzt, dass – insbesondere in Sommermonaten und den Ferienzeiten – Zufahrtswege durch das hohe Verkehrsaufkommen regelmäßig verstopft waren. Betroffen war vor allem der Bereich vor dem Abflug- und Ankunftsterminal. Hier wurden die Reisenden nicht nur mit ihrem Gepäck abgesetzt, sondern teilweise auch noch an den Schalter begleitet. Zubringende und Abholende parkten in zweiter oder auch dritter Reihe. Zudem ging der Trend offenbar dazu, bis zur Ankunft der Gäste „Runden am Flughafen" zu drehen.

Um dem entgegenzuwirken wurde eine effektive Verkehrslenkung zur Beschränkung des Verkehrs auf der Terminalvorfahrt errichtet unter gleichzeitiger Verwendung von Kfz-Kennzeichenerkennung und der kennzeichengebundenen Gewährung eines Zeitraums, innerhalb welchem dieser Bereich kostenfrei genutzt werden darf. Die Hauptziele des

Projekts lagen unter anderem in der Optimierung der Verkehrsflusssteuerung und der Erhöhung der Verkehrseffizienz. Zudem sollte dadurch die Sicherheit auf der Terminalvorfahrt gewahrt und wiederhergestellt werden, insbesondere mit Blick auf die abstrakte Gefährdungslage an internationalen Verkehrsflughäfen wie dem Flughafen Stuttgart. Dazu galt es, die Befahrbarkeit der Terminalvorfahrt für Rettungs- und Einsatzkräfte sicherzustellen.

Begründet wurde die Erforderlichkeit der automatisierten Kennzeichenerfassung auch damit, dass der beschriebene „Drehtür-Effekt" unterbunden würde unter gleichzeitiger Beibehaltung einer begrenzten Aufenthaltsmöglichkeit für die Nutzer_innen. Indem die Kfz-Kennzeichen als Kennung als Ein- und Ausfahrtsmedium und bei einer möglichen Bezahlung bei Zeitüberschreitungen verwendet werden, lassen sich Papiertickets weitestgehend vermeiden.

Durch die weitgehende Vermeidung von Papiertickets kann zudem die Verkehrseffizienz der Terminalvorfahrt erhöht werden. Im Vororttermin wurde uns dies anhand konkreter Berechnungsbeispiele dargestellt. So würde die Einfahrt unter Verwendung einer Papierticketausgabe vom Herablassen der Autoscheibe über das Ziehen eines Tickets und den Folgehandlungen durchschnittlich fünfzehn Sekunden dauern. Die Vorgangsdauer der Kfz-Kennzeichenerkennung beträgt dagegen lediglich drei Sekunden.

In ihrer Gesamtheit waren diese Argumente gewichtig genug, um unsere Behörde von der Erforderlichkeit der Datenverarbeitung zu überzeugen. Bei einer Sichtung der Kameras in den jeweiligen Bereichen der Terminals konnte allerdings der Eindruck entstehen, dass die Kameras, bedingt durch die Anbringungshöhe, direkt in das Kfz hineinfilmen und die Insassen erfassen könnten. Die Erfassung von Fahrzeuginsassen im Ein- und Ausfahrtbereich erachten wir jedoch seit jeher als unzulässig.

Die Ausrichtung der Kamera und somit der Linse war gemäß der Herstellerempfehlung in einem extrem steilen Winkel vorgenommen worden, um fehlerhaften Erfassungen der Kennzeichen vorzubeugen. Das System wird auch ausschließlich auf ein erkanntes Kennzeichen hin „scharfgeschaltet". Erfassen die Videokameras kein Kennzeichen, erfolgt auch keine Datenübermittlung.

Von uns wurde dazu ergänzend angeregt, über den Kameras verlängerte Verblendungen anzubringen, um bei den betroffenen Kfz-Insassen während des Erfassungsvorgangs gar nicht erst den Eindruck einer Ablichtung aufkommen zu lassen. Obgleich diese Maßnahme mehr einer Art „Attrappen-Effekt" abhilft, der nicht mehr vom Anwendungsbereich der DS-GVO umfasst ist, wird mit dieser Maßnahme der subjektive Überwachungsdruck der Fahrzeuginsassen in erheblichem Maße reduziert. Zwischenzeitlich ist uns die Mitteilung zugegangen, dass die Produktion und Anbringung bereits beauftragt wurde und mit einer zeitnahen Umsetzung zu rechnen ist.

Einen großen Wert legen wir bei jeglicher Art der Videoüberwachung auf die Einhaltung des Transparenzgebotes und öffentlich verfügbare Informationen für die Betroffenen. Beim Vororttermin war hier tatsächlich noch Nachholbedarf erkennbar. Die Hinweisbeschilderung war oftmals unübersichtlich gestaltet und Informationen zum Datenverarbeitungsvorgang an ungeeigneten Stellen angebracht. Die Transparenzpflicht gebietet es gerade, dass Verarbeitungen für die Nutzer_innen nachvollziehbar sind, damit dieser insbesondere beim Einsatz von Videokameras bereits zum frühestmöglichen Zeitpunkt – und nicht erst zum Zeitpunkt der Kennzeichenerfassung – absehen kann, dass die Daten zu den in Rede stehenden Zwecken und Interessen verarbeitet werden.

In den Gesprächen mit dem Betreiber konnten wir durchsetzen, dass die bereits existierende Beschilderung zur Kenntlichmachung des Einsatzes der Kennzeichenverarbeitung vor der Schrankenanlage teilweise neu angeordnet beziehungsweise weiter ergänzt wird, um im Ergebnis auch der Transparenz und Vorhersehbarkeit ausreichend nachzukommen. Fahrzeugführer_innen wird über eine Ausfahrt vor der Kennzeichenverarbeitungsanlage zudem die Möglichkeit geboten, sich dem Datenverarbeitungsvorgang entziehen zu können. Nach unserer Auffassung ist dies notwendig, aber auch ausreichend, um einem sogenannten Trichtereffekt und somit der Datenverarbeitung doch noch zu entgehen.

Aufgrund der überaus komplexen Datenverarbeitungsvorgänge werden wir den Gang des Verfahrens auch weiterhin begleiten. Hier gilt dann der schwäbische Grundsatz: „Äbbas isch joh emmer zom Bruddla."

9.5.2 Testfahrt mit der neuen Mercedes S-Klasse – Videotechnik zur Ermöglichung automatisierten Fahrens

Ein weiterer neuer Anwendungsbereich von Videotechnik an Fahrzeugen findet sich im Bereich des automatisierten Fahrens. Im Rahmen eines Besuchs bei der Mercedes-Benz AG erhielten wir aufschlussreiche Einblicke in den „Drive Pilot" der neuen S-Klasse.

Beim Besuch bei der Mercedes-Benz AG wurde uns die neue S-Klasse vorgestellt. Diese nutzt den sog. „Drive Pilot". Die Mercedes-Benz AG hat hierfür als weltweit erster Automobilhersteller eine international gültige Systemgenehmigung für hochautomatisiertes Fahren (SAE-Level 3) erhalten. Bei hohem Verkehrsaufkommen oder Stausituationen kann damit auf geeigneten Autobahnabschnitten in Deutschland bis 60 km/h hochautomatisiert gefahren werden. Der Drive Pilot entlastet Fahrer_innen und ermöglicht Nebentätigkeiten, auch wenn die Person jederzeit bereit sein muss, das Steuer zu übernehmen. Laut der Mercedes-Benz AG kommen dabei neben LiDAR-, Radar-, Ultraschall- und Nässesensoren auch Kameras zum Einsatz, um Objekte in der Fahrzeugumgebung onboard automatisiert zu erkennen. Die sich daraus ergebenden fahrtrelevanten Informationen würden auf dem Display im Cockpit lediglich schematisch dargestellt. Auch wenn zunächst im Moment der Erfassung, vergleichbar der Situation bei der Dashcam, grundsätzlich personenbezogene Daten betroffen sein können, konnten wir in Bezug auf die sog. „Metadaten", die onboard weiterverarbeitet, im Cockpit dargestellt und ggf. ins „Backend" übertragen werden, keine Anhaltspunkte für einen Personenbezug feststellen. Im Falle einer sofortigen Umwandlung in Metadaten, unumkehrbarer Löschung der ursprünglichen Videosequenzen und technischen Ausschlusses einer diesbezüglichen Zugriffsmöglichkeit könnte bereits das Vorliegen einer Verarbeitung im Sinne Art. 4 Nr. 2 DS-GVO und damit die Anwendbarkeit der DS-GVO diskutiert werden. Jedenfalls überwiegen aufgrund der marginalen Eingriffsintensität die berechtigten Interessen an der Verarbeitung im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO. Ob man hingegen auch bei automatisierten Fahrzeugen, die ausschließlich über Sensorik der visuellen Umgebungserfassung verfügen, zum Ausgleich dafür aber mehr Kameras einsetzen und damit potentiell auch mehr personenbezogene Daten verarbeiten, noch die Erforderlichkeit im Sinne von Art. 6 Abs. 1 Unterabs. 1 Bucht. f DS-GVO als gegeben ansehen kann, ist demgegenüber fraglich, insbesondere dann, wenn eine eingriffsintensivere Verarbeitung allein aufgrund des Verzichts auf zusätzliche alternative und in der Herstellung kostspieligere Sensortypen erfolgt.

Ob der Einsatz von Videotechnik bei Fahrzeugen zulässig ist, hängt stark von den damit verfolgten Einsatzzwecken und den einzelnen technischen Gegebenheiten ab. Im Rahmen der rechtlich zulässigen Grenzen eingesetzt, kann er zu bahnbrechenden Weiterentwicklungen beitragen.

9.5.3. Video-Parkwächter

In der Vergangenheit waren Kameras an Fahrzeugen vor allem in der Form von sogenannten Dashcams vorzufinden (siehe Tätigkeitsbericht 2018, S. 87 und Pressemitteilung vom 23. April 2019 zum Positionspapier der DSK zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen). Inzwischen findet Videotechnik auch bei geparkten Fahrzeugen zur Umgebungserfassung Anwendung. In Bezug auf Letztere erhalten wir zahlreiche Beschwerden.

Werden Kameras an einem Fahrzeug eingesetzt, gelten für diese im Ausgangspunkt die gleichen rechtlichen Voraussetzungen wie für andere Formen der Videoüberwachung. Denn die Kameras, die die Umgebung eines geparkten oder fahrenden Fahrzeugs erfassen, erheben in der Regel personenbezogene Daten von anderen Verkehrsteilnehmenden (beispielsweise das äußere Erscheinungsbild von Fußgängern und Kfz-Kennzeichen, die bestimmten Haltern zugeordnet werden können). Bei Kameras, die zu dem Zweck eingesetzt werden, im Falle eines Unfalls entlastendes Beweismaterial für Fahrer_innen zu sammeln (Dashcams), können nur unter sehr engen Voraussetzungen des Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO, insbesondere die Erforderlichkeit und das Überwiegen des Interesses des Verantwortlichen, angenommen werden. Beispielsweise darf regelmäßig nur eine kurze Zeitpanne aufgezeichnet werden und nur im Falle eines besonderen Ereignisses wie beispielsweise einem Unfall eine dauerhafte Speicherung erfolgen. Ansonsten muss eine sofortige „Überschreibung", das heißt eine Löschung, erfolgen.

