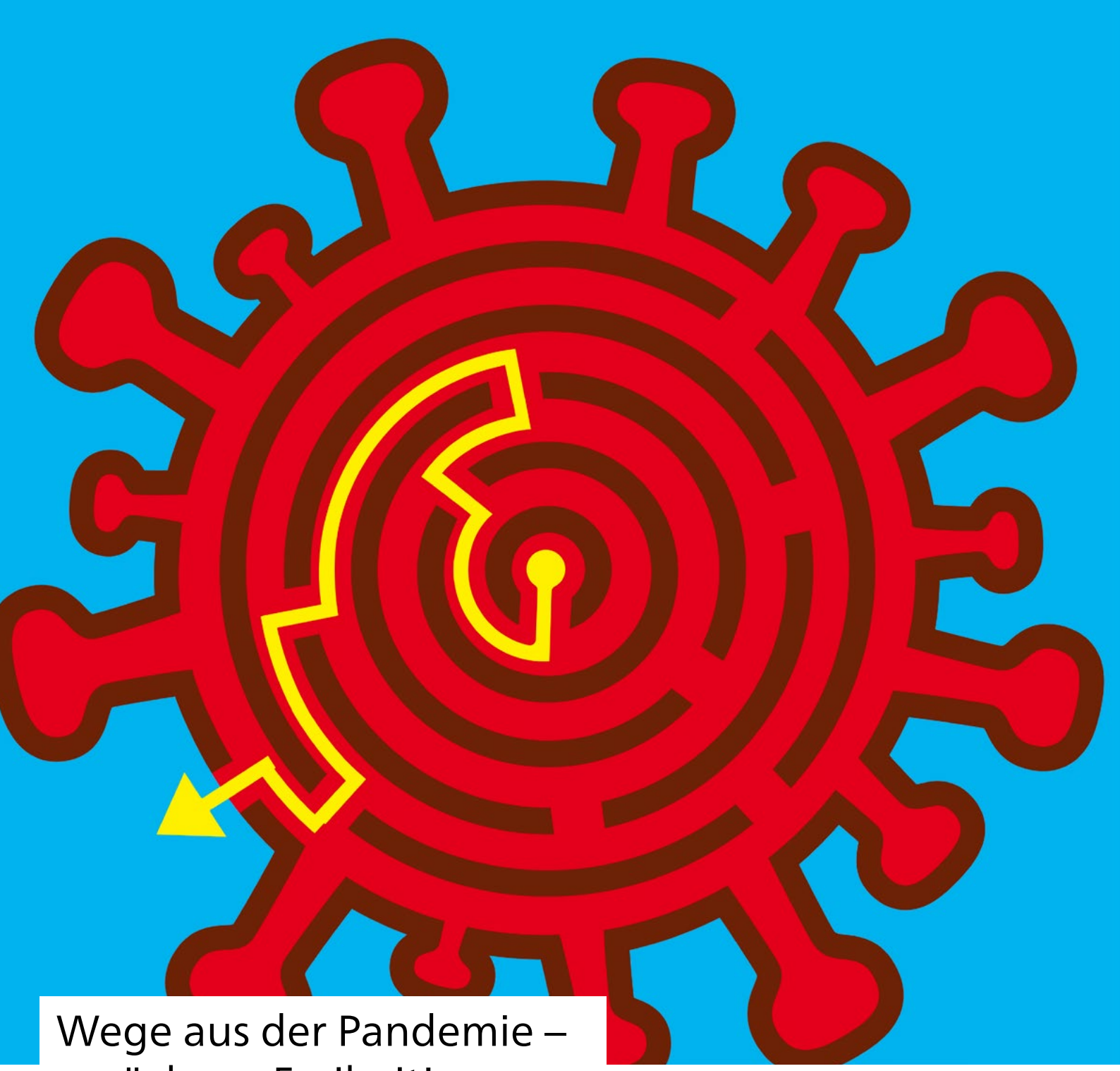


Wege aus der Pandemie – zurück zur Freiheit!

Unsere Freiheiten:
Daten nützen – Daten schützen

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Tätigkeitsbericht
Datenschutz 2021

Herausgegeben vom
Landesbeauftragten für den Datenschutz und die Informationsfreiheit
Dr. Stefan Brink
Lautenschlagerstraße 20, 70173 Stuttgart
Telefon: 0711/615541-0
Telefax: 0711/615541-15
https://www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de
Mastodon: https://bawü.social/@lfdi
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Gestaltung, Redaktion: Cagdas Karakurt, Koordinierungs- und Pressestelle, LfDI

Dezember 2021
Veröffentlicht als Landtags-Drucksache 17/1600

37. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2021

Inhalt

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Vorwort

© Kristina Schäfer

Dr. Stefan Brink

Noch immer steht der Datenschutz unter dem maßgebenden Einfluss der SARS-CoV-2-Pandemie. Noch immer steht der notwendige Schutz der Gesundheit im Vorder- und die persönlichen Freiheiten der Bürger_innen stehen allzu häufig im Hintergrund. Auch gerechtfertigte Eingriffe in Grundrechte sind Eingriffe, sie verkürzen etwa unsere Berufsfreiheit, unsere Reisefreiheit, unsere Versammlungsfreiheit, und eben auch unser Grundrecht auf informationelle Selbstbestimmung, den Datenschutz.

Wir Datenschützer sind dabei auf die Rolle beschränkt, jede unverhältnismäßige Verkürzung der Freiheit zu erkennen und zu kritisieren. Demgemäß haben wir auch 2021 interveniert und beraten, geholfen und diskutiert, aufgeklärt und mitgestaltet – und dort, wo der Eingriff absolut inakzeptabel erschien, ihn auch effektiv unterbunden.

Mit fortschreitender Dauer der Pandemie wurden die Eingriffe in das informationelle Selbstbestimmungsrecht fast durchweg gravierender. Was – etwa an den Schulen – als Testangebot für Schüler_innen begann, wurde im Laufe des Jahres zur Obliegenheit heraufgestuft und ist mittlerweile zum Teil der Schulpflicht geworden. Damit ist die Notwendigkeit und Richtigkeit dieser Maßnahmen nicht in Zweifel gezogen – aber eben auch die wiederholt geäußerte Auffassung widerlegt, das Recht auf informationelle Selbstbestimmung sei durch die Pandemie als einziges Grundrecht „uneingeschränkt davongekommen". Das schmerzt.

2021 sind Tabus gebrochen worden, für den Datenschutz hilfreiche Tabus. Etwa die in Jahrzehnten im Arbeitsrecht entwickelte und von den Gerichten hoch gehaltene Überzeugung, dass den Arbeitgeber Informationen zu Krankheiten der Beschäftigten nichts angehen. Natürlich muss er wissen, ob ein Beschäftigter arbeitsunfähig erkrankt ist oder dass er bestimmte Belastungen nur in medizinisch geklärten Grenzen aushält – aber die ärztliche Diagnose blieb ihm aus guten Gründen vorenthalten. Er sollte damit weder Einstellungspolitik noch Personalplanung oder Kündigungsauswahl betreiben dürfen. Genau dies ist 2021 zu Fall gekommen – mit noch unabsehbaren Folgen. Der „Kampf" um die Offenlegung des Impfstatus des einzelnen Beschäftigten ging, Kraft Beschluss des Bundesgesetzgebers im Infektionsschutz-Gesetz, zu Lasten der Wahrung dieses sensiblen Gesundheitsdatums aus. Nicht grundlos, aber mit gravierenden Folgen, die wir für die Zukunft nach Möglichkeit begrenzen sollten.

Der Datenschutz selbst entfaltet weiter seine Wirksamkeit. Ungebrochen ist etwa die Bedeutung der europäischen Rechtsprechung zum Transfer personenbezogener Daten in die USA. Wer in Europa Geschäfte machen möchte, der muss europäische Standards wie die Datenschutz-Grundverordnung (DS-GVO) erfüllen. Die DS-GVO ist ohne Zweifel ein Standortfaktor geworden und kein „nice to have", auch kein Papiertiger. Die DS-GVO wirkt – und die europäischen Aufsichtsbehörden müssen weiter hart daran arbeiten, diese hervorragende Rechtsgrundlage nachvollziehbar, einheitlich und effektiv zu vollziehen.

Wir nehmen in Baden-Württemberg den Datenschutz ernst. Nicht nur mit unserem Motto „Wenn es nicht vernünftig ist, dann ist es kein Datenschutz!", nicht nur als bundesweit erste Landesbehörde, die ein eigenes Bildungszentrum für Datenschutz und Informationsfreiheit (BIDIB) betreibt und damit große Resonanz erzielt. Sondern gerade auch deswegen, weil unser Weg eines offenen, digitalisierungsfreundlichen und mitgestaltenden Datenschutzes so außergewöhnlich intensiv von der Unterstützung des gesamten Parlaments getragen wird.

Auf dieser Grundlage konnten wir Mitte 2021 eine gut ausgestattete Dienststelle beziehen, die uns alle Möglichkeiten einer modernen Aufsichtsbe-

hörde bietet – und sogar zum Gestaltungsraum von Künstler_innen wird, die wie wir Datenschutz als Kulturaufgabe verstehen. Insbesondere das Bildungszentrum ist jetzt technisch so ausgestattet, dass Fortbildungen, Schulungen, Vorträge, Diskussionen und Fachgespräche analog und digital qualitativ gut möglich sind. Wir nehmen seitdem auch Wünsche von Vereinen, Unternehmen, Verbänden, Schulen und Schulklassen sowie Behörden auf und setzen Fortbildungen und Schulungen an, wenn wir merken, dass die jeweiligen Themen viele Menschen betreffen und interessieren. Das Bildungszentrum wird so immer mehr der Ort für die Beratung, Vermittlung, Schulung und Qualifizierung.

Gleichzeitig konnten wir als Behörde unsere Kommunikationswege ausbauen: Nicht nur das BIDIB ist online, mit Mastodon aus dem freien Fediverse stehen wir in Kontakt zu den am Datenschutz und seiner Fortentwicklung Interessierten, wir führen vor Ort und online Quartalsgespräche mit Großunternehmen, Treffen uns regelmäßig mit behördlichen Datenschutzbeauftragten der Ministerien und der Kommunen ebenso wie mit betrieblichen DSB und ihren Organisationen, der Gesellschaft für Datenschutz und Datensicherheit GDD und dem Berufsverband der Datenschutzbeauftragten BvD. Denn nur ein kommunikativer Datenschutz kann in der digitalen Gesellschaft erfolgreich mitgestalten.

Wir sehen den Datenschutz als Freiheitsschutz. Bürger_innen können mit ihren Daten so umgehen, wie sie es möchten. Alle, die auf diese Daten zugreifen und sie verarbeiten wollen, müssen sich dabei an bestimmte Regel halten, welche die DS-GVO vorgibt. So arbeiten wir dafür, dass Bürger_innen auch in der digitalen Welt die Möglichkeit haben, ihre bürgerlichen Rechte wahrzunehmen und sich nach ihren eigenen Vorstellungen selbstbestimmt zu entfalten. Wir achten darauf, dass Bürger_innen frei und informiert ihre Entscheidungen im Netz treffen können und stellen uns an ihre Seite.

Ökonomisch funktioniert das Netz bereits sehr gut. Doch wie ist unsere kulturelle Praxis ausgeprägt? Wie gehen wir miteinander im Netz um und wie binden wir es in unseren Alltag ein? Diese kulturelle Praxis ist noch nicht gänzlich eingeübt und braucht einen Erfahrungsraum, welcher nicht durchökonomisiert sein sollte. Wie ist es mit Fehlern, die ein Mensch im Netz begeht, sollen die tatsächlich auf ewig im Netz bleiben? Was ist etwa mit einem Kind, dass etwas postet und diesen Post später als Erwachsene nicht mehr richtig findet? Wie gehen wir damit um? Muss ein Fehler immer ironisch mit viel Witz und supportet durch viele Likes korrigiert werden? Müssen gravierende Fehler durch neue harte Vergebungsrituale – wer bestimmt über diese? – ausgemerzt werden? Muss man im Netz immer die Person sein, als die man sich vor vielen Jahren einmal gezeigt hat? Gibt es die Möglichkeit, sich als Persönlichkeit immer wieder einmal neu zu erfinden?

Die DS-GVO schützt Kinder besonders, und sie gibt Bürger_innen das Recht auf Vergessenwerden. Daten können gelöscht werden, aber sind sie einmal im Umlauf, dann wird es sehr schwer, diese wieder einzufangen. Wir arbeiten dafür, dass Bürger_innen selbstbestimmt im Netz unterwegs sein können. Und darin zeigt sich der Freiheitssinn des Datenschutzes. Informationelle Selbstbestimmung eben.

Dennoch verschließen wir nicht die Augen davor, dass Datenschutz in der öffentlichen Wahrnehmung auch als Last, ja geradezu als Freiheitseinschränkung aufgefasst wird. Auch diesen kritischen Stimmen stellen wir uns – und sind zugleich froh, dass mit der neuen Regierungskoalition auf Bundesebene die schädlichen Pläne einer Zentralisierung der Datenschutzaufsicht in Deutschland ad acta gelegt wurden.

Mein Dank gilt auch in diesem Jahr allen meinen Mitarbeitenden für ihre äußerst kreative, engagierte und beherzte Arbeit als „Überzeugungstäter der Freiheit“.

Danken möchte ich auch den Abgeordneten des Landtags, die unsere Tätigkeit aufmerksam und kritisch mitverfolgen und damit maßgeblich gestalten und fördern. Ich danke auch der Landesregierung, der gesamten Landesverwaltung und den Kommunen für die konstruktive, faire und meist einvernehmliche Zusammenarbeit.

Ihr Landesbeauftragter

Dr. Stefan Brink

>> Bleiben Sie informiert –
folgen Sie uns auf Mastodon
https://bawü.social/@lfdi <<

#Corona-Verordnung

#Corona-Verordnung Auftragsverarbeitung

#Corona-Verordnung Schule

#Corona-Verordnung Kita

#Corona-Pandemie-Prüfungs-verordnung 2021/2022

#Corona-Verordnung Musik-, Kunst- und Jugendkunstschulen

#Corona-Verordnung Studienbetrieb

#Corona-Verordnung Bäder und Saunen

#Corona-Verordnung Sport

#Corona-Verordnung Einreise-Quarantäne

#Corona-Verordnung Datenverarbeitung

#Corona-Verordnung Kranken-häuser und Pflegeeinrichtungen

#Corona-Verordnung Familien-bildung und Frühe Hilfen

#Corona-Verordnung Angebote Kinder- und Jugendarbeit sowie Jugendsozialarbeit

#Verordnung über Zuständigkeiten nach dem Infektionsschutzgesetz

#Corona-Erstaufnahme-Schutz-Verordnung

#Corona-Verordnung Werkstätten für behinderte Menschen

#Corona-Stabilisierungshilfe-HOGA- Zuständigkeitsverordnung

#Corona-Verordnung Absonderung

Wenn Corona-Verordnungen und die jeweiligen Änderungsverordnungen die Verarbeitung von personenbezogenen Daten betreffen, ist der Landesbeauftragte zu beteiligen. Leider ist dies immer wieder nicht geschehen.