Als Form der „Weiterentwicklung" bieten manche Hersteller inzwischen Fahrzeuge an, bei denen Ka-

meras im geparkten Zustand zur Umgebungserfassung als Nachweis für Sachbeschädigungen und Vandalismus eingesetzt werden können. Die Kameras sollen damit einen herkömmlichen Parkwächter ersetzen. Muss die Funktion vom Fahrer oder der Fahrerin aktiviert werden, ist zu beachten, dass diese als Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO gelten. Dies hat zur Folge, dass der lange Pflichtenkatalog der DS-GVO jedenfalls auch sie betrifft. Problematisch wird dies vor allem dann, wenn eine solche Funktion im öffentlichen Verkehrsraum zum Einsatz kommt. Insbesondere kann im Hinblick auf Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO nicht gerechtfertigt werden, wenn die Umgebungserfassung anlasslos erfolgt und selbst Umstände, die in keiner Weise die Interessen der Fahrer_innen, Halter_innen oder Eigentümer_innen berühren, dazu führen, dass die Aufzeichnungen gespeichert werden. Damit ist beispielsweise der die Speicherung auslösende Fall gemeint, dass sich eine Person aus einer bestimmten Richtung dem Fahrzeug im Vorbeigehen lediglich nähert. Die Interessen von Passant_innen, sich undokumentiert im öffentlichen Raum frei zu bewegen, überwiegen hier. Auch wenn Fahrer_innen in solchen Fällen, die vom Hersteller angebotene Funktion „lediglich nutzen", müssen sie als Verantwortliche mit aufsichtsrechtlichen Maßnahmen, wie z. B. einem Bußgeld, rechnen.

Bei der Nutzung von vom Hersteller bereitgestellter Videotechnik zur Umgebungserfassung geparkter Fahrzeuge ist für Fahrer_innen Vorsicht geboten. Verleiten Hersteller ihre Kund_innen geradezu dazu, sich datenschutzwidrig zu verhalten, besteht offensichtlich Nachbesserungsbedarf.

9.5.4 Kassenloses Einkaufen

Das kassenlose Einkaufen ist ein Konzept, welches zukünftig dem bislang gewohnten Einkaufsprozess erheblich Konkurrenz bereiten könnte, aber verschiedene datenschutzrechtliche Fragestellungen aufwirft.

Eine Ausprägung ist beispielsweise unter den Bezeichnungen Grab & Go, Just-Walk-Out und Pick & Go bekannt. Sie erlaubt es Einkaufenden, die sich zuvor registriert haben, Waren aus Regalen zu entnehmen und den Laden im Anschluss einfach zu verlassen, ohne dass von Seite der Einkaufenden noch die Abrechnung über eine Kasse oder sonstige Schritte erforderlich wären. Im Anschluss an das Verlassen des Ladens wird der Einkauf automatisch abgerechnet und ein Beleg, etwa per E-Mail oder auch auf eine App, versandt.

Das Konzept wird bereits in einigen (dazu mit spezieller Technik ausgestatteten) Läden im Landes- und Bundesgebiet getestet und sogar teilweise im Alltagsbetrieb genutzt, vor allem im Bereich des Lebensmitteleinzelhandels. Ermöglicht wird der Einkaufsprozess dabei durch intelligente Systeme, die hauptsächlich auf Kameras und Anwendungen der künstlichen Intelligenz beruhen und das Verhalten von Personen im Laden, wie beispielsweise die Entnahme oder das Zurücklegen von Waren, exakt verfolgen. Darüber kann das System den jeweiligen Einkaufenden ihren Einkauf zurechnen und abschließend entsprechend abrechnen. Solche Systeme existieren sowohl in Form hybrider Lösungen, bei welchen gleichzeitig normale Kassen eingerichtet sind, die einen herkömmlichen Einkauf erlauben, als auch in der Gestaltungsform ausschließlich kassenloser Einrichtungen.

Risiken ergeben sich dabei unter anderem daraus, dass die erhobenen Daten geeignet sind, genaue Rückschlüsse auf das Einkaufsverhalten Einzelner zu ziehen. So ließe sich etwa feststellen, wie lange sich eine Person vor einem Regal aufhält, was sie regelmäßig einkauft und wie lange sie sich mit bestimmten Produkten beschäftigt. Einkäufe, Werbung und auch Preise könnten immer weiter personalisiert und dadurch gezielt auf die einzelne einkaufende Person ausgerichtet werden.

Im Rahmen dieser Entwicklungen aufgeworfene datenschutzrechtliche Fragestellungen mit Bezug zu den intelligenten Kamerasystemen werden derzeit im Rahmen einer Unterarbeitsgruppe des von unserer Behörde geleiteten Arbeitskreises Videoüberwachung der DSK behandelt.

Betrachtet werden dabei neben weiteren Aspekten die in Konzepten wie dem Grab & Go, Just-Walk-Out und Pick & Go bestehenden Abläufe und technischen Prozesse. Zudem wird näher thematisiert, ob die mit den Konzepten einhergehenden Verarbeitungen personenbezogener Daten wirklich erforderlich sind. Dies umfasst beispielsweise eine Untersuchung, ob nicht potenziell datensparsamere, aber gleich geeignete Alternativen zum Einsatz

der intelligenten Kamerasysteme verwendet werden könnten. Auch sonstige Systeme, wie solche, die eine Erfassung des Einkaufs mittels auf den Waren angebrachten RFID-Etiketten (wobei die Warenzuordnung über Funkfrequenzen erfolgt) zulassen, könnten ein kassenloses Einkaufen schließlich grundsätzlich ermöglichen.

Zu beachten ist außerdem, dass sich verschiedene Personengruppen in den Läden aufhalten. Diese umfassen im Allgemeinen Einkaufende, Begleitpersonen (beispielsweise Kinder), Beschäftigte und bei hybriden Lösungen zusätzlich konventionell – also an einer herkömmlichen Kasse – einkaufende Personen. Um die im Rahmen des kassenlosen Einkaufens stattfindenden Verarbeitungen von deren personenbezogenen Daten zu rechtfertigen, bedarf es jeweils tauglicher Rechtsgrundlagen.

Einkaufen von „damals“ hat nichts mit dem Einkaufen von „heute“ zu tun.

Welche Rechtsgrundlagen im konkreten Kontext überzeugen können und welche Beschränkungen und Korrekturen erforderlich sind, um datenschutzrechtlichen Risiken der intelligenten Kamerasysteme zu begegnen, ist Gegenstand des Austauschs innerhalb der Unterarbeitsgruppe.

Neben dieser Befassung befinden wir uns derzeit auch mit einem Systembetreiber, einem Unternehmen der Schwarz Gruppe, im Austausch. Dieses Unternehmen betreibt mit der sogenannten „shop. box“ ein kassenloses Einkaufssystem auf dem Bildungscampus Heilbronn. Der Einkauf darin ist bislang nur Campusangehörigen (Studierenden und Lehrenden) vorbehalten.

9.5.5 Streaming von Sportveranstaltungen

Wohl getrieben durch die Pandemie und aufgrund des Vorbilds großer Sportveranstaltungen, die heutzutage von nahezu überall auf der Welt per Livestream empfangen werden können, kommt mittlerweile auch im Bereich des Amateursports vermehrt die Idee auf, Sportveranstaltungen zu filmen und dabei Bilder live über das Internet zu verbreiten. Überlegungen dazu reichen bis hin zu Lösungen, bei denen spezielle Kameras zum Einsatz kommen, die ihren Fokus durch den Einsatz von Anwendungen der künstlichen Intelligenz selbstständig auf das jeweilige Hauptgeschehen des sportlichen Wettkampfs richten sollen.

Aus datenschutzrechtlicher Perspektive werden durch entsprechende Videoaufnahmen und deren Übertragung eine Vielzahl personenbezogener Daten verarbeitet. Betroffen hiervon können Spieler_innen, Wettkampftreibende, Zuschauer_innen, Schiedsrichter_innen sowie sonstige Anwesende sein. Verarbeitungen zu journalistischen Zwecken werden zwar auf der Basis des Artikels 85 Absatz 2 der DS-GVO privilegiert: So sind mit Blick auf diese Öffnungsklausel die Datenschutzbestimmungen der DS-GVO durch § 12 und § 23 Medienstaatsvertrag für Medienvertreter_innen, wie beispielsweise journalistische Tätigkeiten des Südwestrundfunks, weitestgehend ausgeschlossen. Sonstige Stellen (wie etwa Vertreter_innen von Vereinen) können sich jedoch in aller Regel nicht auf diese Ausnahmen berufen.

Für Datenverarbeitungen im Rahmen der Liveübertragung durch solche sonstigen verantwortlichen

Stellen bedarf es daher einer Rechtsgrundlage nach der DS-GVO. Eine Möglichkeit der Legitimation der Verarbeitungen stellen unter anderem zu dokumentierende Einwilligungen gem. Artikel 6 Absatz 1 Buchstabe a DS-GVO i. V. mit Artikel 7 DS-GVO sämtlicher von den Kameraaufnahmen betroffener Personen dar. Einwilligungen sind im konkreten Kontext aber vielfach kein sinnvolles Mittel: Wenn hierzu nur eine Person (Schieds-/Wettkampfrichter_in, Spieler_innen aus Gastmannschaften o.Ä.) ihre Einwilligung verweigern oder später widerrufen würde, wäre das Streaming auf dieser Grundlage unzulässig, da eine Videoaufzeichnung der Veranstaltung ohne die nicht einwilligende Person faktisch nicht möglich ist. Ob eine Verarbeitung erlaubt ist, wird sich daher im Bereich des Amateursports generell an der Rechtsgrundlage des Artikel 6 Absatz 1 Buchstabe f DS-GVO zu messen haben, und somit vor allem an einer Abwägung der betroffenen Interessen des Verantwortlichen mit denen der Gefilmten, wobei Kinder besonders zu schützen sind. Sportveranstaltungen aus dem Bereich des Spitzensports werden hingegen ohnehin in der Regel durch Medienvertreter_innen übertragen, für die (s.o.) eigene datenschutzrechtliche Anforderungen gelten – unabhängig von der im Vergleich zum Amateursport regelmäßig anderen Interessenlage.

Für eine Abgrenzung von Amateur- und Spitzensport lassen sich generell die folgenden Erwägungen heranziehen: Ein zuverlässiger Indikator dafür, dass Sport als Spitzensport betrieben wird, ist, dass die Sportausübungen den Sporttreibenden als Hauptbeschäftigung (zu Erwerbszwecken) dienen. Soweit eine entsprechende Hauptbeschäftigung nicht vorliegt, kann sich die Zuordnung zum Spitzensport zum Teil auch aus sonstigen Umständen ergeben, etwa, wenn die Sportausübung einen erheblichen Teil der Zeit und Lebensgestaltung der Sporttreibenden einnimmt und eine Teilnahme an der obersten nationalen und internationalen Wettkampfklasse (Liga o. ä.) einer Sportart erfolgt.

Sollte dies nicht der Fall sein, wird generell der Bereich des Amateursports betroffen sein. Innerhalb des Amateursports kann noch weiter zwischen dem Leistungs- und Breitensport unterschieden werden. Der Bereich des Leistungssports ist berührt, wo die Sportausübung einen erheblichen Teil der Zeit und Lebensgestaltung der Sporttreibenden einnimmt und diese nach persönlichen Höchstleistungen streben. Sportliche Wettkämpfe werden regelmäßig zumindest auf überregionalem Niveau bestritten. Im Breitensport steht dagegen der Freizeitaspekt an erster Stelle. Die Sportler_innen treiben vorwie-

Je nachdem, ob Leistungssport oder Breitensport, ob Kinder spielen oder Erwachsene, ist es einfacher oder komplizierter, die Veranstaltungen live zu streamen.

gend Sport, um sich zu bewegen, fit zu halten und soziale Kontakte zu pflegen. Der sportliche Wettkampf ist hierbei vorwiegend auf den regionalen Raum begrenzt. Der Breitensport ist meist von vorwiegend lokalem Interesse und seiner Natur nach nicht immer von Professionalität geprägt.

Im konkreten Kontext des Amateursports, also dem Bereich des Leistungs- und Breitensports, sind mögliche Motive der Verantwortlichen für ein Streaming, etwa für einen Verein werben zu wollen und interessierten Personen die digitale Teilhabe an sportlichen Geschehnissen zu ermöglichen, zwar durchaus nachvollziehbar. Dem stehen jedoch die Interessen der von der Übertragung betroffenen Personen gegenüber, welche durch eine solche Übertragung grundsätzlich in ihrem Recht auf informationelle Selbstbestimmung berührt sind.

Im Bereich des Leistungssports kann dies beispielsweise das Interesse der Sporttreibenden sein, nicht zu Unterhaltungszwecken Dritter zur Schau gestellt zu werden.

Im Breitensport werden Videoaufnahmen vorrangig die schutzwürdige Freizeitausübung der Anwesenden betreffen. Die Interessen gehen hierbei deutlich über die bereits im Bereich des Leistungssports bestehenden hinaus. Die Anwesenden haben ein zusätzliches Interesse daran, keinem vom Streaming ausgehenden Anpassungs- Überwachungs- und Leistungsdruck ausgesetzt zu sein und dadurch in der Unbeschwertheit ihrer sportlichen, schieds- oder wettkampfrichterlichen Betätigung beeinträchtigt zu werden. Zudem sind im Bereich des Breitensports mögliche Selbstzweifel der Sporttreibenden hinsichtlich der eigenen körperlichen Fitness verbreiteter als im Leistungssport oder professionellen Sport. Der mit der Übertragung einhergehende Eingriff wiegt bei Nahaufnahmen nochmals schwerer als bei Aufnahmen in der Totale. Insbesondere bei der Teilnahme an Breitensportveranstaltungen erwarten anwesende Personen zudem grundsätzlich nicht, dass eine fortlaufende Veröffentlichung von deren personenbezogenen Daten erfolgt und Bildmaterial weltweit im Internet abrufbar ist beziehungsweise dort möglicherweise sogar dauerhaft abrufbar bleiben könnte.

Wo entsprechende Aufnahmen gefertigt werden, besteht außerdem die Gefahr, dass diese zweckentfremdet werden könnten. So könnten etwa Ausschnitte ungewünscht auf Videoplattformen wie YouTube, TikTok o.Ä. landen. Dies betrifft Inhalte von sportlicher (etwa Siege, Tore, Rekorde), sozialer (etwa Rangeleien, Pöbeleien) oder sogar gesundheitlicher (etwa Verletzungen) Relevanz. Gerade im Breitensport, aber auch im Leistungssport, haben betroffene Personen ein grundsätzliches Interesse daran, dass entsprechende Situationen, insbesondere solche mit negativen Auswirkungen wie Fehlern oder unvorteilhaften Abbildungen, nicht mit der Gefahr eines Kontrollverlustes hinsichtlich solcher Aufzeichnungen einem größeren Publikum offenbart werden.

Es gilt hier im jeweiligen Einzelfall – unter Einbeziehung der genannten Erwägungen – zwischen den berechtigten Interessen des datenschutzrechtlich Verantwortlichen und den zuvor dargestellten Interessen und Rechten der von den Aufzeichnungen betroffenen Personen abzuwägen. Es kann hierbei grundsätzlich festgehalten werden: Je tiefer die sportliche Spiel- beziehungsweise Wettkampfklasse, desto geringer einerseits das Interesse an der Veröffentlichung und desto größer andererseits der Freizeitcharakter der von der Übertragung betroffenen Tätigkeit und damit die Schutzbedürftigkeit für betroffene Personen. Die Interessen und Rechte der betroffenen Personen überwiegen zudem, wo die Intimsphäre betroffen sein könnte.

Innerhalb des Breitensports und der üblichen Sportveranstaltungen unterer Spiel-/Wettkampfklassen wird deshalb regelmäßig ein Überwiegen der Interessen der betroffenen Personen gegenüber den Interessen der Verantwortlichen festzustellen sein, was dem Wunsch einer Übertragung der Veranstaltung entgegensteht.

Im Rahmen des Leistungssports können die Interessen des Verantwortlichen hingegen durchaus überwiegen. In einer besonderen Situation begründeten Widersprüchen gegen die Videoaufzeichnung, etwa durch die Gastmannschaft oder Wettkampfbeziehungsweise Schiedsrichter_innen, ist in geeigneter Form Rechnung zu tragen. Dem Publikum sollte von Vornherein durch entsprechende Kennzeichnung die Möglichkeit eröffnet werden, sich der Aufnahme mit für das Streaming eingesetzten Kameras zu entziehen.

Insbesondere dort, wo Sportveranstaltungen von Kindern Gegenstand des Streamings sein sollen,

überwiegen die Schutzbedürftigkeit und die Interessen, Grundrechte und Grundfreiheiten der minderjährigen betroffenen Personen gem. Artikel 6 Absatz 1 Buchstabe f DS-GVO gegenüber den Interessen des Verantwortlichen. Das Streaming von Veranstaltungen, bei denen sich Kinder sportlich betätigen, wird somit als allgemein unzulässig betrachtet.

Nach der sich u. a. aus der sportlichen Spiel- und Wettkampfklasse ergebenden Schutzbedürftigkeit richten sich generell auch die Anforderungen, die i. S. von Artikel 32 DS-GVO an geeignete technische und organisatorische Maßnahmen zur Umsetzung eines angemessenen Schutzniveaus zu stellen sind. Umfassen können solche beispielsweise eine Beschränkung der Zugriffsmöglichkeiten auf bestimmte Nutzergruppen (z. B. durch Passwortschutz), ein Livestreaming ohne eine dauerhafte Speicherung der Übertragung, die Beschränkung des Aufnahmebereichs auf Spiel- und Wettkampfflächen und Beschränkungen des Aufnahmewinkels auf die Totale.

Zu beachten ist zudem, dass, u. a. an den Zugängen zu den vom Streaming betroffenen Wettkampfbereichen, deutlich auf die Übertragung hinzuweisen ist (etwa durch Hinweisschilder) und dabei die Informationen gem. Artikel 13 DS-GVO zu erteilen sind.

Für ein Streaming des Trainingsbetriebs, also abseits des Wettkampfbereichs, gelten verschärfte Anforderungen. Dem Training kommt – außerhalb des Profibereichs – generell ein noch deutlicherer Freizeitcharakter zu. Die Sporttreibenden treffen sich nicht nur zu Wettkampfzwecken, sondern gleichzeitig zum sozialen Austausch. Hierbei ist die Atmosphäre regelmäßig gelöst. Die Sporttreibenden sind nicht nur in ihrem Recht auf informationelle Selbstbestimmung, sondern auch in ihrer schützenswerten Sozial- oder sogar Privatsphäre betroffen. Die anzulegenden Hürden sind somit höher.

Aufnahmen des Trainings können nur zulässig sein, soweit dies zur Gestaltung des Trainings erforderlich ist, also wenn eine Beobachtung des Trainings durch Trainer_in oder Dritte nicht ausreichen kann, um dem Trainingszweck gerecht zu werden. Für den Amateurbereich ist eine solche Konstellation kaum denkbar, weshalb permanente Aufnahmen des Trainingsbetriebes insoweit generell nicht zu rechtfertigen sind. Wo dies ausnahmsweise im Einzelfall erforderlich ist, z. B. zur Analyse von Spielzügen, können ausnahmsweise zeitlich begrenzte Aufnahmen erstellt werden. Diese müssen den Sportler_innen aber zumindest vorab angekündigt werden, auf die entsprechenden Situationen begrenzt bleiben und sind, soweit sie gespeichert werden, baldmöglich wieder zu löschen.

Besonders zu beachten sind des Weiteren räumlich abgegrenzte Aufwärmbereiche. Sporttreibenden bieten diese Bereiche einen besonders zu schützenden Rückzugsraum. Dort werden u. a. gymnastische Aufwärmübungen und auch feste Rituale zur Wettkampfvorbereitung durchgeführt. Teilweise wird die Wettkampfkleidung an- und ausgezogen. Die Bereiche können zu sportphysiotherapeutischen und medizinischen Behandlungen nach akuten Verletzungen genutzt werden. Außerdem spielen sich hierin oftmals emotionale Szenen der Freude, aber auch der Frustverarbeitung, ab, die keinesfalls für die Öffentlichkeit bestimmt sind. Sportler_innen und betreuende Personen wollen in solchen Momenten grundsätzlich keiner Beobachtung ausgesetzt sein. Daneben ist der Zugang zu den Aufwärmbereichen Zuschauenden überwiegend ohnehin versagt. Entsprechend kann auch keine Übertragung von Szenen aus diesen Bereichen zur Darstellung des Sportereignisses erforderlich sein. Betroffen ist hier regelmäßig die Privatsphäre und teilweise auch die besonders geschützte Intimsphäre. Das Streaming von Szenen aus räumlich abgegrenzten Aufwärmbereichen scheitert daher generell an den überwiegenden Interessen von Sportler_innen sowie Betreuer_innen.