1. Beteiligung bei den Corona-Verordnungen der Landesregierung

Nach dem Jahr 2020 stand auch das Berichtsjahr 2021 ganz unter dem Einfluss der Corona-Krise. Dabei haben wir uns insbesondere mit vielfältigen datenschutzrechtlichen Fragestellungen beschäftigt, die mit den infektionsschutzrechtlichen Maßnahmen zur Bewältigung der Corona-Krise einhergingen. Im Mittelpunkt standen dabei die verschiedenen „Corona-Verordnungen" der Landesregierung und die kraft Subdelegation hierzu erlassenen Verordnungen der Ministerien. Diese Verordnungen unterlagen auch in diesem Jahr wieder ständiger Veränderung. Ein wesentlicher Teil unserer Tätigkeit entfiel dabei auf die Mitwirkung an dem Erlass dieser Verordnungen, soweit sie die Verarbeitung personenbezogener Daten betrafen. Die Ministerien sahen sich hierbei teilweise unter höchstem Zeitdruck. Infolgedessen ist unsere Beteiligung leider nicht immer regelkonform erfolgt – denn auch in Krisenzeiten erfolgt die Beteiligung des LfDI an der Regelsetzung der Landesregierung nicht „gelegentlich", sondern nach klaren Rechtsvorgaben. Wo das nicht gelang, geriet dies aus unserer Sicht zum Nachteil der Qualität so mancher Regelung.

Wie bereits in unserem Tätigkeitbericht für 2020 (S. 9 f.) dargestellt, sind die Landesregierung und die Ministerien nicht nur kraft der Verwaltungsvorschrift der Landesregierung und der Ministerien zur Erarbeitung von Regelungen vom 27. Juli 2010 – Az.: 5-05/22 – (GABl. 2010, S. 277, zuletzt geändert durch Verwaltungsvorschrift vom 9. März 2021, GABl. 2021, S. 186), sondern auch gemäß § 26 Absatz 2 LDSG und Artikel 36 Absatz 4 DS-GVO verpflichtet, uns an der Erarbeitung von Rechts- und Verwaltungsvorschriften, welche die Verarbeitung personenbezogener Daten betreffen, rechtzeitig zu beteiligen. Die Verarbeitung personenbezogener Daten ist dabei durch die Corona-Regelungen in vielfältiger Weise betroffen. Dies beschränkt sich nicht nur auf die Erhebung und Speicherung von Anwesenheits- und Kontaktdaten durch diverse Anbieter, Veranstalter und Einrichtungen (siehe dazu unten den Beitrag: „Die Verpflichtung zur Kontaktdatenverarbeitung, Luca App und Corona-Warn-App").

Auch bei jeder Einlasskontrolle, bei der Nachweise über den Immunisierungsstand oder über aktuelle Tests vorzulegen sind, oder dann, wenn zur Geltendmachung von bestimmten Ausnahmen (z. B. der Befreiung von der Pflicht, eine [medizinische] Maske zu tragen, der Befreiung von der Pflicht zur Teilnahme am Präsenzunterricht in der Schule etc.) Belege vorzuweisen sind, ist der Datenschutz und damit unsere Zuständigkeit berührt. Da können und wollen wir unseren Beitrag leisten – jedenfalls soweit eine automatisierte Verarbeitung oder eine Verarbeitung zwecks Speicherung in einem Dateisystem erfolgt (Artikel 2 Absatz 1 DS-GVO), aber z. B. bei öffentlichen Stellen oder im Rahmen von Beschäftigtenverhältnissen auch ohne diese zusätzlichen Voraussetzungen (vgl. insbesondere § 2 Absatz 4 LDSG und § 26 Absatz 7 BDSG; zum Beschäftigtendatenschutz in der Corona-Krise s. auch noch unseren Beitrag „Corona im Betrieb").

Auch im Berichtsjahr 2021 ist die Landesregierung mit dieser Verpflichtung, uns beim Erlass von Corona-Verordnungen rechtzeitig zu beteiligen, wenig einheitlich umgegangen. Teilweise wurden wir von den Ministerien gar nicht angehört. Teilweise wurden wir erst einbezogen, wenn – so erschien es uns – der Text der Verordnung schon feststand oder es zumindest vor dem geplanten Verkündungstermin kaum noch Gelegenheit zu (substantiellen) Änderungen gab. Außerdem waren wiederholt die Fristsetzungen derart kurz, dass sie uns kaum die Möglichkeit eröffneten, die Entwürfe hinreichend zu prüfen. Wir haben gleichwohl jeweils im Rahmen des Möglichen versucht, erforderlichenfalls kritische, aber konstruktive Hinweise zu geben.

Auch der Umgang mit unseren Hinweisen gestaltete sich sehr unterschiedlich. Zuweilen wurden unsere Vorschläge durch Änderungen in den Regelungsentwürfen selbst noch rechtzeitig umgesetzt. Vielfach sah sich die Landesregierung hierzu aber aus Zeitgründen nicht mehr in der Lage. Dann wurden sie zuweilen immerhin bei einer späteren Änderung der jeweiligen Verordnung noch berücksichtigt.

Das ist aus unserer Sicht zwar besser, als wenn sie gar nicht berücksichtigt worden wären, zu bedenken ist aber, dass zunächst ggf. eine unvollkommene Regelung in Kraft war und durch wiederholte Änderungen das Vertrauen der Rechtsunterworfenen (Bürger_innen, Gastro-Betriebe, Vereine etc.) und ihre Bereitschaft, die aktuelle Rechtslage zur Kenntnis zu nehmen und zu befolgen, gemindert

werden können. Insoweit gilt es abzuwägen, ob der schnelle Erlass einer unvollkommenen Regelung, die später wieder geändert werden muss, tatsächlich im Interesse des Infektionsschutzes besser ist als der Erlass sorgfältiger ausgearbeiteter Regelungen.

Zum Teil führten unsere Hinweise dazu, dass ergänzende Erläuterungen in die nach § 28 Absatz 5 IfSG erforderliche (und zu veröffentlichende) Begründung der Rechtsverordnung aufgenommen wurden. Auch dies kann aus unserer Sicht – sofern eine explizite Regelung in der Verordnung selbst nicht geboten ist – eine sinnvolle Lösung sein. Auch soweit unsere Hinweise – idealerweise in Abstimmung mit uns – zur Erstellung und Veröffentlichung ergänzender Handreichungen oder FAQ auf Internetseiten der Landesregierung geführt haben, kann dies eine wertvolle Hilfestellung für die Bürgerinnen und Bürger sein.

Leider erhielten wir vielfach auch gar keine Rückäußerung von den Ministerien, inwieweit sie unseren Anregungen und Hinweisen Folge leisten würden; vielmehr mussten wir uns ggf. die Ergebnisse der Beratung selbst aus den erfolgten Veröffentlichungen herauslesen. Das ist mit Blick auf den Zeitdruck und die hohe Arbeitslast, unter denen die Ministerien mit Blick auf die Pandemie standen, zwar verständlich, es hemmt aber eine fachliche, die Qualität der Rechtssetzung im Interesse der Rechtsunterworfenen fördernde Diskussion. Vielmehr mussten wir so unsere unberücksichtigten Hinweise vielfach wiederholen, was letztlich den Arbeitsaufwand für beide Seiten erhöhte – und am Ende alle Beteiligten enervierte. Es wäre begrüßenswert, wenn sich trotz des hohen Zeitdrucks in den Ministerien die Verfahrensabläufe besser und effektiver standardisieren und „leben“ ließen.

Es gab aber auch durchaus positive Beispiele der Zusammenarbeit mit den Ministerien. So kam beispielsweise das Ministerium für Wissenschaft, Forschung und Kunst (MWK) im Sommer 2021 frühzeitig mit einer Problemanzeige auf uns zu: Für das Wintersemester sei ein Präsenzbetrieb an den Hochschulen angestrebt. Hierfür werde im Interesse des Infektionsschutzes sicherzustellen sein, dass die am Präsenzbetrieb teilnehmenden Personen gegen SARS-Cov-2 geimpft, von einer entsprechenden Infektion genesen oder auf eine Infektion mit dem Virus negativ getestet seien, bei ihnen also ein sogenannter 3G-Status (geimpft, genesen oder getestet) vorliege. Aus praktischen Gründen sei es aber an den Hochschulen kaum durchführbar, zu Beginn jeder Veranstaltung bei sämtlichen Teilnehmenden die zum Beleg eines 3G-Status erforderlichen Papiere zu kontrollieren.

Deswegen werde vielfach von den Hochschulen die Forderung erhoben, den Impf- und Genesenenstatus der Studierenden und Lehrenden speichern zu dürfen. Wir entwickelten demgegenüber gemeinsam mit dem MWK datensparsame Lösungsmöglichkeiten, die in der CoronaVO Studienbetrieb vom 23. August 2021 (gültig ab dem 14. September 2021) Eingang fanden: Zum einen wurde den zur Überprüfung der 3G-Nachweise verpflichteten

3G – geimpft, genesen, getestet. Zum Schutz der Gesundheit der Bürger_innen wurden zahlreiche Einschränkungen beschlossen.

Hochschulen gestattet, den jeweiligen Test-, Impf- oder Genesenen-Nachweis nur einmal zu prüfen und sodann einen (fälschungssicheren) eigenen *„Hochschulnachweis über einen vorhandenen Impf-, Genesenen- oder Teststatus"* auszustellen, ohne dass hierzu etwas gespeichert werden durfte.

Die Hochschule konnten dann festlegen, dass das Vorzeigen dieses hochschuleigenen Nachweises Voraussetzung für die Teilnahme an einer Präsenzveranstaltung oder zur Betretung von Hochschulgebäuden erforderlich sein soll (und andere, aufwändiger zu kontrollierende Nachweise ausgeschlossen werden). Auf diese Weise konnte die zeitaufwändige Prüfung verschiedener unterschiedlicher Papiernachweise am Hörsaaleingang vermieden werden, ohne dass die Hochschulen hierzu den Immunisierungsstatus aller teilnehmenden Studierenden speichern mussten. Die Regelung in § 5 Absatz 2 Satz 2-5 CoronaVO Studienbetrieb bestimmte dafür genau, welche personenbezogenen Daten im Einzelnen der Hochschulnachweis über einen vorhandenen Impf-, Genesenen- oder Teststatus enthalten durfte, und sah darüber hinaus auch eine gewisse Missbrauchskontrolle zum Schutz vor Mehrfachverwendung desselben Nachweises vor. Weitere datenschutzrechtlich hilfreiche Ausführungen und Erläuterungen hierzu wurden in die Begründung der Verordnung aufgenommen, z. B. auch der Hinweis, dass zur Überprüfung der Echtheit eines digitalen Impfzertifikats auch die datensparsame CovPassCheck-App des Robert-Koch-Instituts verwendet werden könne (siehe auch Infokasten Seite 11).

>> Mehr Infos:

Presseerklärung des MWK vom 24. August 2021: https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/land-schafft-verlaesslichen-rahmen-fuer-praesenzbetrieb-im-wintersemester/ <<

Als weitere Alternativlösung regten wir eine Regelung an, nach der die Hochschulen das Vorliegen des 3G-Satus nur stichprobenartig prüfen. Angesichts dessen, dass Studierenden, die ohne 3G-Nachweis an einer Präsenzveranstaltung teilnehmen, gravierende Folgen (wie ein Bußgeldverfahren nach § 11 Nummer 2-5 CoronaVO Studienbetrieb und

INFOKASTEN

Die Regelung in § 5 Absatz 2 Satz 2 bis 5 CoronaVO Studienbetrieb in der ab dem 14. September 2021 geltenden Fassung lautete:

Die Hochschule kann [Anm. LfDI: zwecks Überprüfung des G-Status von Präsenzteilnehmenden] unentgeltlich einen Hochschulnachweis über einen vorhandenen Impf-, Genesenen- oder Teststatus ausstellen; in diesem Fall kann sie für die weitere Überprüfung nach Satz 1 Nachweise im Sinne des § 4 und § 5 CoronaVO ausschließen. Der Hochschulnachweis über einen vorhandenen Impf-, Genesenen- oder Teststatus enthält die Angabe, dass ein Impf-, Genesenen- oder Teststatus nach § 4 oder § 5 CoronaVO bis zu einem bestimmten Zeitpunkt vorliegt, den Namen sowie die Matrikelnummer oder das Geburtsdatum. Die Hochschule darf einen Nachweis außer, in den Fällen des Satzes 5 Nummer 1, nicht speichern.

Die Hochschule kann

1. Nachweise mittels Pseudonymen im Sinne von Artikel 4 Nummer 5 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (DS-GVO) (ABl. L 119 vom 4.5.2016, S. 1, zuletzt ber. ABl. L 74 vom 4.3.2021, S. 35) abgleichen, um Mehrfachverwendungen desselben Nachweises in derselben Veranstaltung zu verhindern;

2. in einer Veranstaltung die Anzahl der geprüften Nachweise mit der Anzahl der anwesenden Teilnehmenden abgleichen;

3. festlegen, dass der Nachweis nach Satz 1 bereits beim Zugang zum Hochschulgelände oder zu einem bestimmten Hochschulgebäude zu erbringen ist.

andere, hochschulrechtliche Sanktionen) drohten, sei zu prüfen, ob nicht Stichprobenkontrollen in Verbindung mit diesen Sanktionen die Einhaltung der Vorschriften ausreichend sicherstellten. Dieser Gedanke fand – wenngleich mit gewissen Einschränkungen und Bedingungen (wie einer Anzeigepflicht gegenüber dem MWK und die Pflicht zur wissenschaftlichen Begleitung des Stichprobenmodells) – Eingang in § 6 Absatz 3 CoronaVO Studienbetrieb.

Weitere Positivbeispiele lassen sich hier anführen, insbesondere die Beratungen mit dem Sozialministerium zur Überarbeitung der Vorschriften zur Verwendung der Luca-App und der Corona-Warn-App im Rahmen der Anordnung einer Pflicht zur Verarbeitung von Anwesenheits- und Kontaktdaten in § 8 CoronaVO (siehe dazu noch den Beitrag: Kontaktnachverfolgung, Luca-App und Corona-Warn-App) und zur Verwendung von digitalen Anwendungen zur Überprüfung der Echtheit von digitalen Impfzertifikaten in § 6a Absatz 3 CoronaVO im Rahmen der Änderungsverordnung vom 17. Dezember 2021.