9.5.6 Vereinsmitglied als Jubilar wider Willen

Zum runden Geburtstag wurden neben dem Namen die vollständige Wohnanschrift sowie das komplette Geburtsdatum eines seit langem passiven Vereinsmitglieds in der Vereinszeitung eines Sportvereins veröffentlicht. Der so Geehrte wollte davon aber gar nichts wissen und beschwerte sich bei uns.

In der Vereinszeitung eines größeren Sportvereins wurde in der Rubrik „Wir gratulieren zum Geburtstag“ der Name, die private Wohnanschrift sowie das Geburtsdatum eines Vereinsmitglieds veröffentlicht. Der Jubilar nimmt jedoch seit Jahrzehnten nicht mehr aktiv am Vereinsleben teil. Eine Einwilligung zur genannten Veröffentlichung hatte er nicht erteilt. Daher richtete er ein Auskunftsersuchen an den Sportverein. Dieser reagierte per

Kurznachricht deutlich nach dem Fristablauf von einem Monat auf das Auskunftsersuchen – jedoch nicht inhaltlich. Daraufhin richtete der Geehrte eine Beschwerde an unsere Behörde.

Von Seiten des Vereins wurde mitgeteilt, dass Gratulationen im Einklang mit der Ehrenordnung vorgenommen würden. Eine Veröffentlichung in der Vereinszeitung sei jahrzehntelange Praxis ohne ernsthafte Beschwerden. Bei der Jahreshauptversammlung des Vereins sei auf die Möglichkeit der formlosen Mitteilung an den Verein, dass keine Gratulation gewünscht sei, hingewiesen worden. Der Jubilar habe außerdem anlässlich seines vergangenen Geburtstagsjubiläums vor zehn Jahren keine Einwendungen gehabt und ein Präsent in diesem Zusammenhang gerne entgegengenommen. Nach seiner ersten Anfrage im Hinblick auf die aktuelle Veröffentlichung sei jedoch ein interner Vermerk über den Widerspruch erfolgt.

Eine abschließende Stellungnahme des Vereins an den Jubilar erging zirka drei Monate später mit der Bestätigung über den Widerruf der Datenverarbeitung. Der Verein stütze die Veröffentlichung der personenbezogenen Daten in der Vereinszeitung auf eine konkludent erteilte Einwilligung. Es bestehe hilfsweise aber auch ein berechtigtes Interesse des Vereins an der Vereinspflege, die jahrzehntelang unwidersprochen so „gelebt" worden sei. Nach dem Widerspruch beziehungsweise Widerruf werde natürlich keine entsprechende Gratulation beziehungsweise Beglückwünschung mehr erfolgen.

Wir mussten feststellen, dass die genannte Ehrenordnung keine Bestimmungen zu den Veröffentlichungsmodalitäten in der Vereinszeitung enthielt und die angebotene Widerspruchslösung nicht den Erfordernissen einer informierten Einwilligung entsprach. Eine Abwägung im Hinblick auf die berechtigten Vereinsinteressen (vgl. Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO) wurde nicht ausreichend und substantiiert durchgeführt. Eine nur elektronisch ermöglichte Widerspruchslösung verstößt dabei ebenfalls gegen die Vorgaben der DS-GVO. Für die Veröffentlichung in der beschriebenen Weise lag demnach keine Rechtsgrundlage vor.

Sinn und Zweck der DS-GVO ist es, betroffene Personen vor einer beeinträchtigenden Datenverarbeitung zu schützen. Zur Gewährleistung dieses Schutzes sind in Artikel 5 DS-GVO wesentliche Grundsätze für die Verarbeitung von personenbezogenen Daten vorgesehen, wozu nach Artikel 5 Absatz 1 Buchstabe a DS-GVO insbesondere eine rechtmäßige Datenverarbeitung gehört. Damit eine Verarbeitung von personenbezogenen Daten auf eine rechtmäßige Weise erfolgt, muss diese entweder auf Grundlage einer Einwilligung der betroffenen Person oder einer sonstigen einschlägigen Rechtsgrundlage erfolgen (vgl. EwGr. 40). Demzufolge bedarf auch die Veröffentlichung von Daten eines Vereinsmitglieds in der Vereinszeitung einer einschlägigen Rechtsgrundlage.

In unserem Fall sahen wir entgegen der Auffassung der verantwortlichen Stelle den Tatbestand der Einwilligung nach Artikel 6 Absatz 1 Satz 1 Buchstabe a, 7, 4 Nummer 11 DS-GVO nicht als erfüllt. Nach der Legaldefinition aus Artikel 4 Nummer 11 DS-GVO ist unter einer Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung zu verstehen, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Eine wesentliche Voraussetzung ist neben der hinreichenden Bestimmtheit, dass die Einwilligung in informierter Weise abgegeben wird. Die betroffene Person muss also die Auswirkungen und Tragweite der Erklärung abschätzen können. Ferner bedarf eine Einwilligung zwar keiner besonderen Form, weshalb sie auch durch ein konkludentes oder schlüssiges Verhalten erteilt werden kann. Dies setzt jedoch unter anderem ein eindeutiges Erklärungsbewusstsein der betroffenen Person voraus, das einen Rückschluss auf den eindeutigen Willen des Erklärenden zulässt. Die Voraussetzungen für eine wirksame Einwilligung wurden uns jedoch von der Verantwortlichen nicht hinreichend schlüssig dargelegt. Die Nachweispflicht für das Vorliegen der Voraussetzungen der Einwilligung liegt nach Artikel 7 Absatz 1 DS-GVO beim Verantwortlichen, also beim Verein.

Die Veröffentlichung der Daten war auch nicht aufgrund der Wahrung von berechtigten Interessen des Verantwortlichen nach Artikel 6 Absatz 1 Satz 1 Buchstabe f DS-GVO gerechtfertigt. Danach ist

die Verarbeitung von personenbezogenen Daten rechtmäßig, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen […]. Es kommt also auf eine umfassende Interessenabwägung im konkreten Einzelfall an. Zu den berechtigten Interessen kann auch das Interesse des Vereins zur Vereinspflege aufgrund der jahrzehntelangen Praxis gehören. Mit in die Abwägung einzubeziehen sind dabei allerdings auch vernünftige Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, vgl. EwGr. 47. Insoweit ist es Aufgabe des Verantwortlichen, aufgrund eines schlüssigen Sachvortrags eine umfassende Interessenabwägung vorzunehmen. Eine Abwägung im Hinblick auf die berechtigten Vereinsinteressen (vgl. Art. 6 Abs. 1 Satz 1 Buchstabe f DS-GVO) wurde jedoch nicht ausreichend und substantiiert durchgeführt.

Insgesamt mussten wir nach unserer datenschutzrechtlichen Prüfung feststellen, dass keine Rechtsgrundlage für die Veröffentlichung der Daten zum Geburtstagsjubilar vorlag, mithin war die Datenverarbeitung rechtswidrig.

Der Fall zeigt, dass künftig nur solche Geburtstage / Gratulationen veröffentlicht werden sollten, bei denen jeweils vorher eine ausdrückliche und informierte Einwilligung des zu Ehrenden vorliegt.

Um Vereine hinsichtlich ihrer datenschutzrechtlichen Verantwortung bei ihren ihren vielfältigen Tätigkeiten zu unterstützen, haben wir verschiedene Handreichungen, ein Online-Tool, mit dem Vereine ihre Datenschutzhinweise innerhalb kurzer Zeit „zusammenbasteln“ können, und weitere Hinweise etwa zu Fotos auf unserer Homepage bereitgestellt. So einfach hier der Grundsatz „Frag den Betroffenen“ ist, so einfach lautet ein weiterer Grundsatz: Wenn Vereine unsicher sind, was die Datenverarbeitungen betrifft, können sie uns kontaktieren und sich beraten lassen. Bei Bedarf bieten wir auch Veranstaltungen in unserem Bildungszentrum speziell zu Themen von Vereinen an, so wie wir es z. B. bei der Einführung unseres Tools DS-GVO.clever getan haben.

9.5.7 „GAME, SET, MATCH“: Veröffentlichung von Sperren im Leistungssport

Ein Sportler aus dem Bereich der Ballsportarten wandte sich an unsere Behörde und berichtete uns, dass er durch eine internationale Sportvereinigung zu einer Sperre und einer erheblichen Geldstrafe „verurteilt“ wurde. Dem Sportler wurde von einem britischen Sport-Dachverband vorgeworfen, bei einem Turnier in einem sonnigen Urlaubsland den Versuch unternommen zu haben, eine Wildcard zu erwerben. Diese Privilegierung ist jedoch vom Ermessen der Veranstalter_innen oder der Genehmigung des gastgebenden nationalen Verbandes abhängig und kann nicht einfach „erkauft“ werden. Auch soll er einen anderen Spieler aufgefordert haben, absichtlich ein Spiel zu verlieren.

Die Meldung an den Sport-Dachverband erfolgte über ein sogenanntes „Whistleblowing System“ des Verbandes. Nach einem rechtskräftigen Urteil habe sich der Sportler der Wettmanipulation schuldig gemacht. Die internationale Organisation übermittelte die personenbezogenen Daten des Spielers und die Tatsache des Sportverbotes an den deutschen Fachverband.

Gleichfalls wurden die Umstände der Sperre und die personenbezogenen Daten des Sportlers auf der Homepage der intenationalen Organisation veröffentlicht. Der Sportler berichtete uns, dass er im Bekannten- und Freundeskreis nunmehr dauerhaft als Betrüger „gebrandmarkt“ sei. Auch Personen, die mit der Sportart nichts zu tun hätten, wüssten detailliert über seinen Fall Bescheid.

Eine Sichtung der Homepage durch unsere Behörde ergab, dass tatsächlich auf einer Sanktionsliste neben dem Namen unseres Beschwerdeführers auch eine Vielzahl anderer gesperrter Spieler_innen wegen Dopings oder Korruption unter Benennung der Nationalität und des zugrundeliegenden Deliktes genannt wurden.

Anzumerken ist, dass es sich bei dem Beschwerdeführer nicht um einen professionellen Tennisstar handelt. Vorliegend geht es um einen jungen talentierten Sportler, der sich beim Weltverband registrieren ließ. Gemäß den Statuten ist dies auch eine der Voraussetzungen, um an internationalen Turnieren teilnehmen zu dürfen. Ungeachtet der

sportlichen Ziele erfolgte die Teilnahme an Turnieren in erster Linie, um seinem Hobby nachgehen zu können.

Zwar besteht durchaus ein Interesse daran, all jene Sportler_innen zu sanktionieren, die bei der Ausübung der sportlichen Betätigung in erheblichem Maße gegen die Regeln und den Codex verstoßen haben. Darunter fallen insbesondere der Bereich der Wettmanipulation und Verstöße gegen das Anti-Doping. Für uns ist durchaus nachvollziehbar, dass Wettkampfveranstalter und Sportverbände in geeigneter Weise darüber zu informieren sind, über welchen Sportler eine Sperre verhängt wurde. Damit soll aber ausschließlich der Zweck verfolgt werden, dass diese Sportverbände ihren Verpflichtungen nachkommen können.

Aus unserer Sicht ist die vorliegende Veröffentlichung von personenbezogenen Daten und sportinternen Schiedssprüchen aus Disziplinarverfahren im Internet durch Sportvereinigungen in der bislang durchgeführten Art und Weise aus datenschutzrechtlicher Sicht nicht zulässig.

Unzulässig sind insbesondere die Veröffentlichung der Sanktionsentscheidungen mit der Namensnennung und der Datenweitergabe an Dritte.

Die DS-GVO war hier gegeben, da es nach dem Marktortprinzip nicht entscheidend ist, wo ein Unternehmen seinen Sitz hat, sondern, ob es die Dienstleistungen in der Union anbietet und damit EU-Bürger_innen betroffen sind (Artikel 3 Abs. 2 DS-GVO).

Datenschutz gilt auch für Leistungssportler_innen.

Wir wandten uns an die deutsche Verbindungsstelle des Sport-Dachverbandes und erhielten eine ausführliche Sachverhaltsdarstellung und Begründung zur Vorgehensweise.

Entschieden mussten wir allerdings der vorgetragenen Argumentation des Sport-Dachverbandes entgegentreten. Demnach soll die Veröffentlichung von Sanktionen in erster Linie eine abschreckende Wirkung auf andere Sportler entfalten. Dieses harte Vorgehen sei deshalb von entscheidender Bedeutung, da gerade auf niedrigen Ligaebenen des Profisports die meisten Korruptionsdelikte begangen würden. Aus welchen Gründen es hierzu einer namentlichen Benennung des verurteilten Sportlers bedarf, konnte nicht beantwortet werden. Anzunehmen ist daher, dass es hier gerade darauf ankommt, gezielt die Person der Sportler_innen der Öffentlichkeit preis zu geben und dauerhaft zu stigmatisieren. Gerade diese Art der Verletzung des Schutzes personenbezogener Daten hat ein hohes Risiko für die persönlichen Rechte und Freiheiten der Sportler_innen als natürlicher Personen zur Folge. Trotz entsprechender rechtlicher Darstellung durch den Sportverband ist für uns eine einschlägige Rechtsgrundlage zur Veröffentlichung dieser Daten nicht ersichtlich.

So besteht gerade keine Notwendigkeit, dass neben den betroffenen Sportverbänden auch die breite Öffentlichkeit und somit jedermann mit Zugang zum Internet über den Namen und den Grund der Sperre Auskunft erhält.

Wie sich immer wieder in der Berichterstattung der Medien zeigt, hat für Sportler_innen die Veröffentlichung eine enorme „Prangerwirkung“, die mit sozialer Ausgrenzung und Stigmatisierung sowie dem Ausbleiben von Angeboten zur Teilnahme an Wettbewerben einhergeht.

Nach unserer Auffassung ist deswegen die uferlose Information der Allgemeinheit über eine Homepage eines Fachverbandes oder sonstiger privater Organisationen unzulässig.

Eine derartige Veröffentlichung bewirkt, dass jedermann, auch ohne anzuerkennendes Informations-

bedürfnis, jederzeit über gängige Suchmaschinen prüfen kann, über wen welche Sperren im Bereich Doping und Wettmanipulation verhängt wurden. Nach Art. 6 Abs. 1 lit. c) DS-GVO ist eine Datenverarbeitung zwar rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Nach Art. 6 Abs. 3 DS-GVO müssen derartige Verpflichtungen aber ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zum verfolgten legitimen Zweck stehen. Hier wurde von der Organisation jedoch keinerlei Unterscheidung vorgenommen, ob es sich um eine/n TOP-Spieler_in handelt oder um eine/n Spieler_in, der/die durch die Ausübung des Sports keine Einkünfte erzielt. In derartigen Fällen ist der Verhältnismäßigkeitsgrundsatz umso genauer zu beachten.

Die fehlende Angemessenheit in der praktizierten Veröffentlichung von personenbezogenen Daten verstößt mithin gegen die datenschutzrechtlichen Grundsätze. Eine zwischenzeitliche Sichtung durch uns ergab, dass der Sportler zwar zwischenzeitlich von der Sanktionsliste gelöscht wurde. Zu unserer Verwunderung mussten wir allerdings feststellen, dass sich weiterhin auf der Homepage ein ausführlicher Informationstext zur Art und Dauer der zwischenzeitlich getilgten Strafe unter namentlicher Benennung des Sportlers befindet. Erschwerend kommt hinzu, dass Leser durch den Betreiber mit der Bereitstellung von Verknüpfungsmöglichkeiten zu sozialen Netzwerken und Co. geradezu zum „Sharing“ animiert werden.

Nicht nur aus diesem Grund sehen wir es als erforderlich an, der Sache weiter nachzugehen.

9.5.8 Polizei stattet Streifenwagen mit Kameras aus

Das Innenministerium Baden-Württemberg hat vor einiger Zeit bekannt gegeben, dass mehr als 100 Streifenwagen der Verkehrspolizei innerhalb der regionalen Polizeipräsidien mit fest verbauten Dashcam-Systemen ausgestattet wurden. Darüber berichtete auch der Südwestrundfunk.

Unsere Behörde wurde bereits frühzeitig in das Projekt des Polizeivollzugsdiensts einbezogen. Datenschutzrechtliche Hinweise unsererseits fanden dabei stets unmittelbaren Einfluss in der weiteren Planungs- und Umsetzungsphase. Unverkennbar war jedoch, dass der Polizeivollzugsdienst im Interesse seiner Aufgaben im Zusammenhang mit der Strafverfolgung und Ahndung von Ordnungswidrigkeiten wiederholt den Vorstoß unternahm, die Einsatzbereiche der Dashcams in Teilbereichen sukzessiv auszuweiten. Von unserer Behörde wurden daher auch die rechtlichen Grenzen zum Dashcam-Einsatz aufgezeigt, um sicherzustellen, dass datenschutzrechtlichen Belangen in ausreichendem Maße Rechnung getragen wird.

So war der vorgesehene Einsatz der Dashcams innerhalb der Streifenwagen und deren Erforderlichkeit in unserem Erstgespräch mit der Polizei im Jahr 2020 noch ausschließlich auf die Verfolgung von Verkehrsverstößen im Zusammenhang mit der Bildung von Rettungsgassen beschränkt.

Anschaulich wurde uns zum damaligen Zeitpunkt dargestellt, dass das gesteigerte Verkehrsaufkommen in den letzten Jahren zu erheblichen Problemen im Hinblick auf die Sicherheit und die Leichtigkeit des Verkehrs geführt habe. Ein verkehrspolizeilicher Schwerpunkt liege hier in der Bildung und Überwachung von Rettungsgassen zur Rettung und Bergung von Unfallopfern. Die Videoaufzeichnung mittels Dashcam solle hier die Möglichkeit eröffnen, neue aussagekräftige Beweismittel zu gewinnen und die Beweisführung zu verbessern.

In der weiteren Planungsphase wurde die Zielrichtung des Kameraeinsatzes auf sämtliche Verkehrsverstöße erweitert. Hiergegen wurde von unserer Behörde dargelegt, dass es sich bei einem staatlichen Einsatz von Kameras zur Überwachung des öffentlichen Straßenverkehrsraums um einen intensiven Grundrechtseingriff handelt, der keinesfalls mit der Verfolgung von Bagatelldelikten und einfachen Ordnungswidrigkeiten gerechtfertigt werden kann.

Im Ergebnis wurde uns von Seiten der Polizei hierzu mitgeteilt, dass man mit den Dashcam-Aufzeichnungen priorisiert die Rettungsgassenproblematik angehen möchte, sich aber gleichfalls im Hinblick auf die weitere Entwicklung auch die Option der Verfolgung von erheblichen Verkehrsverstößen offenhalten möchte.

Als Rechtsgrundlage kann in diesen Fällen § 100h Absatz 1 Nummer 1 der Strafprozessordnung (StPO) herangezogen werden, zur Verfolgung von erheb-

lichen Ordnungswidrigkeiten in Verbindung mit § 46 Absatz 1 des Ordnungswidrigkeitengesetzes (OwiG). Nach § 100h Absatz 1 Nummer 1 StPO dürfen Bildaufnahmen, als spezielle Form der Datenverarbeitung, auch ohne Wissen der betroffenen Person hergestellt werden, wenn die Erforschung des Sachverhalts auf andere Weise weniger erfolgversprechend oder erschwert wäre. Diese Voraussetzungen liegen vor, da die Beweisführung ohne die Dashcam-Aufnahmen trotz des möglichen Zeugenbeweises durch die Polizeibeamt_innen erheblich erschwert und die nachträgliche Aufklärungsmöglichkeit damit weniger erfolgversprechend wäre.

Eine klare Absage erteilten wir den polizeilichen Überlegungen einer Einsatzausweitung auf einen dauerhaften Live-Monitoring-Betrieb der Kameras. Dies begründeten wir damit, dass durch ein ständiges „Mitlaufen" der Videokameras während einer ganzen Streifenfahrt der in § 100h Absatz 1 Nummer 1 StPO genannte Zweck (Beweisführung) nicht erreicht wird. Eine Live-Bild-Übertragung ist daher nur dann zulässig, wenn bereits bei Aktivierung dieser Funktion tatsächliche Anhaltspunkte für den Anfangsverdacht einer Straftat oder Ordnungswidrigkeit vorliegen und gleichzeitig eine Bildaufzeichnung gestartet wird.

Parallelen zur Videotechnik in privaten Fahrzeugen können in rechtlicher Hinsicht nicht gezogen werden, weil die Rechtsgrundlage für die Anwendung von Kameratechnik in privaten Fahrzeugen (namentlich Artikel 6 Absatz 1 Buchstabe f DS-GVO) für Fahrzeuge von öffentlichen Stellen aufgrund des hoheitlichen Tätigwerdens und des damit verbundenen Grundrechtseingriffs nicht anwendbar ist.

Aufgrund unserer ablehnenden Haltung hat die Polizei die Pläne zur Live-Bild-Übertragung fallen gelassen.

Demnach soll sich der Einsatz der Dashcams ausschließlich auf die Überwachung zur Einhaltung der Rettungsgasse sowie zur Verfolgung strafrechtlicher Verkehrsverstöße und erheblicher Verkehrsordnungswidrigkeiten beschränken.

Unserem Hinweis, dass das Dashcam-System den Anforderungen an Transparenz und Nachvollziehbarkeit entsprechen muss, berücksichtigte der

Krankenwagen müssen im Notfall schnell zum Unfallort kommen können, daher: Rettungsgasse bilden.

Polizeivollzugsdienst ebenfalls: Im Konzept fand insbesondere das Thema der Dokumentation und Protokollierung i.S. von § 76 Absatz 2 des Bundesdatenschutzgesetzes (BDSG) in Verbindung mit § 500 Absatz 1 StPO und ggf. § 46 Absatz 1 OwiG vollumfänglich Berücksichtigung. Eine vollumfängliche Dokumentationspflicht kommt immer dann zum Tragen im Falle einer Einsichtnahme der Polizei in gespeicherte Bildaufzeichnungen.