Die Erwägungen, die wir bei der Prüfung von Regelungsentwürfen (hier: zur Bekämpfung der Corona-Pandemie) im Rahmen des Beteiligungsverfahrens zugrunde legen, resultieren naturgemäß in erster Linie aus der DS-GVO. Dabei ist zunächst zu prüfen, ob die beabsichtigte Materie durch das vorrangige europäische Recht abschließend geregelt ist oder ob dieses eine sogenannte Öffnungsklausel enthält, die den Mitgliedsstaaten der Europäischen Union eine Regelungskompetenz belässt. Die DS-GVO enthält insoweit zahlreiche Öffnungsklauseln, die für die Corona-Verordnungen relevant sind.

Beispielsweise gilt nach Artikel 6 Absatz 1 Satz 1 der DS-GVO, dass für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten bestimmte Mindestbedingungen (auch „Rechtsgründe“ genannt) vorliegen müssen. Für die Regelung in den Corona-Verordnungen enthalten insoweit insbesondere Artikel 6 Absatz 2 und 3 DS-GVO maßgebliche Öffnungsklauseln. Danach können die Mitgliedsstaaten Regelungen zur Datenverarbeitung treffen, in denen rechtliche Verpflichtungen zur Verarbeitungen personenbezogener Daten statuiert werden. Eine solche Verpflichtung stellt dann nach Artikel 6 Absatz 1 Buchstabe c DS-GVO einen Rechtsgrund zur Datenverarbeitung für den Verpflichteten dar. Wenn also etwa das Infektionsschutzrecht eine Erhebung und Speicherung von Anwesenheits- und Kontaktdaten von bestimmten Verpflichteten verlangt, stellt dies für die Verpflichteten grundsätzlich einen Rechtsgrund zur Datenverarbeitung dar. Auch können die Mitgliedsstaaten öffentlichen Stellen hoheitliche Aufgaben zuweisen mit der Folge, dass die zur Aufgabenerfüllung erforderlichen Datenverarbeitungen gemäß Artikel 6 Absatz 1 Buchstabe e DS-GVO als gerechtfertigt gelten.

Freilich müssen diese Regelungen der Mitgliedsstaaten einem legitimen Zweck dienen (Artikel 5 Absatz 1 Buchstabe b DS-GVO). Dieser muss – und das wird zuweilen übersehen – in der Regel in der rechtlichen Regelung des Mitgliedsstaates festge-

Normales Studieren? Pandemiebedingt kaum möglich.

>> Mehr Informationen:

Begründung zur Corona-Verordnung Studienbetrieb vom 23.8.2021: https://www.baden-wuerttemberg.de/fileadmin/redaktion/m-mwk/intern/bilder/Corona/21_08_23_Begr%C3%BCndung_CVO_Studienbetrieb.pdf

Sechste Verordnung der Landesregierung zur Änderung der Corona-Verordnung vom 17.12.2021: https://www.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Coronainfos/211217_Sechste_VO_der_LReg_zur_Aenderung_der_CoronaVO.pdf <<

Die Corona-Warn-App konnte im Verlauf des Jahres auch zum Check-in in Cafés genutzt werden.

legt werden (Artikel 6 Absatz 3 Satz 2 DS-GVO). Diese Vorgabe der DS-GVO hat ihren guten Grund: Denn nur wenn der Zweck eindeutig festgelegt ist, kann geprüft werden, ob eine Datenverarbeitung zur Zweckerreichung geeignet, erforderlich und angemessen ist (vgl. Artikel 5 Absatz 1 Buchstabe c DS-GVO) und ob der Zweck einer Weiterverarbeitung noch mit dem ursprünglich verfolgten Zweck vereinbar ist (vgl. Artikel 6 Absatz 4 DS-GVO).

Vor dem Hintergrund dieses Gebots der Zweckfestlegung war z. B. problematisch, dass die CoronaVO in der bis zum 19. Dezember 2021 gültigen Form festlegte, dass der zur Überprüfung von Impfnachweisen Verpflichtete stets Einsicht in ein *„amtliches Ausweisdokument"* nehmen müsse. Abgesehen davon, dass die Formulierung dahingehend hätte verstanden werden können, dass hiermit eine Obliegenheit zur ständigen Mitführung und Vorlage des Personalausweises begründet werden soll, fehlte eine hinreichende Definition des Zwecks dieser Einsichtnahme im Normentext. Auf unseren Hinweis wurden immerhin zunächst in die Begründung der Verordnung vom 23. November 2021 zu § 6a CoronaVO weitere wesentliche Ausführungen hierzu aufgenommen. So wurde dort insbesondere dargelegt, dass die Angaben in dem Ausweisdokument ausschließlich zu dem nach dieser Verordnung vorgesehenen Zweck des Abgleichs der Personalien mit den Angaben auf dem (Impf-)Nachweis genutzt werden dürften, um eine missbräuchliche Nutzung von Nachweisen zu verhindern, und dass unter einem amtlichen Ausweis im Sinne der Vorschrift nicht nur der Personalausweis zu verstehen sei, sondern alle Ausweisdokumente gelten, die zum Nachweis der Identität einer Person geeignet und von einer Behörde oder sonstigen Stelle, die Aufgaben der Verwaltung wahrnimmt, ausgestellt worden sind.

In die gemeinsam mit dem Sozialministerium überarbeitete, ab dem 19. Dezember 2021 geltende Fassung wurde dann der Zweck der Einsichtnahme in das amtliche Ausweisdokument dahingehend im Normentext angegeben, dass die Verpflichteten die Test-, Impf- oder Genesenennachweise *„zum Zweck der Identitätsprüfung mit den Personalien der nachweispflichtigen Person abzugleichen"* haben, *„sofern nicht die Identität anderweitig bekannt ist."*

Ein weiteres Beispiel für eine mit Blick auf den Zweck unklare Regelung war die Bestimmung in § 6a Satz 4 CoronaVO in der Fassung der Änderungsverordnung vom 23. November 2021. Danach waren die

„zur Überprüfung der Nachweise Verpflichteten […], soweit dies nicht technisch ausgeschlossen ist, verpflichtet, elektronische Anwendungen zur Überprüfung einzusetzen",

ohne dass geregelt worden wäre, was diese elektronischen Anwendungen denn leisten beziehungsweise überprüfen müssen. Auch diese Bestimmung konnte mit unserer Mitwirkung durch die Änderungsverordnung vom 17. Dezember 2021 präzisiert werden. Sie lautet nunmehr:

„Die zur Überprüfung von Nachweisen im Sinne des § 6 Absatz 1 Verpflichteten haben die nach Absatz 2 Satz 2 vorzulegenden Impfnachweise mittels elektronischer, dazu vorgesehener Anwendungen zu verifizieren, die die Echtheit der Signatur des Zertifikatsausstellers mit dem Stand der Technik entsprechenden Methoden überprüfen. Dabei darf die Verarbeitung der in dem Nachweis nach Absatz 2 Satz 2 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."

Geeignet, erforderlich, angemessen?

Ein Hauptbestandteil unserer Prüfung ist stets, ob die vorgesehene Datenverarbeitung zur Erreichung des so festgelegten Zwecks geeignet, erforderlich und angemessen ist. Ein dafür im Rahmen der Corona-Verordnungen immer wieder zu klärender Punkt ist dabei, inwieweit eine Speicherung personenbezogener Daten (etwa zum Zweck der Dokumentation einer ordnungsgemäßen Kontrolle) statt einer bloßen visuellen Einsichtnahme ohne Speicherung erforderlich ist.

Dankenswerter Weise ist die Landesregierung insoweit immer wieder auf unseren Hinweis eingegangen und hat nicht nur den Begriff der bloßen „Vorlage" von Nachweisen verwendet, sondern auch in den Begründungen zur Verordnung ausgeführt, dass mit der Pflicht beziehungsweise Obliegenheit zur Vorlage und Prüfung keine Verpflichtung oder Berechtigung zur Speicherung durch den Überprüfenden begründet werden soll.

Im Übrigen lässt sich freilich über die Erforderlichkeit und Angemessenheit von Eingriffen in das Recht auf informationelle Selbstbestimmung vielfach trefflich streiten. Wir haben insoweit regelmäßig auf in Betracht zu ziehende mildere Maßnahmen hingewiesen. Eine solche mildere Maßnahme kann es z. B. sein, nur stichprobenartige statt flächendeckende Kontrollen oder lückenlose Nachweispflichten anzuordnen (s. dazu oben das Beispiel mit der CoronaVO Studienbetrieb); diese Möglichkeit, von der immerhin z. B. der Bundesgesetzgeber in § 28b Absatz 5 Satz 3 IfSG für die Kontrollen des Immunisierungs- beziehungsweise Teststatus der Fahrgäste durch Beförderer Gebrauch gemacht hat, wird häufig zu wenig in Erwägung gezogen. Freilich steht dem Verordnungsgeber, der letztlich auch

Corona-Tests sind an Schulen zu einer Pflicht geworden.

die politische Verantwortung für die zu treffende Regelung trägt, bei der Beurteilung der Erforderlichkeit und Angemessenheit eine auch von uns zu respektierende Einschätzungsprärogative zu.

Besondere Beachtung verdient bei den Regelungsentwürfen zur Bekämpfung der Corona-Pandemie auch die Frage, ob die besonderen Voraussetzungen für die Verarbeitung von Gesundheitsdaten aus Artikel 9 DS-GVO beachtet werden. Diese dürfen nach der DS-GVO nur unter wesentlich engeren Voraussetzungen verarbeitet werden.

Auf Unverständnis stößt bei uns insoweit etwa die Regelung in § 3 Absatz 1, 2. Halbsatz der CoronaVO Schule (in der Fassung der Verordnung vom 26. September 2021). Nach dem ersten Halbsatz haben die Schulen Schüler_innen und dem dort tätigen Personal in gewissen Abständen Testungen auf das Coronavirus anzubieten. Die Regelung fährt dann im zweiten Halbsatz fort: *„hiervon [sc. von dem Testangebot] ausgenommen sind immunisierte Personen im Sinne des § 4 Absatz 1 CoronaVO."*

Diese Regelung haben wir wiederholt gegenüber dem Kultusministerium kritisiert, weil der Ausschluss immunisierter Personen vom schulischen Testangebot von den Schulen dahingehend verstanden werden könne, dass sie den Impf- oder Genesenenstatus der Schüler_innen sowie des in der Präsenz tätigen Personals schon für die Frage, ob sie einen Test anzubieten haben, überprüfen müssten und anderen Personen (etwa auch solchen, die einen Impf- oder Genesenennachweis nicht vorlegen wollen) keinen Test anbieten dürften. Wir können jedoch nicht erkennen, dass

a) eine Erhebung des Impf- oder Genesenenenstatus zur Einsparung von Kosten (hier nämlich von Kosten der Testung auch von Personen, die immunisiert sind und sich trotzdem einer Testung unterziehen wollen) von einer der Ausnahmen aus Artikel 9 Absatz 2 DS-GVO gedeckt wäre,

b) eine Speicherung des Impf- oder Genesenenstatus des genannten Personenkreises sonst für nach Artikel 9 Absatz 2 DS-GVO zulässige Zwecke erforderlich wäre.

Dass immunisierte Personen nach Auffassung des Kultusministeriums nicht zwingend einen Test benötigen, rechtfertigt allein nicht, diese Personen vom Testangebot auszuschließen und hierfür den Immunisierungsstatus zu verarbeiten, zumal die Testung auch von immunisierten Personen im Interesse des Infektionsschutzes durchaus sinnvoll sein kann, wie die Debatte um 2G und 2G+ zeigt. Leider hat das Kultusministerium diese Kritik nicht aufgegriffen, sondern im Gegenteil mit der Änderungsverordnung vom 7. Januar 2022 – ohne uns insoweit angemessen zu beteiligen – noch einen Passus aufgenommen:

„Soweit es zur Erfüllung der [vorgenannten] Pflichten […] erforderlich ist, darf die Schulleitung zu diesem Zweck personenbezogene Daten einschließlich Daten zum Impf-, Sero- und Teststatus […] in Bezug auf die Coronavirus-Krankheit-2019 verarbeiten."

Wir sehen nicht, dass insoweit eine Verarbeitung von Gesundheitsdaten für im Sinne von Artikel 9 Absatz 2 DS-GVO zulässige Zwecke erforderlich und damit zulässig wäre.

Kurzum, man hätte es einfacher regeln können: Allen Schüler_innen und dem gesamten Lehrpersonal wird ein Test angeboten, ohne dass insoweit der Immunisierungsstatus erhoben oder gespeichert wird. Somit hätte man zweierlei erreicht: Dies ergäbe ein standardisiertes Vorgehen, das allen klar und zugleich datenschutzfreundlich wäre. Und man könnte ergänzen: Wer sich dann nicht immer testen lassen möchte, kann sich durch die Erbringung des Nachweises über die Impfung oder Genesung von der Testung ausnehmen lassen. Leider ist das Kultusministerium dieser klaren und datenschutzfreundlichen Linie nicht gefolgt und hat nun eine Regelung geschaffen, die zu einer Datenverarbeitung ermächtigen soll, deren gewünschter Umfang unklar und deren Berechtigung uns nicht ersichtlich ist.

Von besonderer Bedeutung ist auch, inwieweit die nach Artikel 9 (z. B. Buchstabe i) DS-GVO für die Verarbeitung von Gesundheitsdaten erforderlichen „angemessenen und spezifischen Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person", wie insbesondere Maßnahmen des Berufsgeheimnisses oder sonstiger Geheimhaltungspflichten, vorgesehen sind. Gerade angesichts der massenhaften Erhebung und Verarbeitung von Gesundheitsdaten auch durch Pri-

vate zum Zweck der Pandemiebewältigung wären insoweit normenklare Regelungen zielführend, die einen Rückgriff auf die wenig konkrete Norm des § 22 BDSG, die lediglich in allgemeiner Form potentielle Schutzmaßnahmen für die Verarbeitung besonderer Kategorien personenbezogener Daten regelt, entbehrlich erscheinen lässt.

Auch im Übrigen sind die Regelungsentwürfe darauf zu prüfen, inwieweit bei den vorgesehenen Datenverarbeitungen überhaupt die Einhaltung angemessener technischer und organisatorischer Maßnahmen zum Datenschutz zu erwarten ist. Diesbezüglich ist etwa bei der Durchführung von massenhaften Tests in Schulen und künftig in Kindertagesstätten zu bedenken, dass den zu testenden Personen der Test als medizinische Untersuchung so anzubieten ist, das weder die Testteilnahme für Dritte beobachtbar ist noch das Testergebnis für Unbefugte offenbar wird. Bei Reihentestungen in Schulungen und Kindertagesstätten scheint dies in der Praxis allerdings schwerlich realisierbar.

Klare Normen, klarer Blick

Einen wesentlichen Prüfungspunkt stellt darüber hinaus die Frage dar, ob die Regelungen zur Verarbeitung von personenbezogenen Daten mit Blick insbesondere auf das deutsche Verfassungsrecht ausreichend normenklar sind. Dies scheint uns nicht durchweg gegeben zu sein, wobei die Grenzen zwischen einer zur Nichtigkeit führenden Normenunklarheit und einer bloßen durch Auslegung noch zu „rettenden" Unschärfe natürlich fließend sind.

So wurde etwa die bereits in unserem vergangenen Tätigkeitsbericht (im Beitrag „Befreiung von der Maskenpflicht: nicht ohne meinen Arzt") kritisierte Regelung nicht konkretisiert, wem gegenüber eine Person, der das Tragen einer medizinischen Maske oder einer Atemschutzmaske aus gesundheitlichen Gründen nicht möglich oder nicht zumutbar ist, diese Umstände wie glaubhaft machen muss. Auch wenn der Verwaltungsgerichtshof Baden-Württemberg diese Norm für bestimmte Anwendungsfälle gegenüber öffentlichen Einrichtungen wie den Schulen nicht beanstandet und durch seine Rechtsprechung (insbesondere durch Beschluss vom 8. Juli 2021 – 1 S 2111/21) näher konkretisiert hat, bleibt fraglich, gegenüber wem und mit welchem Detailierungsgrad in anderen Fällen die Glaubhaftmachung zu erfolgen hat. Durch normenklarere Regelungen, insbesondere die Umsetzung der im vergangenen Tätigkeitsbericht angeregten alternativen Gestaltungsmöglichkeiten,

Zahlreiche Verodnungen hat die Landesregierung erlassen. Nicht immer wurde der LfDI eingebunden.

hätte hier viel Streit und Ungewissheit vermieden werden können.

Ein kurioses Beispiel für eine Normenunklarheit, auf das wir das Kultusministerium wiederholt – leider ohne Korrekturerfolg – hingewiesen haben, ist ferner etwa die Regelung in § 10 Absatz 1 Nummer 6 und Absatz 2 Nummer 3 CoronaVO Schule in der Fassung vom 26. September 2021. Diese Bestimmung lautet auszugsweise:

„§ 10 Zutritts- und Teilnahmeverbot
(1) Für die Einrichtungen nach § 1 Absatz 1 besteht ein Zutritts- und Teilnahmeverbot für Schülerinnen und Schüler, für Kinder, Lehrkräfte sowie sonstige Personen, […]

6. die weder einen Testnachweis im Sinne von § 3 Absatz 2 noch einen Impf- oder Genesenen-Nachweis im Sinne des § 4 Absatz 2 CoronaVO vorlegen.
(2) Das Zutritts- und Teilnahmeverbot nach Absatz 1 Nummer 6 besteht nicht
[…]
3. für immunisierte Personen im Sinne des § 4 Absatz 1 CoronaVO, …“

Die geneigte Leserschaft mag selbst entscheiden, ob eine immunisierte Person (nach den in Bezug genommen Vorschriften ist darunter eine geimpfte oder genesene Person zu verstehen, die einen entsprechenden Nachweis besitzt) zur Vermeidung des Zutritts- und Teilnahmeverbots ihren Nachweis über den Immunisierungsstatus vorlegen muss – und die Schule diesen prüfen darf. Nachdem die in Absatz 1 begründete Obliegenheit, einen Impf- oder Genesenennachweis vorzulegen, um den Zutritt zu erlangen, nach Absatz 2 für genesene und geimpfte Personen nicht gelten soll, scheint dies nicht der Fall zu sein. Ob dieses Ergebnis der Intention des Gesetzgebers entspricht, sei dahingestellt.

Teilweise waren wir mit unseren Bitten um Klarstellung insoweit erfolgreich. Anzumerken bleibt, dass wir uns bewusst sind, dass es ein äußerst schweres bis nahezu unmögliches Unterfangen ist, Normen so zu formulieren, dass sie über jeden Zweifel erhaben sind. Hinzu kommt, dass durch die sich ebenfalls ständig ändernden bundesrechtlichen Vorgaben die Formulierung von Landesregelungen „im Akkord“ nicht einfacher wird. Gleichwohl wären eine klarere Sprache und Systematik der Corona-Verordnungen – auch wo die Formulierungen nicht von Rechts wegen zu beanstanden sind – bürgerfreundlicher und würden sicherlich zu einer größeren Akzeptanz beitragen.

Gesetze und Verordnungen können kompliziert sein – sie sollten, so gut es geht, einfach und verständlich erklärt werden.

Ein wesentlicher zu Unklarheiten führender Gesichtspunk im Aufbau des Systems der Corona-Verordnungen sei noch angeführt: Die Corona-Verordnung regelt vielfach selbst Sachverhalte, obwohl sie zugleich eine subdelegierende Verordnungsermächtigung zur Regelung desselben Sachverhalts enthält.

So regelt etwa § 14 Absatz 1 der CoronaVO detailliert – unterschieden nach der jeweiligen Pandemiestufe (Basis-, Warn- oder Alarmstufe I oder Alarmstufe II im Sinne von § 1 Absatz 2 und 3 CoronaVO) –, unter welchen Bedingungen und unter Vorlage welcher (Test-)Nachweise Sportstätten betreten werden dürfen beziehungsweise der Zutritt verboten ist, wobei noch Sonderregelungen für Sport zu dienstlichen Zwecken und für Reha-Sport getroffen werden. Dennoch werden in § 21 Absatz 5 CoronaVO das Kultusministerium und das Sozialministerium ermächtigt, durch gemeinsame Rechtsverordnung für den Betrieb von Sportstätten zum Schutz vor einer Infektion mit dem Coronavirus Bedingungen und Anforderungen, Testpflichten und Zutrittsverbote festzulegen. Was soll die subdelegierte Corona-Verordnung Sport denn nun noch regeln? Und inwieweit darf sie dabei von den Vorgaben der Corona-Verordnung abweichen? Dieses wenig sinnvolle System führt dazu, dass a) die kraft der Subdelegation erlassenen Verordnungen vielfach deklaratorische Wiederholungen der Hauptverordnung enthalten, b) bei Abweichungen von der Hauptverordnung aber die Zulässigkeit dieser Regelungen fragwürdig ist. Hier wäre es deutlich übersichtlicher und normenklarer, wenn entweder der Regelungsbereich komplett in der Hauptverordnung geregelt würde oder vollständig der Unter-Verordnung zur Regelung überlassen bliebe.

Kritisch bleiben, Austausch fördern

Abschließend ist zu festzuhalten, dass mit fortschreitender Dauer der Pandemie die Eingriffe in das informationelle Selbstbestimmungsrecht durch das Recht der Corona-Verordnungen im Berichtsjahr fast durchweg gravierender wurden. Dies sei nur an wenigen Beispielen ausgeführt:

- Während zunächst an den Schulen nur Testangebote für Schüler_innen unterbreitet wurden, wurde im Laufe des Jahres die Offenlegung von Testergebnissen zunächst zur Obliegenheit für die Teilnahme am Präsenzunterricht und zuletzt zum Teil der Schulpflicht.

Ausblick: Der LfDI wird künftig datenschutzrechtliche Schulungen für Ministerien anbieten um die Zusammenarbeit zu stärken.

- Generell wurden Testobliegenheiten zunächst nur für das Betreten von Krankenhäusern und ähnliche vulnerable Einrichtungen eingeführt; inzwischen sind sie ubiquitär zu erfüllen, wobei teilweise – je nach Pandemiegeschehen – ausschließlich PCR-Tests akzeptiert werden.

- Die Obliegenheit, Impfnachweise vorzulegen, wurde erst im Mai 2021 eingeführt und seitdem ausgebaut beziehungsweise zum Teil noch durch zusätzliche Obliegenheiten zur Vorlage von Testnachweisen verstärkt. Dabei waren die Geimpften zunächst frei in der Führung des Nachweises, bis mit der Änderungsverordnung vom 23. November 2021 bestimmt wurde: *„Impfnachweise sind in digital auslesbarer Form vorzulegen"*, was den vorherigen Erwerb des – an sich freiwillig zu beziehenden – digitalen Impfzertifikats voraussetzt.

- Die Verpflichtungen zur Überprüfung der Impfzertifikate sind massiv ausgebaut worden. Nach der Änderungsverordnung vom 3. Juni 2021 stand zunächst lediglich in § 21 Absatz 8 Satz 2 CoronaVO: *„Anbieter und Betreiber sind zur Überprüfung der Nachweise verpflichtet."* Zu der von uns aufgeworfenen Frage, was genau überprüft werden sollte, insbesondere inwieweit eine Identitätsprüfung vorgenommen werden solle, wurde in einer späteren Begründung ausgeführt, dass lediglich eine Plausibilitätsprüfung der Echtheit durchzuführen sei. Noch in der Begründung der Corona-Verordnung vom 21. September 2021 wurde ergänzend ausgeführt: *„Eine Identitätsüberprüfung erfolgt nicht."* Mit der Änderungsverordnung vom 23. November 2021 wurde dann doch die Identitätsüberprüfung anhand eines amtlichen Ausweisdokuments eingeführt.

- Schließlich sei noch auf die Zunahme der Verarbeitung des Immunisierungsstatus im Beschäftigtenkontext verwiesen (siehe dazu den Beitrag Corona im Betrieb)

Die Landesregierung kann zu der Einschätzung kommen, dass diese zunehmenden Eingriffe in das informationelle Selbstbestimmungsrecht sämtlich zur Pandemiebekämpfung erforderlich und verhältnismäßig sind. Wie ausgeführt steht hier dem Gesetz- und Verordnungsgeber eine zwar nicht uneingeschränkte, jedoch erhebliche Einschätzungsprärogative zu, die weder von uns noch von den Gerichten vollständig überprüft werden kann. Aber schon diese längst nicht abschließende Auflistung zeigt, dass die wiederholt geäußerte Auffassung, das Recht auf informationelle Selbstbestimmung sei durch die Pandemie als einziges Grundrecht „uneingeschränkt davongekommen", verfehlt ist. Anders formuliert: Behauptungen, die informationelle Selbstbestimmung sei unangetastet geblieben, sind schlicht falsch. Hinzu kommt: Das Datenschutzrecht bietet zahlreiche Möglichkeiten für zulässige Datenverarbeitungen. Es behindert keineswegs die Pandemie-Bekämpfung.

Es gelten dabei aber Regeln, die zu beachten sind. Insbesondere bedarf es hierzu normenklarer Gesetze beziehungsweise Verordnungen. Gesetzgeberische und exekutive Defizite bei der Pandemie-Bekämpfung „dem Datenschutz" anzulasten, ist dann doch etwas zu einfach. Natürlich bleiben wir dankbar für jede fachliche Kritik, die uns dabei hilft, unsere Kontroll- und Beratungsaufgabe besser zu erfüllen.

Davon unabhängig: Wir werden auch künftig bei der Pandemie-Bekämpfung nach Kräften helfen und, so gut es geht, im Interesse der Bürger_innen handeln. Wir wissen, dass die Ministerien unter Hochdruck arbeiten, um einen bestmöglichen Gesundheitsschutz sicherzustellen. Wir werden gleichwohl die Entwicklung weiterhin kritisch begleiten und auf eine angemessene Rücknahme der Einschränkungen des Rechts auf informationelle Selbstbestimmung drängen, soweit und sobald das Pandemiegeschehen dies zulässt.

Unser Fazit: Die Corona-Verordnung sehen mit andauerndem Pandemiegeschehen in der Tendenz zunehmende Einschränkungen des informationellen Selbstbestimmungsrechts vor. Beim Erlass der Regelungen wurden wir nicht immer ordnungsgemäß beteiligt. Zur verbesserten Verankerung der Prinzipien des Datenschutzes in der Normengebung des Landes planen wir für das kommende Jahr unter anderem, für Referent_innen der Ministerien, die mit dem Entwurf von Regelungen betraut sind, Fortbildungen zu den zu beachtenden europa- und verfassungsrechtlichen Anforderungen des Datenschutzes anzubieten. Wir hoffen, hierdurch auch den konstruktiven Austausch mit den Ministerien weiter fördern zu können.

Tabubruch: Gesundheitsinformationen der Beschäftigten gingen Arbeitgebende bislang nichts an. Mit der neuen Regelung von 3G am Arbeitsplatz hat sich das nun geändert.

1.1 Corona im Betrieb

Das Jahr 2021 stand nach wie vor im Zeichen der Covid-19 Pandemie. Den Mittelpunkt unserer Tätigkeit bildeten daher die unzähligen Beratungsanfragen, insbesondere zum datenschutzkonformen Umgang mit den enormen organisatorischen Herausforderungen der Pandemie für viele Betriebe und Arbeitgebende.

Abfrage Impfstatus durch Arbeitgebende

Mit Blick auf die mittlerweile bestehende Möglichkeit eines Impfschutzes fokussierten sich die Anfragen zunehmend auf die Frage, ob die Abfrage des Impfstatus durch Arbeitgebende datenschutzrechtlich zulässig ist. Bei der Beurteilung der Fragestellungen klang stets die Sorge mit, gesellschaftliche Verwerfungen hinsichtlich der Freiwilligkeit der Impfung nicht in die Betriebe zu tragen, da der betriebliche Kontext oftmals wie ein Brennglas wirkt, etwa bestehende Friktionen zwischen Arbeitgebenden und Beschäftigten sich verstetigen und Beschäftigungsverhältnisse unumkehrbar zerrütten können. Dennoch war das Interesse der Arbeitgebende an der Offenlegung des Impfstatus durch die Beschäftigten groß. Bei dem Datum „Impfstatus" handelt es sich um ein Gesundheitsdatum gem. Art. 4 Nr. 15 DS-GVO und demnach um eine besondere Kategorie personenbezogener Daten nach Art. 9 DS-GVO.

Im Bereich des Beschäftigtendatenschutzes ist die Verarbeitung dieses sensiblen Datums außerhalb der gesetzlich geregelten §§ 23a IfSG und 36 Abs. 3 IfSG der Sphäre des Arbeitgebenden auch in den besonderen Zeiten der Pandemie grundsätzlich entzogen. Für die Abfrage des Impfstatus innerhalb der Einrichtungen nach § 36 Abs. 1 (beispielsweise Obdachlosenunterkünfte, Justizvollzugsanstalten) ist weiterhin die Feststellung der epidemischen Lage von nationaler Tragweite durch den Bundestag erforderlich, welche seit dem Beschluss am 27. März 2020 auch im Jahr 2021 überwiegend fortbestand.