Bereits frühzeitig wurde uns zugesichert, dass diese Anforderungen im Rahmen des Ausschreibungsverfahrens Einfluss finden. Gemäß der offiziellen Beschreibung des Dashcam-Systems werden die auf einer verschlüsselten SD–Karte (engl. Secure Digital Memory Card) gespeicherten Daten mittels einer Auswertesoftware automatisiert übertragen sowie protokolliert und zentral recherchierbar abgelegt.

Die in den Streifenwagen der Verkehrspolizei eingebauten Dashcam-Systeme befinden sich seit Juni 2022 im Einsatz. Aus der Presse konnten wir entnehmen, dass der Einsatz der Kameras bereits zu einer Vielzahl von Bußgeldverfahren und Fahrverboten geführt hat. Im Rahmen einer wiederkehrenden Evaluation und auch durch die Wahrnehmung von aufsichtsrechtlichen Kontrollterminen werden wir diese Thematik nicht aus dem Blickfeld verlieren. Derartige Systeme leiden gerade in der Anfangszeit oft an „Kinderkrankheiten".

9.5.9 Polizeiliche Videoüberwachung an Kriminalitätsbrennpunkten als Antwort auf die „Stuttgarter Krawallnacht"

Vielen sind noch die Bilder der Zerstörung aus der „Stuttgarter Krawallnacht" vom 20./21. Juni 2020 vor Augen.

Als unmittelbare Folge wurde eine Sicherheitspartnerschaft zwischen dem Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg und der Landeshauptstadt Stuttgart vereinbart, die – aufgrund der Einbeziehung unserer Behörde – zu einer datenschutzkonformen Konzeption geführt hat.

Derartigen Szenarien soll zukünftig mit effektiven rechtsstaatlichen Mitteln der Gefahrenprävention entgegengetreten werden. Ein wichtiger Stützpfeiler hierfür ist der Einsatz von Videokameras in eng begrenzten Bereichen der Stuttgarter Innenstadt.

Die polizeiliche Videoüberwachung ist in § 44 Absatz 3 des Polizeigesetzes Baden-Württemberg (PolG) geregelt. Nach dieser Vorschrift „kann die Polizei an öffentlich zugänglichen Orten Bild- und Tonaufzeichnungen von Personen anfertigen, wenn sich die Kriminalitätsbelastung dort von der des übrigen Gemeindegebiets deutlich abhebt und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist".

Der Zweck der offenen polizeilichen Bild- und Tonaufzeichnungen besteht aber auch darin, das Sicherheitsgefühl an lokalen Brennpunktbereichen zu erhöhen und vorrangig erhebliche Straftaten (unter anderem Körperverletzung, Bedrohung, Nötigung und Raub) zu reduzieren.

Nachdem wir aus der Presse von den Plänen für eine Videoüberwachung erfahren und die Beteiligten um Einbeziehung gebeten hatten, erfolgte eine Einbindung unserer Behörde bis zur finalen Inbetriebnahme der Kameras. Erfahrungen mit bereits existierenden Konzeptionen anderer Großstädte in Baden-Württemberg, sowie mit erfolgten Evaluationen wirkten sich positiv auf den Gesamtablauf des Verfahrens aus. Die von uns eingebrachten datenschutzrechtlichen Hinweise aber auch Kritikpunkte fanden zu jedem Zeitpunkt des Planungsverfahrens Gehör und wurden auch unmittelbar im weiteren Verlauf der Konzeption eingearbeitet und umgesetzt. Maßstab waren stets die strengen Voraussetzungen aus den gesetzlichen Regelungen für eine polizeiliche Videoüberwachung.

So stand eine flächendeckende und zeitlich uneingeschränkte Videoüberwachung der Stuttgarter Innenstadt für unsere Behörde zu keinem Zeitpunkt zur Debatte. Die Stuttgarter Polizei ist vielmehr bereits zu einem frühen Verfahrenszeitpunkt unserem Hinweis nachgekommen, dass die eigentlichen „Kriminalitätsbrennpunkte" zu ermitteln und anhand belastbarer Zahlen aus der zurückliegenden polizeilichen Kriminalitätsstatistik (PKS) zu belegen sind. Bagatelldelikte und bloße Ordnungsstörungen sollten bei der Auswertung keine Berücksichtigung finden.

Das Ergebnis wurde uns vorgelegt und anschließend diskutiert. Die Analyse hat gezeigt, dass sich die der Kriminalitätsbelastung in den Bereichen des Oberen Schlossgartens, des Schlossplatzes und des Kleinen Schlossplatzes von der des übrigen Stadtgebiets besonders in den Wochenendnächten und Nächten vor Feiertagen deutlich abhebt.

Die vorstehenden Erwägungen haben in die endgültige Konzeption Eingang gefunden. Durch den offenen Einsatz von Videotechnik in Form des Live-Monitorings und einer zeitlich begrenzten Aufzeichnung sollen potentielle Straftäter von der Begehung erheblicher Straftaten abgehalten werden. Gleichfalls soll die Effizienz und Effektivität polizeilicher Maßnahmen verbessert und so das Sicherheitsgefühl der Bevölkerung gestärkt werden.

Beim Live-Monitoring erfolgt eine unmittelbare Bildübertragung auf einen Bildschirm verbunden mit einer Beobachtung und Auswertung des dargestellten Kamerabereichs in Echtzeit durch eine natürliche Person.

Hierdurch soll in erster Linie das schnelle und frühzeitige Erkennen polizeilich relevanter Ereignisse und die Einleitung polizeilicher Eingriffsmaßnahmen vor Ort ermöglicht und die Reaktionszeit der Eingreifkräfte erheblich verkürzt werden. Die erhobenen Videobilder werden in das Führungs- und Lagezentrum des Polizeipräsidiums Stuttgart übertragen und dort ausgewertet.

Basierend auf dem Grundsatz der Datensparsamkeit erfolgt eine Löschung der aufgezeichneten Daten grundsätzlich automatisiert nach 72 Stunden. Ein weiterer Speichergrund i.S. von § 44 Absatz 10 PolG könnte allerdings vorliegen, wenn die gespeicherten Bilder für ein konkretes Ermittlungsverfahren beweiserheblich wären.

Das Polizeipräsidium Stuttgart hat nicht nur die jeweiligen Kamerastandorte auf einer Gesamtkarte grafisch dargestellt; wichtig war uns auch, dass mit zahlreichen Hinweisschildern unmittelbar vor Ort der Transparenzpflicht ausreichend nachgekommen wird. Den Ausführungen der Polizei zufolge werden 27 Kameras in den Bereichen Schlossplatz, Kleiner Schlossplatz, Parkanlage Oberer Schlossgarten, Zu-/Ausgänge der ÖPNV-Haltestelle Schlossplatz in die angeführten Bereiche eingesetzt.

Mittels technischer Maßnahmen wird dafür Sorge getragen, dass Innen- und Außenbereiche der Gastronomie, sowie sonstiger Gewerbebetriebe nicht von der Überwachung umfasst werden.

Die Stuttgarter Polizei weist auch in ausreichender Form auf die allgemeinen Informationen zur Verarbeitung der personenbezogenen Daten i.S. von § 85 PolG hin. Nach Aussage der Polizei halten sich die datenschutzrechtlichen Auskunftsanträge derzeit noch in Grenzen. Wir werden die weitere Entwicklung, insbesondere aber das Ergebnis der ersten Evaluation mit großem Interesse verfolgen.

10. Einblick in die Dienststelle

10.1 Organisatorische Entwicklung schreitet voran

Die Dienststelle des Landesbeauftragten für den Datenschutz und die Informationsfreiheit wurde in den vergangenen Jahren vom Landtag dankenswerterweise mehrmals mit zusätzlichen Personalstellen ausgestattet. Dies war auch für das Jahr 2022 der Fall. Für das Themenfeld „Künstliche Intelligenz" genehmigte der Landtag zwei Stellen sowie zwei weitere Stellen im Verwaltungsbereich zur Stärkung des Bildungszentrums. Um intensiv den Beratungs- und Fortbildungsbedarf über den Datenschutz an Schulen des Landes zu begleiten, haben wir drei befristete Stellen erhalten.

Der Personalaustausch mit den Ministerien und Behörden der Landesverwaltung konnte durch Abordnungen (also durch das „Ausleihen" von Personen, die zeitweise eine Tätigkeit in einer anderen Behörde wahrnehmen) dabei weiter intensiviert werden. Aktuell sind zwei Personen aus unserer Dienststelle zu Ministerien abgeordnet, im Gegenzug konnten drei Personen aus der Landesverwaltung zu uns abgeordnet werden. Zudem wurden auch Versetzungen, also der dauerhafte Wechsel von Personen an eine andere Dienststelle, vollzogen.

Ein solcher Austausch ist für die Arbeit in unserer Dienststelle in mehrfacher Hinsicht erforderlich: Zum einen erhöht die Möglichkeit des (zeitweisen oder endgültigen) Wechsels in die übrige Landesverwaltung mit Blick auf die sich hieraus ergebenden Perspektiven in der Personalentwicklung erheblich die Attraktivität der Arbeit an unserer Dienststelle. Der Personalaustausch gibt darüber hinaus Personen aus anderen Behörden die Möglichkeit, neue Erfahrungen und Einblicke zu gewinnen und insbesondere Interesse an den unserer Behörde obliegenden Themen des Datenschutzes und der Informationsfreiheit zu entwickeln und diese Rechtsgebiete besser kennenzulernen. Auch können Mitarbeitende aus unserer Dienststelle beim Wechsel (zurück) in die übrige Landesverwaltung ihre Kenntnisse und Erfahrungen auf den Rechtsgebieten des Datenschutzes und der Informationsfreiheit mitnehmen, dort als Multiplikatoren weitergeben und so insgesamt die Beachtung dieser Themen und der einschlägigen Vorschriften fördern.

Nicht zuletzt werden durch einen regelmäßigen Personalaustausch etwaige Berührungsängste zwischen den Behörden abgebaut, was den Wissensfluss in der Landesverwaltung insgesamt und namentlich die Effektivität unserer Beratung anderer Dienststellen ganz erheblich verbessern kann. Wir hoffen daher sehr, dass wir den Personalaustausch künftig noch weiter ausbauen können und danken hieran beteiligten Behörden.

Unsere aktuellen Stellenausschreibungen stehen immer auf unserer Homepage. Bewerben oder weitersagen!

Fortschreitende Digitalisierung und Modernisierung

Mit dem Jahreswechsel waren auch wir verpflichtet, künftig nur noch auf elektronischem Weg mit den Einrichtungen der Justiz zu kommunizieren. Neu zu etablierende Prozesse haben den Blick weiter dafür geöffnet, mit welchen Mitteln und auf welchen digitalen Wegen die Dienststelle künftig arbeiten soll: Vom mobilen Arbeitsplatz aus kann fristwahrend ein Schriftsatz bei Gericht eingereicht werden. Eingehende Anrufe nimmt die Telefonzentrale im Homeoffice entgegen und verbindet zum mobilen Arbeitsplatz der Mitarbeitenden. Einsichtnahme in Akten wird ohne Papier und vollelektronisch vorgenommen. Diese Beispiele sind zwar noch Zukunftsmusik, aber die ersten Takte wurden im Jahr 2022 schon gespielt und ein schöner Rhythmus ist erkennbar.

Migration zur BITBW

Im Jahr 2021 bezog die Dienststelle des LfDI die neuen Räumlichkeiten in der Lautenschlagerstraße. Nach diesem räumlichen Umzug erfolgte im Jahr 2022 sozusagen ein „virtueller Umzug". Unsere Dienststelle schloss sich der einheitlichen System- und Benutzerverwaltung der Landesverwaltung durch die BITBW an. Die Arbeiten für die Migration vollzogen sich Zug um Zug und begannen zunächst im Hintergrund, weitgehend unsichtbar für die Mitarbeitenden in der Dienststelle. Erst der Austausch der Benutzer_innenhardware und die Einführung des sogenannten „Landesclients" machte die Migration dann tatsächlich für die Kolleg_innen sichtbar. Auch aufgrund eingespielter Routinen bei der BITBW und den beauftragten Dienstleistern konnten die Ausfallzeiten niedrig gehalten werden. In der darauffolgenden Zeit wurden sukzessive diverse Serveranwendungen migriert und auch organisatorische Änderungen vorgenommen. So bleiben die Kollegen der IuK als First Level Support weiterhin die ersten Ansprechpartner bei Fragen zur und Problemen mit der IT, alles jenseits der „Ersten Hilfe" deckt künftig die BITBW mit ihrem Leistungsportfolio ab. Zudem hat jeder Mitarbeitende mit der Migration die technische Ausstattung erhalten, die für das mobile Arbeiten in der digitalisierten Welt notwendig ist.

Einführung der landeseinheitlichen E-Akte

Die erfolgreiche Durchführung der Migration und Integration in die IT-Systemlandschaft der BITBW ebnete den Weg für die Einführung der E-Akte BW und damit für das nächste Großprojekt zur Digitalisierung unserer Verwaltungsarbeit. Die dienststelleninterne Projektstruktur setzt sich aus dem Steuerkreis, zu welchem die Dienststellenleitung, die Abteilungsleitungen, der Personalrat, die Beauftragte für Chancengleichheit und der behördliche Datenschutzbeauftragte gehören, und dem Projektteam mit Kolleg_innen der Abteilung 1, zusammen. Am 4. April erfolgte gemeinsam mit der Stabsstelle E-Akte der Projektstart, gefolgt von einer Systempräsentation für die Projektbeteiligten der Dienststelle. Die E-Akte BW vereint auf digitaler Ebene das Dokumentenmanagement, die Aktenführung und die Vorgangsbearbeitung, d.h. die Aufgabenerledigung mit Hilfe eines elektronischen Geschäftsgangs. Dieses für die Dienststelle tiefgreifende Veränderungsprojekt forderte das Projektteam in den zurückliegenden neun Monaten durch die intensive Analyse von Prozessen und der Erstellung von Konzepten, welche in regelmäßigen Besprechungsterminen mit der Zentralen Unterstützungsgruppe Rollout der BITBW und der Stabsstelle E-Akte besprochen und entwickelt worden sind. Die Phasen 1 und 2 des Gesamtprojekts konnten termingerecht abgeschlossen werden, so dass die weitere Projektarbeit, die sich vor allem auf das Aufsetzen des Produktivmandanten, die Datenmigration, die Schaffung von Schnittstellen und nicht zuletzt auf die Schulung der künftigen Anwendenden konzentriert, auf den Starttermin im Mai 2023 gerichtet bleibt (Zur E-Akte siehe auch Kapitel 1.3).

eRechnung und Umstellung auf neue SAP Version

Seit dem Jahreswechsel müssen Rechnungssteller ab einem Nettobetrag in Höhe von 1.000 Euro ihre Rechnungen digital als eRechnung stellen. Diese landesrechtliche Vorgabe wurde im Vorfeld der Einführung einer neuen SAP Version eingeführt, um künftig eine rein digitale Verarbeitung von Rechnungen zu ermöglichen. Bereits seit einigen Jahren laufen die Vorbereitungen und die Konfiguration des neuen SAP Systems, welches als Projekt unter dem Namen „Restrukturierungsprojekt Baden-Württemberg („RePro BW") bekannt ist. In diesem Jahr wurden die letzten Konfigurationen vorgenommen. Weiterhin konnte das System

und die entsprechenden WorkFlows getestet und die Anwendenden entsprechend geschult werden. Ab dem 01. Januar 2023 ist das neue System im Einsatz. Trotz der Schulungen und Tests ist davon auszugehen, dass weitere Anpassungen der WorkFlows im laufenden Betrieb notwendig sein werden, um eine reibungslose, automatisierte und vollständig digitale Rechnungsbearbeitung gewährleisten zu können.

Neuer Einzelplan im Staatshaushaltsplan

Seit dem 1. Januar 2022 sind die Einnahmen und Ausgaben der Dienststelle nicht länger im Einzelplan des Landtags abgebildet, sondern in einem eigenen Einzelplan mit der Nummer 17. Über einen eigenen Einzelplan verfügen des Weiteren der Landtag, die Ministerien, der Rechnungshof sowie der Verfassungsgerichtshof.

Die Trennung bildet hierbei die gesetzlich geforderte Unabhängigkeit des LfDI von anderen Ministerien und Behörden des Landes Baden-Württemberg nun auch haushaltsrechtlich ab. Die Bewirtschaftung des ersten eigenen Einzelplanes des LfDI verlief auch aufgrund der guten Zusammenarbeit mit dem Finanzministerium reibungslos. Für den Doppelhaushalt 2023/24 mussten zudem lediglich kleinere Anpassungen vorgenommen werden.

10.2 Digitale und direkte Kommunikation

Mastodon & PeerTube

Wir suchen das direkte Gespräch mit den Bürger_innen. Dafür nutzen wir auch die datenschutzfreundliche Twitter-Alternative Mastodon. Mittlerweile folgen uns über 6.000 Interessierte auf Mastodon. In nur wenigen Monaten hat sich die Zahl der Accounts, die uns folgen mehr als verdoppelt. Immer mehr Menschen sind neugierig auf alternative Kommunikationsformen und entdecken den nicht gewerblichen Micro-Blogging Dienst. Der neue Twitter-Eigentümer Elon Musk hat Twitter selbst problematisiert durch sein Handeln, dass viele Bürger_innen, insbesondere in Deutschland, darüber diskutieren, wie Kommunikation auf einer Plattform aussehen kann und soll, und ob Plattformen wie Mastodon nicht eine gute Alternative zu den Angeboten großer Tech-Konzernen sein können. Obwohl sich immer mehr Menschen einen Account einrichten, tummeln sich im Vergleich zu Twitter noch verhältnismäßig wenig Menschen dort. Dennoch ist erkennbar: Immer mehr öffentliche Stellen, Multiplikatoren und auch Journalist_innen sind auf Mastodon aktiv. Mastodon entwickelt sich weiter, und es wird sich künftig zeigen, wie sehr sich diese Plattform als Alternative durchsetzt.

Besonders erfreulich ist, dass zahlreiche öffentliche Stellen und solche mit Bezug zu öffentlichen Aufgaben auf unserem Server einen eigenen Account eingerichtet haben und jetzt datenschutzfreundlich kommunizieren. Wir sehen hier die öffentlichen Stellen weiterhin in der Pflicht: Sie sollten Bürger_innen das Angebot machen, frei zugänglich und ohne ökonomisch verwertet zu werden Informationen über Soziale Medien zu erhalten. Es ist möglich für Nutzende, ohne Anmeldung Informationen der öffentlichen Stellen einzusehen, sich zu informieren. Das Staatsministerium ist vorausgegangen und hatte sich bereits frühzeitig einen Mastodon-Account eingerichtet, ist dann auf unseren Server umgezogen. Zahlreiche weitere Ministerien sind ebenfalls hier, ebenso der Beauftragte der Landesregierung Baden-Württemberg gegen Antisemitismus, Dr. Michael Blume, zudem auch etwa das Regierungspräsidium Freiburg und das Patent- und Markenzentrum Baden-Württemberg. Auch machen sich immer mehr Städte und Gemeinden auf den Weg: Die Stadt Freiburg und auch etwa die Stadt Laupheim hatten sich einen Account bei uns eingerichtet, bereits kurz nachdem wir unseren Server geöffnet hatten. Anschließend dauerte es noch etwas, doch dann kamen sehr viele weitere Städte und Gemeinden, beispielsweise die Städte Ulm, Mannheim, Reutlingen und die Landeshauptstadt Stuttgart. Je mehr hier aktiv sind, desto mehr Diskussionen wird es auf Mastodon geben und damit die Attraktivität gesteigert, hierüber zu kommunizieren.

☛ Mehr Informationen:

Der LfDI auf Mastodon: bawü.social/@lfdi

Die PeerTube-Instanz des LfDI: tube.bawü.social

LfDI-Newsletter: www.baden-wuerttemberg.datenschutz.de/newsletter-anmeldung

LfDI-App:
www.baden-wuerttemberg.datenschutz.de/lfdi-app

Über 35 Hochschulaccounts sind inzwischen auf dem LfDI Server. Außerdem haben weitere Einrichtungen, wie die Verbraucherzentrale, das Medienzentrum Mittelbaden, der Katastrophenschutz des Landkreis Ludwigsburg, die Heidelberger Akademie der Wissenschaften, die Städtischen Museen Freiburg und das Badische Landesmuseum, die Uniklinik Heidelberg und das Popup Labor Baden-Württemberg sowie die Komm.One bei uns einen Account eingerichtet. Kurzum: Es wird immer vielfältiger auf Mastodon, damit wird Mastodon interessanter für alle Nutzenden.

Wir bauen unser Angebot aus. Wir wollen ergänzend zur Twitter-Alternative eine YouTube-Alternative anbieten. Das ist zum Beispiel mit PeerTube möglich. Auf einem eigenen Server (wie bei Mastodon) stellen bereits unsere Videos online zur Verfügung. Diese sind dann für Interessierte, die sich in Sozialen Netzwerken bewegen, sehr leicht zugänglich und gut teilbar. Und auch hier werden wir bald die Instanz öffnen, sodass etwa die Ministerien und Städte hier für ihre Inhalte einen Account einrichten können.