Trotz der allgemeinen Unzulässigkeit der Abfrage des Impfstatus wurde oftmals ein branchenübergreifendes „berechtigtes Interesse" an der Erhebung dieser Daten vorgebracht. In diesem Zusammenhang ist jedoch die reine Fürsorgepflicht des Arbeitgebers gegenüber den anderen Beschäftigten nicht ausreichend, um die Abfrage des Impfstatus zu rechtfertigen. Auch vor dem Hintergrund der gesetzgeberischen Entscheidung, Impfstatus-Abfragen nur für bestimmte Branchen und Einrichtungen zuzulassen, ist eine Erhebung auf Grundlage allgemeiner arbeitsschutzrechtlicher Erwägungen jedenfalls nicht zulässig. Vielmehr waren Arbeitgebende zunächst auf organisatorische Maßnahmen zur Pandemiebekämpfung sowie auf das reine Anbieten von Tests zur eigenverantwortlichen Durchführung zu verweisen. In der SARS-CoV2-Arbeitsschutzverordnung wurde deutlich geregelt, dass das Abstandhalten sowie Tragen einer medizinischen Maske auf Grundlage einer Gefährdungsbeurteilung und unter Berücksichtigung der SARS-CoV2-Arbeitsschutzregel innerbetrieblich auf Grundlage eines Hygienekonzepts umzusetzen sind.

§ 2 Abs. 1 der fortgeschriebenen SARS-CoV2-Arbeitsschutzverordnung normierte mit zunehmender Impfquote der Bevölkerung außerdem, dass Arbeitgebende bei der „Festlegung und der Umsetzung des betrieblichen Infektionsschutzes einen ihm bekannten Impf- und Genesungsstatus der Beschäftigten berücksichtigen" können. Hiermit war zunächst jedoch weiterhin nicht die Befugnis zur Abfrage des Impfstatus verbunden. Auch konnten die Arbeitsschutzmaßnahmen nicht mit Blick auf eine „freiwillige Impfabfrage" außer Acht gelassen werden. Eine mangelnde Sensibilität der Arbeitgebenden für Datenschutzgesichtspunkte und im Hinblick auf die Verbreitung der Gesundheitsdaten offenbarte sich durch zahlreiche Beschwerden von Beschäftigten: So sahen sich einige Betriebe dazu veranlasst, eine allgemeine betriebliche Impfquote zu erheben und diese unter den Mitarbeitenden kundzutun – nicht selten ohne eine hieran geknüpfte Aufforderung an die nicht geimpften Mitarbeitenden, die Inanspruchnahme einer Schutzimpfung nochmals zu überdenken.

Im Sommer 2021 wurden wir beispielsweise auf einen Betrieb aufmerksam gemacht, welcher vor dem Hintergrund einer verträglichen Bürobelegung eine Büroplan versendete, in welchem der jeweilige Impfstatus der Mitarbeitenden mit einer entsprechenden Ampelkennzeichnung vermerkt war (grün = geimpft, orange = teilweise geimpft, rot = nicht geimpft). Hiergegen schritten wir sofort ein.

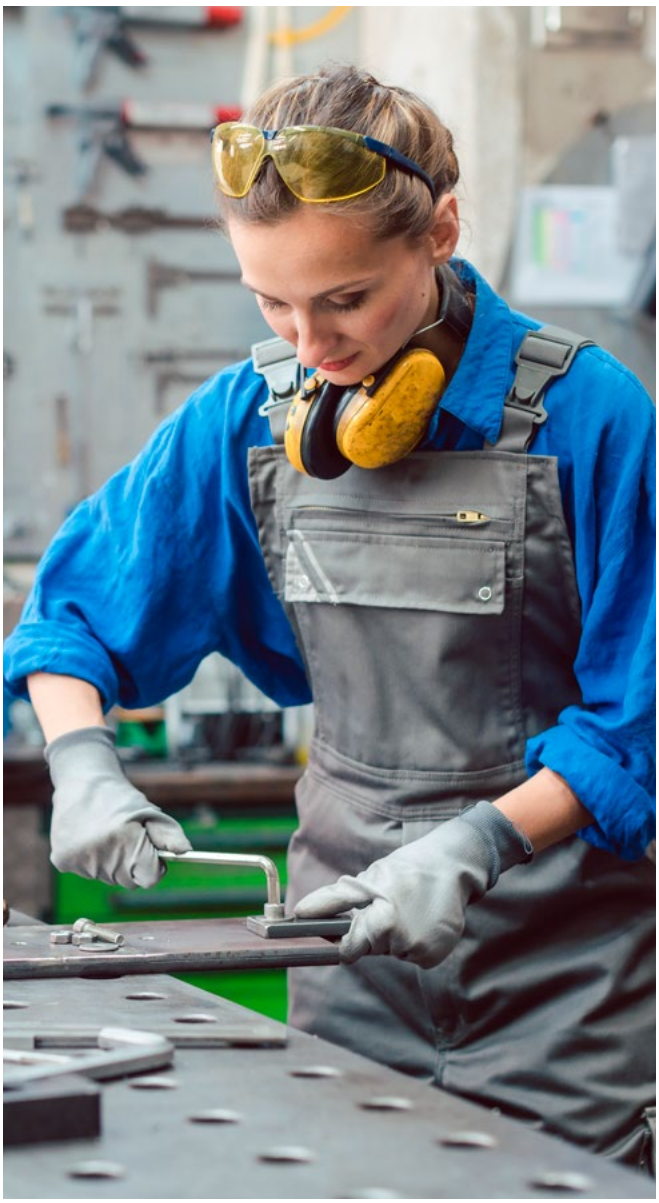
Im Zuge der Umsetzung des 2G-Optionsmodells, welches im Herbst Einklang in die landesrechtliche CoronaVO fand und Beschäftigten mit Kontakt zu Dritten die Möglichkeit geben sollte, bei freiwilliger Bekanntgabe des Impfstatus ohne eine entsprechende Mund-Nasen-Bedeckung zu arbeiten, sahen sich Arbeitgebende mit der Frage konfrontiert, inwieweit dies umsetzbar ist, ohne hierbei einen „Offenbarungsdruck" auf die jeweiligen Beschäftigten auszuüben. Vordergründig war hier das Dilemma aufzulösen, in welchem Maße bei einem kollektiven Zwang, ohne Maske zu arbeiten, noch eine Freiwilligkeit bei der Offenlegung des Impfstatus angenommen werden kann.

Saisonal bedingt stiegen in Deutschland die Zahlen der COVID-19-Infektionen im Herbst trotz zahlreicher Impfungen nochmals heftig an. Neben zahlreichen anderen Einschränkungen wurde die sogenannte „4. Welle" zum Anlass genommen, den betrieblichen Infektionsschutz weiter zu intensivieren und entsprechende neue Regelungen zu erlassen.

Mit Inkrafttreten des § 28b IfSG wurde im November 2021 erstmals eine bundesweite gesetzliche Grundlage für eine 3G-Zugansregelung am Arbeitsplatz geschaffen und Arbeitgebenden eine ausdrückliche Verarbeitungsbefugnis des Impfstatus ihrer Beschäftigten eingeräumt. Jedoch gewährte auch diese Ermächtigung Arbeitgebenden kein vollumfängliches Auskunftsrecht im Hinblick auf den Immunisierungsstatus ihrer Beschäftigten. Vielmehr war es den Beschäftigten weiterhin freigestellt, ihren Immunisierungsstatus zurückzuhalten und statt ihren Impf-oder Genesenenstatus zu offenbaren Zutritt, in die Arbeitsstätte auch durch Vorlage eines tagesaktuellen Testnachweises erhalten zu können.

Wesentliche Fragen zur Dokumentationspflicht sowie zur Speicherung der Gesundheitsdaten wurden von §28b IfSG weiterhin offengelassen. So häuften sich bereits in den ersten Tagen nach Inkrafttreten des Bundesgesetzes Beschwerden über Arbeitgebende, die über eine Sichtkontrolle hinaus beispielsweise das Einsenden von Screenshots des digitalen Impfzertifikats verlangten.

Da die Rechtsunsicherheit zunächst groß war und bei Erlass der Neuregelung des §28b IfSG nicht bekannt war, ob und mit welchem Inhalt das Bundesministerium für Arbeit und Soziales von seiner Verordnungsermächtigung zur Konkretisierung der Dokumentationspflichten und -möglichkeiten Gebrauch machen würde, hieß es, schnell zu reagieren. Kurz nach dem Inkrafttreten der Neuregelung veröffentlichten wir daher eine Handreichung zur Konkretisierung der 3G-Regelungen am Arbeitsplatz, um Arbeitgebenden in der ersten Zeit nach Inkrafttreten des §28b IfSG eine Orientierungshilfe zur datenschutzkonformen Umsetzung in die betrieblichen Praxis zu geben.



© Kzenon – stock.adobe.com

Wer vor Ort im Betrieb arbeiten will, muss einen 3G-Nachweis bei sich führen.

Impfung durch Betriebsmedizin – Impfabfrage durch die Hintertür?

Nachdem die Betriebsmedizin als Teil der „Nationalen Impfstrategie COVID-19“ ab dem 7. Juni 2021 systematisch in die „Impfung am Arbeitsplatz“ eingebunden wurde (vgl. Nationale Impfstrategie COVID-19 des Bundesministeriums für Gesundheit v. 22. Juni 2021) nahm die Diskussion hinsichtlich der Abfrage des Impfstatus durch Arbeitgebende nochmals Fahrt auf.

Diesbezüglich wandten sich insbesondere Arbeitgebende, betriebliche Datenschutzbeauftragte, aber auch Mitglieder der Arbeitnehmervertretungen an uns. Hintergrund waren neue datenschutzrechtliche Fragestellungen im Zusammenhang mit der Vereinbarung von Impfterminen mit der Betriebsmedizin.

Gesondertes Augenmerk war hier auf den betrieblichen Kontext der Rahmenbedingungen bei der Einbeziehung der Betriebsmedizin zu richten. In der Regel befinden sich die Betriebsmedizin oder, je nach Größe des Unternehmens und Betriebs, die errichteten Impfzentren auf dem Werksgelände des jeweiligen Unternehmens. Möchte ein_e Beschäftigte_r zudem, dass die Warte-, Behandlungs- und Ruhezeiten als Arbeitszeit erfasst werden, muss sie/er den jeweiligen Arbeitgebenden oder die vorgesetzte Person zunächst auch Rechenschaft ablegen, wo und auf Grund welcher betrieblichen Veranlassung hin die konkrete Arbeitszeit verbracht wurde. Für Produktionsmitarbeitende im Schichtdienst muss zudem für die Dauer des Gangs zur Betriebsmedizin meist auch eine Vertretung disponiert werden. Den Beschäftigten steht es frei zu entscheiden, ob sie das Angebot annehmen wollen oder ob sie sich stattdessen selbst um einen Impftermin bei Haus-/ Fachärzt_innen bemühen wollen.

So befürchteten viele Beschäftigte, dass die Teil-/ oder insbesondere Nichtteilnahme am Impfprogramm durch die Betriebsmedizin vom Arbeitgebenden bemerkt und entsprechend erhoben werden könnte, und dass die Arbeitgebenden so etwa „durch die Hintertür“ den Impfstatus der Mitarbeitenden erfahren könnten. Hiergegen wendeten viele Arbeitgebende berechtigterweise ein, dass Impfstoffe nur schwer zu lagern seien und nach Öffnung keine lange Haltbarkeit mehr hätten, sodass die Vergabe und Planung der Impftermine systematisch und mit Blick auf interessierte Beschäftigte notwendigerweise mit einer gewissen Planungssicherheit einhergehen müsse.

Aus unserer Sicht war im Rahmen der datenschutzrechtlichen Beurteilung zum einen entscheidend, ob es sich bei einer reinen Terminvereinbarung mit der Betriebsmedizin und der damit einhergehenden Mitteilung, dass man etwa für einen näher bezeichneten Zeitraum auf Grund des Termins nicht zur Verfügung stehe, bereits um ein Gesundheitsdatum nach Art. 9 Abs. 1 DS-GVO handelt.

Die Kenntnis, dass eine beschäftigte Person schlichtweg einen Termin oder einen „Zeitslot“ bei der Betriebsmedizin gebucht hat, ohne dass darüber hinaus nähere Informationen vorliegen, genügt für sich allein genommen noch nicht, um von einem Gesundheitsdatum im Sinne des Art. 9 Abs. 1 DS-GVO auszugehen. So kann es sich hierbei beispielsweise auch etwa nur um ein Impfberatungsgespräch oder andere Beratungs-/ Vorsorgemaßnahmen der betrieblichen Gesundheitsfürsorge handeln. In diesem Sinne entschied etwa auch der französische Conseil d´Etat (vgl. Conseil d´Etat, Urt. v. 12.03.2021 – 450163) vor dem Hintergrund der Nutzung einer App mit Drittstaatentransfer zur Terminvergabe von Impfterminen. Das Gericht führte hierbei aus, dass etwa reine Termindaten hinsichtlich einer beabsichtigten Impfung noch keine besonders sensiblen Gesundheitsdaten darstellen. Sobald allerdings weitere Informationen hinzutreten und sich die Umstände derart verdichten, dass der Impfstatus eines Beschäftigten konkretisiert und ableitbar wird, kann durchaus mit allen in Frage kommenden Konsequenzen, ein Gesundheitsdatum angenommen werden.

Wir haben daher dahingehend beraten, dass die Impfterminkoordination weitgehend unter der Federführung der Betriebsmedizin zu erfolgen habe. Nachdem die Impfpriorisierungen aufgegeben wurden und ebenfalls auch Haus-/ oder Fachärzt_

>> Mehr Informationen:

Orientierungshilfe des LfDI zur datenschutzkonformen Umsetzung in die betrieblichen Praxis https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/11/Orientierungshilfe-3G_Arbeitsplatz.pdf <<

innen in die Impfkampagne eingebunden wurden, war für Arbeitgebende allerdings ohnehin nicht mehr erkennbar, ob sich die Beschäftigten nicht „privat" bereits um einen Impftermin bemüht hatten.

Einführung von 3G im Betrieb

Die zu Pandemiebeginn nahezu bundesweit umgesetzte und geschätzte Arbeit im Homeoffice wurde im Jahr 2021 mehr und mehr von dem Wunsch der Arbeitgebende verdrängt, wieder einen kollegialen Austausch herzustellen und die Beschäftigten zu diesem Zwecke „zurück in die Betriebe kehren zu lassen". Um eine sichere Rückkehr an den Arbeitsplatz sowie die dauerhafte Arbeit in Präsenz zu ermöglichen, häuften sich die Anfragen, inwieweit ein Betrieb selbständig die „3G-Regel" einführen könne.

Für die meisten Branchen war für die Erhebung der 3G im Betrieb keine einschlägige Rechtsgrundlage vorhanden. Auch wenn in der CoronaVO zwischenzeitlich Teilnahme- und Zutrittsverbote für Personen ohne 3G-Nachweise für einzelne Veranstaltungen und Einrichtungen normiert waren, so konnte jedenfalls eine allgemeine „3G-Erhebung" im Betrieb in der Regel im Laufe des Jahres zunächst nicht datenschutzkonform durchgeführt werden.

Neben der rein innerbetrieblichen Fragestellung stellten sich auch Abgrenzungsschwierigkeiten im Hinblick auf den Betrieb von Betriebskantinen. Hier wurde seitens des Verordnungsgebers zeitweise der Zutritt ebenfalls nur für 3G vorgesehen. Die Arbeitgebenden sahen sich demnach vor die Herausforderung gestellt, diese Gesundheitsdaten nur zum Zwecke der Begehung der Betriebskantine zu erheben. Da hierbei vom Verordnungsgeber eine reine Überprüfung durch Kenntnisnahme in Form einer Sichtkontrolle gefordert wurde, konnten wir von solchen Ideen, wie der Erstellung eines grünen Kantinenpasses für die geimpften und genesenen Mitarbeitenden, nur abraten.

Auch der mit dem erneuten Steigen der Infektionszahlen im frühen Herbst laut gewordene Wunsch, ebenfalls die Betriebskantinen im 2G-Modell betreiben zu dürfen, war in der landesrechtlichen Verordnung sowie in bundesrechtlichen Vorschriften erst einmal nicht aufgenommen worden und war somit datenschutzrechtlich nicht ohne Weiteres abzubilden.

Mit der Frage, ob eine kollektivrechtliche Vereinbarung prinzipiell als Rechtsgrundlage für die Verarbeitung des 3G-Status in Betracht gezogen werden kann, beschäftigten sich die Gerichte nur vereinzelt. Zwar hatte das Arbeitsgericht Offenbach (4 Ga 1/21) mit Beschluss vom 03. Februar 2021 entschieden, dass ein Arbeitnehmer im Rahmen einer Betriebsvereinbarung zur Durchführung eines COVID-Schnelltests vor Aufnahme seiner Tätigkeit verpflichtet werden kann. Diese im einstweiligen Rechtsschutz ergangene Entscheidung ist vor dem Hintergrund der gesetzgeberischen Wertung der §§ 23a, 36 IfSG und im Bereich von Produktionsstätten aber durchaus fragwürdig.

Auch hier wurde erst im November mit Inkrafttreten des § 28b IfSG eine Rechtsgrundlage zur Abfrage des 3G-Status normiert, was jedoch weiterhin zu zahlreichen Umsetzungsschwierigkeiten in der Praxis sowie Beschwerden führte.

Abfrage des Impfstatus in besonderen Fällen insbesondere in der Heil-/ Pflegebranche

Besonderheiten bestehen bei der Abfrage des Impfstatus bei Berufen der Heil- und Pflegebranche. Viele Beschäftigte und Arbeitgebende sind nach wie vor verunsichert, ob und inwieweit im Kontext von Einrichtungen, in denen vulnerablen Personen sind, Abfragen zulässig sind. Zu berücksichtigen ist hierbei, dass § 23a IfSG ausdrücklich die Verarbeitung des Impf- und Serostatus von Beschäftigten in den dort näher bezeichneten Einrichtungen wie etwa Krankenhäuser und Arztpraxen (vgl. § 23 Abs. 3 IfSG) ermöglicht. Hintergrund dieser Befugnis ist der stetige Kontakt zu besonders vulnerablen Personengruppen, wie z. B. kranken oder alten Menschen.

Die Verarbeitung des Impfstatus wurde im Sommer 2021 durch die Regelung des § 36 Abs. 3 IfSG etwa für Gemeinschaftseinrichtungen, Justizvollzugsanstalten und Obdachlosenunterkünfte erweitert. Darin heißt es:

„Sofern der Deutsche Bundestag nach § 5 Absatz 1 Satz 1 eine epidemische Lage von nationaler Tragweite festgestellt hat und soweit dies zur Verhinderung der Verbreitung der Coronavirus-Krankheit-2019 (COVID-19) erforderlich ist, darf der Arbeitgeber in den in den Absätzen 1 und 2 genannten Einrichtungen und Unternehmen personenbezogene Daten ei-

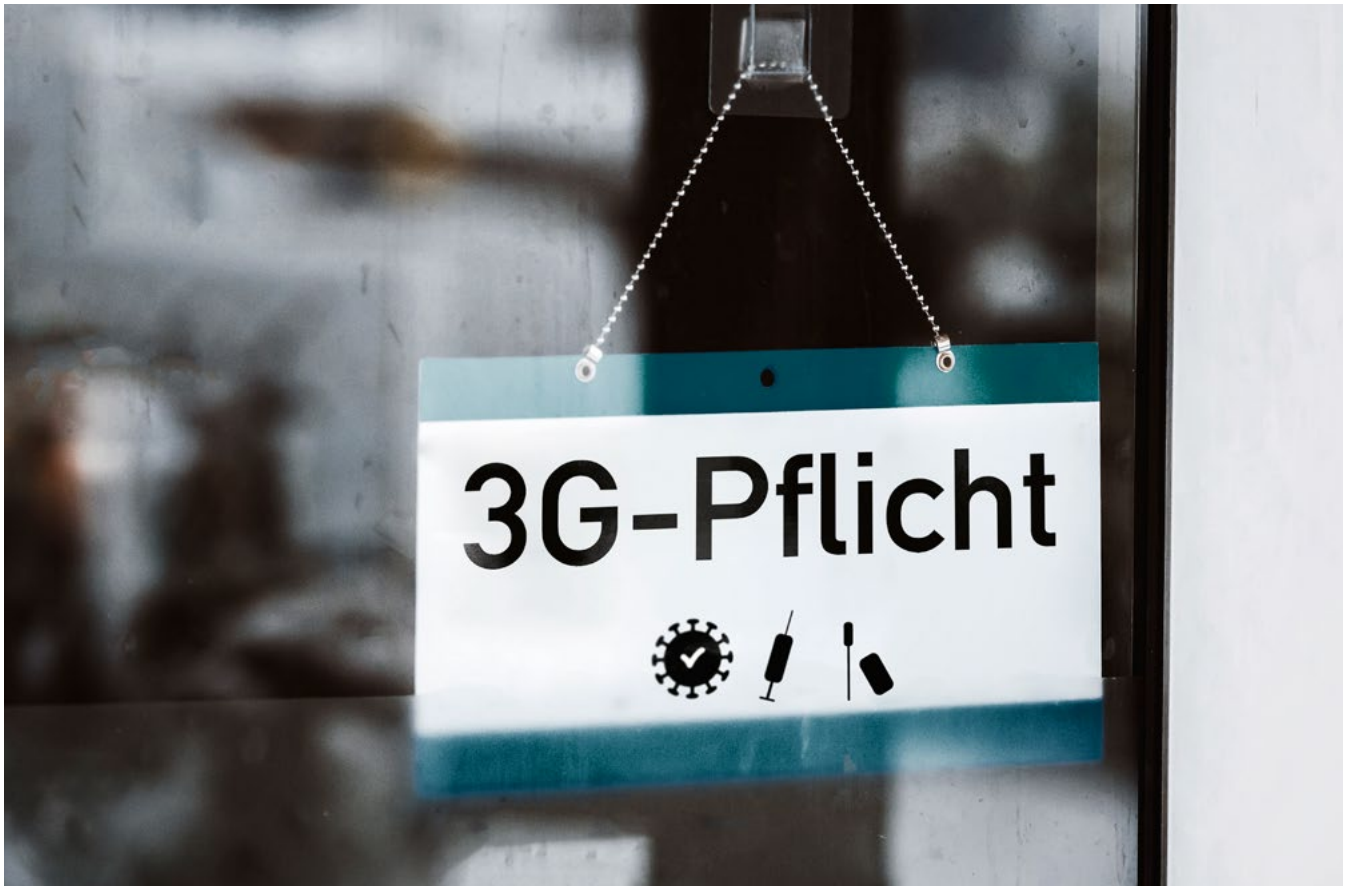
nes Beschäftigten über dessen Impf- und Serostatus in Bezug auf die Coronavirus-Krankheit-2019 (COVID-19) verarbeiten, um über die Begründung eines Beschäftigungsverhältnisses oder über die Art und Weise einer Beschäftigung zu entscheiden. Im Übrigen gelten die Bestimmungen des allgemeinen Datenschutzrechts".

Die Regelung erweitert damit das Fragerecht auf weitere Bereiche und ausdrücklich auf den Beschäftigtenkontext und stellt die Abfrage unter den Vorbehalt der Erforderlichkeit. Damit wird ein Gleichlauf mit dem schonenden und die widerstreitenden Interessen abwägenden Vorbehalt der Erforderlichkeit im engeren Sinne nach § 26 Abs. 3 BDSG gewährleistet. Gleichwohl handelt es sich hierbei um Ausnahmeregelungen, welche nicht auf andere Branchen, Betriebe und Produktionsstätten übertragbar sind.

In Baden-Württemberg besteht darüber hinaus auch die Verordnung des Sozialministeriums zur Eindämmung von Übertragungen des Virus SARS-CoV-2 in Krankenhäusern, Pflegeeinrichtungen und vergleichbaren Einrichtungen sowie Unterstützungsangeboten im Vor- und Umfeld von Pflege, sogenannte „CoronaVO Krankenhäuser und Pflegeeinrichtungen" vom 24. August 2021. Die Verordnung sieht in § 2 Abs. 12 vor:

„Das nicht-immunisierte Personal im Sinne von § 5 Absatz 1 CoronaVO von Einrichtungen nach § 1 Nummer 1 hat sich arbeitstäglich einem Antigen-Schnelltest in Bezug auf eine Infektion mit dem Coronavirus zu unterziehen; für immunisierte Personen im Sinne des § 4 Absatz 1 Satz 1 und Absatz 2 CoronaVO kann die Einrichtung eine anderweitige Regelung treffen. Das Testergebnis, die Impfdokumentation oder der Nachweis der bestätigten Infektion ist jeweils auf Verlangen der Leitung der Einrichtung vorzulegen; die Einrichtungen haben die erforderlichen Testungen zu organisieren".

Die Verordnung regelt somit nähere Modalitäten der Durchführung von Testungen und knüpft begrifflich an die Immunisierung der Beschäftigten (vgl. „nicht-immunisierte"; „immunisierte" Personen) an. Dies basiert auf der Regelung § 4 Abs. 1



Unsere Aufgabe wird es nach der Pandemie sein, die harten Eingriffe wieder zurückzudrehen.

(„Immunisierte Personen") der Corona-Verordnung – CoronaVO, wonach immunisierte Personen entweder gegen COVID-19 geimpft oder von COVID-19 genesen sind. Mit Blick auf die ohnehin bestehende Befugnisnorm des 23a IfSG für Krankenhäuser und Pflegeeinrichtungen, welche ebenfalls an den „Impf- und Serostatus" anknüpft, bestehen zunächst gegen das Verlangen der Vorlage der näher bezeichneten Nachweise aus datenschutzrechtlicher Sicht keine schwerwiegenden Argumente. Mit Blick auf den Grundsatz der Datensparsamkeit ist aber in jedem Falle kritisch zu prüfen, welche Angaben der vom Beschäftigten tatsächlich erforderlich sind, um die Immunisierung nachzuweisen. Außerdem ist, vor dem Hintergrund der weit und offen gefassten Formulierung „auf Verlangen der Leitung der Einrichtung vorzulegen", eine Klarstellung wünschenswert, ob eine dauerhafte Speicherung möglich sein soll.

Streitfrage der Verdienstausfallentschädigung nach § 56 IfSG

Nachdem die Impfpriorisierung im Herbst zwischenzeitlich aufgehoben wurde und somit die Corona-Schutzimpfung jeder erwachsenen Person zugänglich gemacht werden konnte, wurde seitens des Bundes sowie des Landessozialministeriums die „Änderung der Entschädigungspraxis" angekündigt: Die bei einer Quarantäneanordnung wegen eines Kontakts zu einer infizierten Person bis dato gezahlte Dienstausfallentschädigung sollte zukünftig nicht mehr erstattet werden, wenn der/die Beschäftigte durch die Inanspruchnahme einer Schutzimpfung eine Quarantäne hätte vermeiden können.

Dieser in § 56 Abs. 1 S. 4, 5 IfSG verankerte Grundsatz löste neben einer rechtlichen Diskussion um die Erhebungsbefugnis des Impfstatus zu diesem Zwecke insbesondere auch zahlreiche praktische Folgefragen aus. Die überraschende und eindeutige Positionierung des Bundesgesundheitsamts, wonach

„es [Arbeitgebern] schon heute möglich [sei], in rechtlich zulässiger Weise von ihren Arbeitnehmern die erforderlichen Informationen einzuholen, die für eine wirksame Anwendung des Anspruchsausschlusses nach § 56 Absatz 1 S. 4 IfSG erforderlich sind",

motivierte einige Arbeitgebende in entsprechenden Beratungsanfragen an die Dienststelle, zeitnah zu einer pauschalen Abfrage des Impfstatus für Fälle einer zukünftigen etwaigen Lohnfortzahlung im Quarantänefall überzugehen.

Das berechtigte Interesse der Arbeitnehmenden an einer ununterbrochenen Lohnfortzahlung wird hierdurch konterkariert, dass neben der reinen Darlegung des Impfstatus bei Nicht-Geimpften auch mögliche Kontraindikationen (z. B. schwere Erkrankung/Operation, Schwangerschaft, Immunstörung) gegenüber dem Arbeitgebenden vorzulegen wären. Die Pflicht, diese Daten dem Arbeitgebenden offenzulegen ergibt sich jedoch weder aus dem IfSG noch aus § 26 Abs.3 und Art. 9 Abs. 2 lit b DS-GVO, da hier lediglich die Verarbeitungsbefugnisse des Arbeitgebenden angesprochen sind, nicht aber eine Auskunftspflicht des/der Betroffenen.

Nach unserer Auffassung bleibt der/dem Beschäftigten in jedem Fall die Möglichkeit, anstelle einer Auskunft gegenüber seinem Arbeitgeber die Entschädigung nach § 56 Abs. 5 Satz 4 IfSG selbst bei der zuständigen Behörde (hier: dem Regierungspräsidium) zu verlangen und (nur) der Behörde gegenüber die erforderlichen Angaben zu machen. Sein Arbeitgeber erfährt dabei weder seinen Impfstatus, noch weitere persönliche Angaben oder ob und in welchem Umfang eine Entschädigung gegenüber dem Beschäftigten gewährt wurde.