LfDI-App

Mit unserer LfDI-App haben wir die Erfahrung gemacht, dass es sehr gut funktioniert, datenschutzrechtliche Aspekte mit digitalen Tools zu verbinden. Es ist nicht zwingend, Apps so zu programmieren, dass möglichst viele personenbezogene Daten für anderen Zwecke des Anbieters abgegriffen werden. Digitale Angebote gerade der öffentlichen Stellen für Bürger_innen sollten ohne die Aufforderung auskommen, personenbezogene Daten zu sammeln.

Im September 2021 wurde die LfDI-App für iPhone veröffentlicht. Eine Veröffentlichung der Android-App folgte Anfang des Jahres 2022, anschließend folgte die F-Droid Version. Auch erhielten wir viel Zuspruch für die F-Droid Version der App. Bei der In-House Entwicklung der nativen App haben wir uns im Rahmen von „Datenschutz by design" darüber bedacht, welche Risiken für betroffene Personen bei der Nutzung durch die App entstehen können. Die Verbindungen der App haben wir über unseren App-Test-Parcours überprüft und ein Code-Review durchgeführt. Daneben waren auch Aspekte aus anderen Rechtsgebieten zu beachten, wie etwa aus dem Urheberrecht. Die Android- und F-Droid App haben wir extern produzieren lassen, das Projekt SECUSO am Karlsruher Institut für Technologie (KIT) hat uns hier geholfen.

Es geht also, und wenn wir eine nachhaltige Digitalisierung fördern wollen, dann müssen die Bürger_innen darauf vertrauen können, dass ihre Bürgerrechte auch in der digitalen Welt gelten. Staatliche Stellen können hier vorausgehen und das Vertrauen ins Internet stärken.

10.3 Dienst für die Bürgerschaft

Als unabhängige Aufsichtsbehörde gehört es zu unserer Kernaufgabe, uns in öffentliche Debatten um die Freiheit einzubringen, wie es die DS-GVO vorsieht. Wir leisten hier unseren Beitrag. Was die Beschwerden angeht, nehmen wir wahr, dass ihre Zahl in diesem Jahr rückläufig war und sich in etwa der Beschwerden auf den vor-Corona-Zustand zu konsolidieren scheint. Dass hängt sicher damit zusammen, dass die zur Bewältigung der Pandemie vorgenommenen Grundrechtseingriffe weitgehend zurückgegangen ist, weil sie zum Schutz der Gesundheit der Menschen nicht mehr notwendig sind. Wir gehen aber davon aus, dass eine Ursache für den Rückgang an Beschwerden auch unsere erfolgreiche Arbeit in der Beratung, der Aufklärung und im Bereich der Fortbildungen zum Datenschutz zu suchen ist. Mit unseren Handreichungen, unserem Tool „DS-GVO. clever" für Vereine und kleinere Unternehmen, mit denen einfach und schnell Datenschutzhinweise erstellt werden können, sowie unseren FAQ und Handreichungen bieten wir zusätzliche Unterstützung für Bürger_innen und verantwortliche Stellen. Die DS-GVO gilt inzwischen seit fast fünf Jahren, ihre Akzeptanz ist gestiegen und Auslegungsunsicherheiten sind durch Rechtsprechung der Gerichte sowie Leitlinien und Handreichungen des EDSA und der Aufsichtsbehörden verringert worden.

Bei der Zahl der uns gemeldeten Datenpannen erreichten wir im Jahr 2021 auch wegen der Microsoft-Exchange- und der log4j-Lücke einen Höchstwert. Im Jahr 2022 lag die Zahl der Datenpannenmeldungen wieder unter 3.000. Ransomware-Angriffe etwa auf Kommunen bleiben aber weiter bedrohlich, hier gilt für Verantwortliche auch für 2023 angemessene technisch-organisatorische Maßnahmen zu treffen, um solche Angriffe möglich unwahrscheinlich oder zumindest nicht so gravierend ausfallend zu machen.

Im Jahr 2021 hatten wir zudem beobachten können, dass die Zahl der schriftlichen Beratungsanfragen in

etwa in dem Maße sank wie die Zahl der Teilnehmenden an Beratungs-und Schulungsangeboten in unserem Bildungs- und Beratungszentrum BIDIB stieg.

Im Jahr 2022 entkoppelte sich dies: Die Zahl der Beratungsanfragen sank etwas im Vergleich zum Vorjahr, doch die Zahl der Teilnehmenden an BIDIB-Veranstaltungen stieg enorm. Das liegt auch daran, dass wir mit unserem speziellen Fortbildungsangebot „Schule digital" ein sehr nachgefragtes Angebot vorgehalten haben. Wir sehen insgesamt, dass unser Bildungs- und Beratungszentrum mit seinem Programm aktuelle Themen aufgreift und Interessen der Nutzenden entgegenkommt. Regelmäßig fragen wir auch – etwa über unseren Newsletter, der mittlerweile rund 5.500 Abonnenten hat, und auf Mastodon, welche Themen die Bürger_innen, Behörden und Unternehmen interessieren, um unser Programm entsprechend auszurichten – ganz offensichtlich erfolgreich.

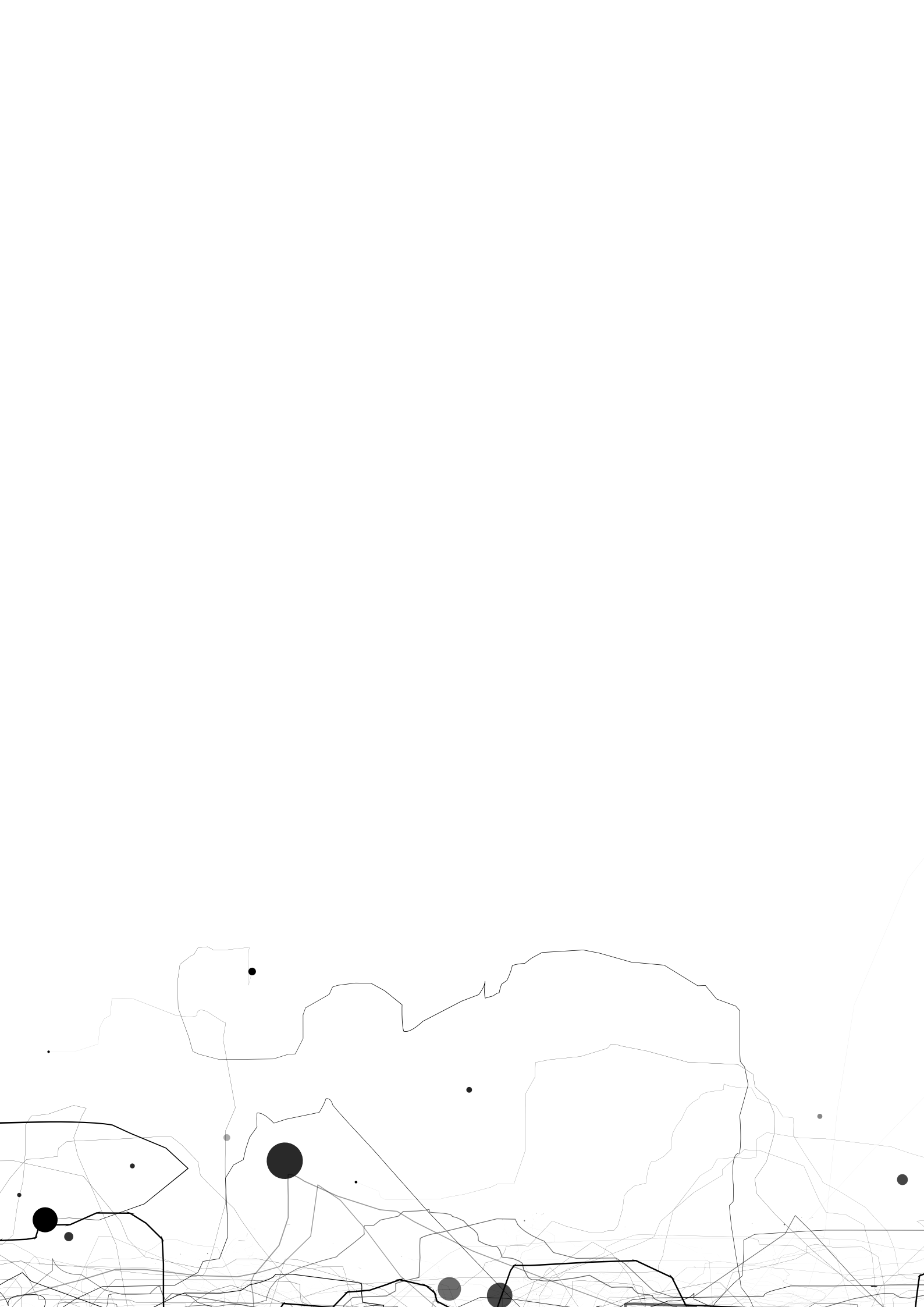
Unsere Bußgeldstelle hat in diesem Jahr wieder verstärkt Prüfungen vorgenommen. Insgesamt waren 213 neue Verfahren anhängig. Die Zahl der Neueingänge lag damit deutlich über dem der letzten beiden Jahre und erreichte das Vor-Corona-Niveau. Im Berichtszeitraum hat die Bußgeldstelle 19 Bußgeldbescheide erlassen, von denen 18 rechtskräftig wurden und die sich sowohl gegen Unternehmen als auch nicht-unternehmerisch tätige richteten.

Uns wird auch im kommenden Jahr die Arbeit nicht ausgehen: Die neuen Technologien, mit denen wir uns schon in diesem Jahr u. a. in der diesjährigen KI-Woche intensiv beschäftigt haben, werden weiterhin viele neuartige Fragen aufwerfen. Die zunehmende Digitalisierung in Wirtschaft und Verwaltung wird einen zunehmenden Beratungsbedarf mit sich bringen. Neue und grundlegende Gesetzesvorhaben – namentlich auch die europäischen Verordnungen zur Entwicklung von Datenräumen – werden kommen und umzusetzen sein. Bei all diesen Entwicklungen werden wir weiter dafür einstehen, dass das Grundrecht auf Datenschutz als wesentlicher Teil unserer freiheitlichen Gesellschaftsordnung gewahrt ist. Denn in ihr gehören Digitalisierung und Datenschutz zusammen.

Statistische Übersicht – Zeitraum jeweils vom 01.01. – 31.12.

	2016	2017	2018	2019	2020	2021	2022
Beschwerden	2048	3058	3902	3757	4782	4708	3796
Kontrollen	16	55	13	111	31	10	33
Beratungen[1]	1515	1786	4440	3842	3285	2206	1935
Anmeldungen Bildungs und Beratungszentrum BIDIB					785	2016	3255
Datenpannen	68	121	900	2030	2321	3136	2747
Bußgeldverfahren (eingeleitet)			138[2]	233	174	136	213

1 ohne telefonische Beratung
2 Mai – Dez



Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Hintergrungrafik: xenia_design-stock.adobe.com