Das sehen die in Baden-Württemberg zuständigen Behörden allerdings anders und verneinen eine eigene Antragsbefugnis der/des Beschäftigten. Nach deren Auffassung muss der/die Beschäftigte zwar seinen Impfstatus, nicht aber die gegen eine Impfung sprechenden Gründe, wie beispielsweise Informationen über eine medizinische Gegenindikation, gegenüber dem Arbeitgebenden preisgeben. Insbesondere müsse eine Schwangerschaft nicht offengelegt werden. Die Regierungspräsidien forderten in diesen Fällen beim Arbeitgebenden ein ärztliches Attest an, in dem ohne Angabe von Gründen bestätigt wird, dass eine Impfung aus medizinischen Gründen nicht erfolgen konnte. Dieses Attest könne der Arbeitnehmende unter Angabe der Vorgangskennung auch direkt beim Regierungspräsidium einreichen. Solch unterschiedliche Auffassungen sind für Arbeitgebende wie Beschäftigte misslich, gesetzgeberische Klarheit könnte

hier helfen. Mittlerweile hat die Konferenz der Datenschutzbehörden der Länder und des Bundes (DSK) die Position des LfDI übernommen und bestätigt die Antragsmöglichkeit jeder/jedess Beschäftigten beim Regierungspräsidium.

Sollte eine/ein Beschäftigte_r zum Zwecke der Geltendmachung des Erstattungsanspruchs nach § 56 Abs. 5 S. 3 IfSG seinen Impfstatus gegenüber dem Arbeitgebenden offenlegen, so kann dies ausschließlich nach Maßgabe einer Einwilligung nach DS-GVO erfolgen. Hierbei sind insbesondere an die Freiwilligkeit der Angabe des Impfstatus hohe Anforderungen zu stellen.

Unsere Dienststelle positionierte sich hierbei als erste Aufsichtsbehörde zu dieser bundesweit umstrittenen Rechtslage und verwies hierbei insbesondere auch auf eine strenge Zweckbindung.

Da viele Arbeitgebende, aber auch Beschäftigte, mit Blick auf die umstrittene Rechtslage im Bereich Lohnfortzahlung und Datenschutz verunsichert waren, haben wir hierzu ein Positionspapier veröffentlicht.

Wenn die personenbezogenen Daten für den Einzelfall der Auszahlung beziehungsweise Beantragung einer Lohnentschädigung verarbeitet werden, dürfen diese in keinem Fall dazu genutzt werden, etwaige innerbetriebliche Impfregister aufzubauen oder Impfquoten abzubilden. Vielmehr sind die personenbezogenen Daten nach der Verwendung zur Erlangung der Entschädigungszahlung unverzüglich zu löschen.

1.2 Vergessen, die Rechnung zu bezahlen?

Mittlerweile ist es fast zu unser aller alltäglichen Gewohnheit geworden: Wer in diesem Jahr Gaststätten, Freizeiteinrichtungen o. ä. besucht hat, wurde regelmäßig dazu aufgefordert, seine Kontaktdaten zu hinterlegen. Daher haben sich viele betroffene Personen im Rahmen von zahlreichen Beratungsanfragen mit der Frage an den LfDI gewandt, was denn eigentlich mit ihren Daten bei den Unternehmen und Gaststätten passieren würde.

Zu klären war daher, welche konkreten Maßgaben verantwortliche Stellen in Zeiten der Corona-Pandemie beachten müssen, um die personenbezogenen Daten ihrer Kund_innen beziehungsweise Besucher_innen datenschutzgerecht zu verarbeiten. Die Erhebung und Speicherung personenbezogener Daten zur Nachverfolgung von Infektionswegen des Covid-19-Erregers gemäß §§ 16 und 25 des IfSG i. V. m. § 8 Abs. 1 der Corona-Verordnung (Stand: 24. November 2021) soll es den Gesundheitsbehörden ermöglichen, Infektionswege zurückzuverfolgen. Ausschließlich für diesen spezifischen dürfen die Kontakt- und Anwesenheitsdaten von den Gesundheitsbehörden genutzt werden.

Innerhalb des Berichtszeitraumes gingen bei uns zudem auch zahlreiche Beschwerden ein, aus denen hervorging, dass Datenverarbeitungen teilweise für andere beziehungsweise eigene Zwecke erfolgten. Beispielsweise wurde in einem Fall die Telefonnummer eines Gastes durch einen Restaurantmitarbeitenden zweckentfremdet dafür genutzt, den Gast nach seinem Besuch anzurufen, um die Begleichung einer ausstehenden Rechnung einzufordern. In einem weiteren Fall wurde uns berichtet, dass ein Betreiber eines Kinos ebenfalls die Telefonnummer aus der Kontaktnachverfolgung verwendet hatte, um den Gast nach einer schlechten Online-Bewertung persönlich am Telefon im Anschluss an die der Kinovorstellung zur Rede zu stellen.

Diese und die Vielzahl anderer vergleichbarer Fälle machen deutlich, dass es bei einigen verantwortlichen Stellen offenbar noch immer Unklarheiten hinsichtlich der Verwendung der gem. §§ 16 und 25 IfSG i. V. m. § 8 Abs. 1 CoronaVO erhobenen personenbezogenen Daten und der daraus resultierenden starken Zweckbindung gibt. Grundsätzlich dürfen im Rahmen dieser Vorschriften folgende Daten erhoben werden: Vor- und Nachname, Anschrift,

>> Mehr Informationen:

Positionspapier des LfDI „Lohnfortzahlung, Corona und Datenschutz" vom 30.9.21: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/Positionspapier_Lohnfortzahlung_Rechtslage.pdf

Stellungnahme der DSK vom 20.12.21: https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_dsk_anwendungshilfe.pdf <<

eine sichere Kontaktinformation (Telefonnummer oder E-Mail-Adresse) sowie der Zeitraum, in der sich jeweils eine Person pro Hausstand in den spezifischen Räumlichkeiten aufgehalten hat. Diese Daten müssen vom Verantwortlichen über einen Zeitraum von vier Wochen aufbewahrt und nach Ablauf dieser Aufbewahrungsfrist datenschutzgerecht vernichtet werden. Ein handelsüblicher Aktenvernichter mit Sicherheitsstufe 3/4 (nach DIN 66399) ist hierfür ausreichend. Elektronisch erhobene Daten müssen ebenso dauerhaft gelöscht werden. Bei der Erhebung und Speicherung ist stets unbedingt darauf zu achten, dass die Daten so aufbewahrt werden, dass unbefugte Personen (z. B. andere Gäste) auf die Daten weder zugreifen noch diese einsehen können. Ausgefüllte Papierformulare dürfen daher nicht offen einsehbar herumliegen und sollten am Ende eines jeden Arbeitstages sicher verschlossen aufbewahrt werden. Erfreulicherweise konnten wir einen starken Rückgang der Anzahl an Beschwerden über die Verwendung von fortlaufenden Listen bei unserer Behörde in diesem Jahr feststellen.

Die Daten dürfen ausschließlich auf Anforderung der Gesundheitsbehörden oder der Ortspolizeibehörde zur Nachverfolgung möglicher Infektionsketten weitergeben werden. Sämtliche darüber hinaus gehende Verarbeitungen (z. B. für eigene Zwecke wie Werbung etc.) sind datenschutzrechtlich unzulässig.

Verantwortliche Stellen sollten daher von der Verwendung der im Rahmen der Kontaktnachverfolgung erhobenen Daten für andere als in § 8 Abs. 1 CoronaVO bestimmte Zwecke absehen.

1.3 SORMAS: 2021 immer noch kein Erfolgsmodell

Angesichts der weiterhin massiven Herausforderungen durch das SARS-CoV-2-Virus sind nach wie vor, möglicherweise mehr denn je, kluge und effiziente Verfahren gefragt, die den Stellen des öffentlichen Gesundheitswesens die Arbeit erleichtern. Dabei auch auf eine weitere Digitalisierung von Abläufen bei den Gesundheitsämtern zu setzen, liegt auf der Hand. Zur Vermeidung von Wiederholungen dazu verweisen wir auf unseren Beitrag Nummer 1.6 „Die Digitalisierung des (öffentlichen) Gesundheitswesens zur Pandemiebekämpfung“ im 36. Datenschutz-Tätigkeitsbericht 2020.

Eines der bedeutenden Projekte dabei ist das elektronische Verfahren SORMAS („Surveillance Outbreak Response Management and Analysis System“) zur Vereinfachung und Verbesserung der Kontaktnachverfolgung. Bereits 2020 haben wir uns intensiv um die datenschutzrechtlichen Aspekte dieses Projekts gekümmert. Wegen der Einzelheiten verweisen wir auf den Abschnitt „Die Software SORMAS des Helmholtz-Instituts zur Kontaktnachverfolgung“ im oben genannten Beitrag Nummer 1.6 des 36. Datenschutz-Tätigkeitsberichts.

Unsere Erwartung, dass den darin geschilderten Problemen (u. a.: unvollständige Informationen seitens der Projektbetreibenden, von dort nicht oder erst auf Nachfrage gelieferte, und dann teilweise doch nicht brauchbare Dokumente) 2021 rasch ein Ende gesetzt und die datenschutzrechtliche Beurteilung abgeschlossen werden könnte, wurde leider enttäuscht. Zahlreiche Dokumente sind zwar umfangreich, enthalten oft aber nur Mustertexte, die an den entscheidenden Stellen auf Ergänzung der spezifischen Inhalte für dieses Projekt warten. Ebenso ist bei zahlreichen abgefragten Daten unklar, ob diese notwendig sind und somit auf einer soliden rechtlichen Basis verarbeitet werden. Auch im Bereich der IT-Sicherheit sind einige Fragestellungen offen, und der Anbieter sollte dort dringend nacharbeiten.

Daher ließ sich auch 2021 eine Klärung aller datenschutzrechtlichen Fragen nicht erzielen; trotz des weiterhin sehr arbeitsintensiven Einsatzes unserer Behörde, etwa bei der Beratung des Helmholtz-Zentrums für Infektionsforschung (HZI) in Braunschweig, in schriftlicher Korrespondenz, in Einzelgesprächen sowie in Telefonkonferenzen der ins Leben gerufenen SORMAS-Arbeitsgruppe (ein Forum unter Beteiligung des HZI und anderer Akteure auf Projektträgerseite, des Bundesministeriums für Gesundheit, des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie einiger Landesdatenschutzbehörden).

>> Mehr Informationen:

36. Datenschutz-Tätigkeitsbericht 2020 des LfDI: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/02/LfDI-BW_36_Tätigkeitsbericht_2020_WEB.pdf <<

Eine dieser anderen Landesdatenschutzbehörden ist angesichts des eher zähen Fortgangs inzwischen aus der SORMAS-Arbeitsgruppe ausgestiegen. Dieser Ausstieg ist für uns nachvollziehbar, auch unter Berücksichtigung der Notwendigkeit, dass natürlich auch Datenschutzbehörden das Gebot der Verfahrensökonomie beachten. Nach sorgfältiger Abwägung haben wir uns entschieden, dieses Forum der Beratung zunächst nicht zu verlassen und diesem Ansatz eine letzte Chance zu geben.

Angesichts der offenbar gewordenen Misere haben wir, auch im Schulterschluss mit anderen beteiligten Datenschutzbehörden, nun aber, bei allem gebührenden Respekt gegenüber den Gesprächspartner_innen auf Seiten der Projektbetreibenden, dann doch auch sehr deutliche Worte geäußert. Etwa mit der Frage, ob es dort möglicherweise auch ein Kapazitäts- und Kompetenzproblem geben könnte. Man hat sich diese Worte wohl zu Herzen genommen. Im Dezember 2021 haben wir jedenfalls erfahren, dass sich auf Seiten der Projektbetreibende zusätzliches Personal mit datenschutzrechtlichen Aspekten befassen soll. Wir rechnen damit, dass bis spätestens Ende März 2022 entscheidende Verbesserungen und Ergebnisse erreicht sind. Parallel dazu setzen wir auf die bewährte weitere Zusammenarbeit mit dem Sozialministerium Baden-Württemberg. Dabei geht es u. a. um die Frage, welche Gesundheitsämter in Baden-Württemberg nach den Vorstellungen des Sozialministeriums als deren oberster Aufsichtsbehörde auf der Grundlage auch nicht datenschutzrechtlicher, etwa epidemiologischer, politischer oder ökonomischer Vorschriften und Erwägungen, das Verfahren SORMAS bereits einsetzen und eventuell künftig einsetzen dürfen, sollen oder müssen. Nach den Informationen, die wir vom Sozialministerium dazu erhalten haben, scheint die Zahl der baden-württembergischen Gesundheitsämter, die SORMAS auf die eine oder andere Weise nutzen, recht überschaubar. Auch der Landkreistag Baden-Württemberg hat auf unsere Bitte wertvolle Informationen zum Einsatz von SORMAS bei Landratsämtern zukommen lassen.

© Heiko Küverling – stock.adobe.com

Für Bürger_innen keine gute Nachricht: Zahlreiche Testzentren hatten ein Datenschutzproblem.

Pandemiebedingt sind die Möglichkeiten unserer Behörde, sich in einzelnen Gesundheitsämtern einen unmittelbaren Eindruck von den dortigen Verhältnissen mit Blick auf SORMAS zu verschaffen, stark eingeschränkt. Wir gehen davon aus, dass wir 2022 dennoch die notwendigen Informationen gewinnen, um bei Bedarf dann auch gezielt Rat erteilen und Kontrolle ausüben zu können.

1.4 Datenschutz in Corona-Testzentren

Als bedeutendes Mittel zur Bekämpfung der Ausbreitung der Coronavirus-Krankheit-2019 (COVID-19) wurde schon seit geraumer Zeit das Testen genannt.

Das Bundesministerium für Gesundheit hat mit seiner Verordnung zum Anspruch auf Testung in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 (Coronavirus-Testverordnung – TestV) vom 8. März 2021 die so genannte Bürgertestung eingeführt. Danach erhielten asymptomatische Personen einen Anspruch auf Testung mittels PoC-Antigen-Tests, wobei solche Testungen im Rahmen der Verfügbarkeit von Testkapazitäten mindestens einmal pro Woche in Anspruch genommen werden konnten. (Diese Tests waren für die Bürger_innen zunächst kostenlos, ab dem 11. Oktober 2021 mussten sie solche Tests vorübergehend selbst bezahlen, im November wurde die ursprüngliche Regelung wieder eingeführt).

Diese Regelungen fanden, wohl ganz im Sinne der dahinter stehenden Strategie zur Pandemiebekämpfung, große Resonanz. Nicht nur bei

Menschen, die sich testen lassen wollten, sondern auch bei Unternehmern oder sonstigen Interessierten, die solche Tests anbieten wollten. Auch in Baden-Württemberg entstand rasch eine beeindruckende Testinfrastruktur mit einer Vielzahl neu eingerichteter Testzentren (zeitweise konnte man den Eindruck gewinnen, dass Testzentren „wie Pilze aus dem Boden schießen"), beispielsweise in rasch aufgestellten Zelten an zentralen Orten von Städten und Gemeinden. Die mit der genannten Verordnung sowie mit der „Allgemeinverfügung des Ministeriums für Soziales und Integration Baden-Württemberg" vom 12. März 2021, „Beauftragung zur Durchführung von Bürgertestungen nach § 4a der Verordnung zum Anspruch auf Testungen in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 des Bundesministeriums für Gesundheit (TestV) vom 8. März 2021" gesetzten Hürden für Errichtung und Betrieb der entsprechenden Testzentren waren relativ niedrig, die Modalitäten der Abrechnung für deren Betreibende in ökonomischer Hinsicht offenbar recht attraktiv (erst im Juli 2021 hat das Bundesministerium für Gesundheit die ökonomischen Rahmenbedingungen geändert, u. a. durch Einführung von Regelungen zur Abrechnungsprüfung). Dies führte nicht nur dazu, dass, wie in der Presse immer wieder berichtet, Unregelmäßigkeiten bei der Abrechnung auffielen und auch strafrechtlich verfolgt wurden. Auch eine Vielzahl teilweise gravierender Datenschutzprobleme war zu beklagen.

Testzentren wurden (und werden) nicht nur von Ärzt_innen, Apotheker_innen, Organisationen des Rettungsdienstwesens und anderen Akteur_innen betrieben, die in vergleichbarer Weise mit datenschutzrechtlichen Anforderungen bei der Verarbeitung personenbezogener Daten, einschließlich besonders sensibler Gesundheitsdaten, typischerweise in hohem Maß vertraut sind. Auch Unternehmer, die sich zuvor, und leider auch bei Gründung ihrer Testzentren, mit solchen Anforderungen nicht oder nur in geringem Maß befasst hatten, haben kurzfristig solche Testzentren eröffnet. Getragen, wie es scheint, teilweise vor allem auch von einer Art „Goldgräberstimmung", nicht von dem Willen, auch datenschutzrechtlichen Anforderungen oder den Grundsätzen der IT-Sicherheit gerecht zu werden.

Für besondere Probleme sorgte etwa der Einsatz elektronischer Anwendungen. Viele der Testzentren boten Getesteten den Service, das Testergebnis über Apps, per SMS oder E-Mail direkt auf das Handy zu schicken. Die bei der Verwendung solcher Anwendungen notwendigen Maßnahmen des technischen und organisatorischen Datenschutzes waren leider in vielen Fällen mangelhaft, zum Teil mit der Folge, dass Testergebnisse offen im Internet von Unbefugten abgerufen werden konnten. Wir haben frühzeitig auf diese Probleme hingewiesen und den verantwortlichen Stellen empfohlen, sofort sorgsam zu überprüfen, ob sie die angemessene Sicherheit der Gesundheitsdaten Getesteter durch technisch-organisatorische Maßnahmen jederzeit gewährleisten können.

Da uns leider weiterhin massive Probleme bekannt wurden, haben wir uns erneut an die Öffentlichkeit gewandt und die zu beachtenden Anforderungen beispielhaft konkretisiert, etwa hinsichtlich des Schutzes für über das Internet bereitgestellte Tes-

>> Mehr Informationen:

„Faktenpapier Testen" des Bundesministeriums für Gesundheit „Testen, testen, testen" – aber gezielt" vom 17.4.2020 https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/C/Coronavirus/Faktenpapier_Testen.PDF

Beauftragung zur Durchführung von Bürgertestungen nach § 4a der Verordnung zum Anspruch auf Testungen in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 des Bundesministeriums für Gesundheit (TestV) vom 8.3.2021: https://sozialministerium.baden-wuerttemberg.de/fileadmin/redaktion/m-sm/intern/downloads/Downloads_Gesundheitsschutz/Corona_SM_AV-Anbieter-Buergertestung_210312.pdf

Testzentren: LfDI empfiehlt dringend, Sicherheitsvorkehrungen bei der Datenverarbeitung zu überprüfen, vom 25.5.2021: https://www.baden-wuerttemberg.datenschutz.de/testzentren-lfdi-empfiehlt-dringend-sicherheitsvorkehrungen-bei-der-datenverarbeitung-zu-ueberpruefen/

Pandemie-Bekämpfung: Datenschutz in Testzentren, vom 2.6.21: https://www.baden-wuerttemberg.datenschutz.de/pandemie-bekaempfung-datenschutz-in-testzentren/ <<

tergebnisse. (Im weiteren Verlauf wurde bundesweit das Thema diskutiert und die massiven Sicherheitsrisiken für die Bürger_innen erkennbar und fassbar.)

Um die vielfältigen Aspekte dieser Problematik auch in ihrer Vereinzelung zu würdigen – wir betrachten stets auch Einzelfälle – hier zur Übersicht weitere von uns bearbeitete Datenpannen (im Sinne des Artikels 33 Absatz 1 DS-GVO in Verbindung mit Artikel 4 Nummer 12 DS-GVO) bei Testzentren: Testergebnisse waren für Unbefugte einsehbar. Der E-Mail-Versand ging an die falsche Adresse. Die Kasse eines Schnelltestzentrums, in welcher u. a. die Testergebnisse aufbewahrt wurden, wurde entwendet. Es wurden fehlerhafte „Ausweise" ausgestellt aufgrund einer falschen Excel-Tabelle. Das Vertauschen von Testergebnissen wurde festgestellt. Die Bescheinigung eines Corona-Tests-Ergebnisses wurde an den falschen Empfänger ausgehändigt. Bei der Bearbeitung solcher Datenpannen haben wir insbesondere bei Bedarf auf die Verbesserung der technischen und organisatorischen Maßnahmen sowie auf die Erfüllung der Benachrichtigungspflicht nach Artikel 34 DS-GVO hingewirkt und die verantwortlichen Stellen beraten, wie die Benachrichtigung bei einer großen Anzahl von Betroffenen umgesetzt werden kann, beispielsweise durch öffentliche Bekanntmachung. Zudem sahen wir uns immer wieder veranlasst, darauf hinzuweisen, dass bereits eine Terminbestätigung ein Gesundheitsdatum im Sinne des Artikels 4 Nummer 15 DS-GVO darstellt. Für die Übermittlung des Testergebnisses haben wir wiederholt empfohlen, soweit die Betroffenen insoweit freiwillig und informiert einwilligen, die Corona-Warn-App des Robert-Koch-Instituts als einen sicheren Übertragungsweg zu nutzen (siehe Infokasten).

Ein weit verbreitetes Problem waren die bei vielen Testzentren fehlenden oder mangelnden Informationen nach Artikel 13 DS-GVO, so dass für viele Menschen, die sich testen lassen wollten und gegebenenfalls getestet wurden, unklar war, wer für die Verarbeitung ihrer personenbezogener Daten überhaupt verantwortlich ist und an wen sie sich demnach wenden können, wenn sie beispielsweise von ihren jeweiligen Datenschutzrechten Gebrauch machen wollten, etwa von ihrem Recht auf Auskunft nach Artikel 15 DS-GVO oder ihrem Recht auf Löschung nach Artikel 17 DS-GVO. Die Frage nach dem Verantwortlichen klingt einfach, sie ist

INFOKASTEN

Artikel 33 Absatz 1 DS-GVO ordnet an:

„Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen."

Nach Artikel 4 Nummer 12 DS-GVO ist eine

„Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, 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."

Artikel 34 Absatz 1 DS-GVO bestimmt:

„Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung."

Nach Artikel 4 Nummer 15 DS-GVO sind

„Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

es aber nicht – ein bestimmter Arzt, ein bestimmter Ortsverband einer Rettungsdienstorganisation, ein bestimmter Kreisverband einer solchen Organisation, die Kassenärztliche Vereinigung Baden-Württemberg, eine Kommune, mehr als ein Akteur in gemeinsamer Verantwortung im Sinne des Artikels 26 DS-GVO, gegebenenfalls mit welcher Aufteilung datenschutzrechtlich bedeutsamer Pflichten untereinander?

Dieses Problem zeigte sich leider auch bei Akteuren, die typischerweise im Umgang mit Gesundheitsdaten und anderen personenbezogenen Daten versiert sind und sein müssen. Angesichts der für meine Behörde unübersehbaren Vielzahl von Testzentren in Baden-Württemberg konnte sich meine Behörde nur punktuell mit diesem Problem befassen.

Bemerkenswert ist, dass sich in den Jahren seit dem Wirksamwerden der DS-GVO am 25. Mai 2018 immer noch nicht die Selbstverständlichkeit herumgesprochen hat, dass ein fairer und sauberer Umgang mit personenbezogenen Daten u. a. rechtzeitige und vollständige Informationen nach Artikel 13 DS-GVO voraussetzt, u. a. über den Namen und die Kontaktdaten des Verantwortlichen, wie von Artikel 13 Absatz 1 Buchstabe a DS-GVO ausdrücklich angeordnet. Meine Behörde wird sich damit weiter befassen. Wir werden dabei auch die weitere Zusammenarbeit mit bewährten und wirkungsmächtigen Akteur_innen des baden-württembergischen Gesundheitswesens suchen, etwa mit den zuständigen Kammern, der Kassenärztlichen Vereinigung Baden-Württemberg und den einschlägigen Berufsverbänden (siehe Infokasten Seite 33).

Eine immer wieder gestellte Frage war die nach der Dauer, für die in solchen Testzentren angefallene personenbezogene Daten aufbewahrt werden dürfen oder müssen. Nachdem die oben genannte Coronavirus-Testverordnung vom 8. März 2021 dazu noch keine ausdrücklichen Regelungen enthalten hatte, hat das Bundesministerium für Gesundheit im Juli 2021 insofern für eine gewisse Klarheit gesorgt. Nach § 7 Absatz 5 der Coronavirus-Testverordnung in der am 11. Oktober 2021 in Kraft getretenen Fassung gilt:

„*Die nach § 6 Absatz 1 berechtigten Leistungserbringer und die sonstigen abrechnenden Stellen haben die nach Absatz 4 in Verbindung mit Absatz 6 Nummer 1 zu dokumentierenden Angaben und die für den Nachweis der korrekten Durchführung und Abrechnung notwendige Auftrags- und Leistungsdokumentation bis zum 31. Dezember 2024 unverändert zu speichern oder aufzubewahren. Zur Auftrags- und Leistungsdokumentation zählen soweit erforderlich insbesondere*

1. *bei nach § 6 Absatz 1 Nummer 2 beauftragten Leistungserbringern der Nachweis der Beauftragung,*

2. *bei Leistungen nach § 4a die Öffnungszeiten des Leistungserbringers je Tag und die Anzahl der Tests durchführenden Personen je Tag,*

3. *bei der Abrechnung von Leistungen nach § 12 Absatz 3 das einrichtungs- oder unternehmensbezogene Testkonzept und für jede abgerechnete Leistung die Unterschrift der die Testung durchführenden Person,*

4. *bei der Abrechnung von Sachkosten nach § 11 der Kaufvertrag oder die Rechnung oder bei unentgeltlicher Bereitstellung einen Nachweis des Bezugs,*

5. *für jede durchgeführte Testung der Vorname, der Familienname, das Geburtsdatum und die Anschrift der getesteten Person, die Art der Leistung, der Testgrund nach den §§ 2 bis 4b, der Tag, die Uhrzeit, das Ergebnis der Testung und der Mitteilungsweg an die getestete Person,*

6. *bei Durchführung eines PoC-Antigen-Tests oder eines Antigen-Tests zur Eigenanwendung die individuelle Test-ID gemäß der Marktübersicht des Bundesamtes für Arzneimittel und Medizinprodukte nach § 1 Absatz 1 Satz 6,*

7. *bei einem positiven Testergebnis ein Nachweis der Meldung an das zuständige Gesundheitsamt,*

8. *die schriftliche oder elektronische Bestätigung der getesteten Person oder ihres gesetzlichen Vertreters über die Durchführung des Tests.*

Das Nähere zur Auftrags- und Leistungsdokumentation, insbesondere von welchen einzelnen Angaben nach Satz 2 Nummer 1 bis 8 in den jeweiligen Fällen ganz oder teilweise abgesehen werden kann, regelt die Kassenärztliche Bundesvereinigung in ihren Vor-

INFOKASTEN

Artikel 13 DS-GVO ordnet an:

(1) Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

a) den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
b) gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
c) die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
d) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
e) gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
f) gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.

(2) Zusätzlich zu den Informationen gemäß Absatz 1 stellt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten folgende weitere Informationen zur Verfügung, die notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten:

a) die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
b) das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
c) wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
d) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
e) ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
f) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(3) Beabsichtigt der Verantwortliche, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die personenbezogenen Daten erhoben wurden, so stellt er der betroffenen Person vor dieser Weiterverarbeitung Informationen über diesen anderen Zweck und alle anderen maßgeblichen Informationen gemäß Absatz 2 zur Verfügung.

(4) Die Absätze 1, 2 und 3 finden keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt.

gaben nach Absatz 6 Nummer 1. Das Ergebnis der Testung nach Satz 2 Nummer 5 und der Nachweis nach Satz 2 Nummer 7 sind abweichend von Satz 1 bis zum 31. Dezember 2022 unverändert zu speichern oder aufzubewahren."

Damit scheint derzeit klar geregelt, wie lange die genannten Unterlagen zu speichern oder aufzubewahren sind. Allerdings stellt sich die Frage, welche Aufbewahrungsfristen gelten, wenn die soeben zitierten Regelungen des § 7 Absatz 5 der Coronavirus-Testverordnung, wie von deren § 19 Absatz 1 vorgesehen, am 31. März 2022 außer Kraft getreten sein werden. Wir gehen davon aus, dass insofern das Bundesministerium für Gesundheit, unter Umständen etwa auch im Kontakt mit dem Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg oder auch mit dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, für Klärung sorgen kann, beispielsweise durch entsprechende Überarbeitung der Coronavirus-Testverordnung.

1.5 Datenschutz in Corona-Impfzentren

Ende des Jahres 2020 galt es für das Sozialministerium, im Lande Impfzentren zu errichten, um eine möglichst rasche Impfung gegen das Virus SARS-Cov-2 nach den Priorisierungsvorgaben der seinerzeit gültigen Coronavirus-Impfverordnung zu ermöglichen. Unsere Behörde war gefragt, das Sozialministerium zu der Fülle der sich dabei ergebenden datenschutzrechtlichen Fragestellungen schnellstmöglich zu beraten. Einige der zuvor mit Blick auf Corona-Testzentren dargestellten Datenschutzprobleme gab es bei den vom sodann 27. Dezember 2020 bis zum 30. September 2021 betriebenen Impfzentren in Baden-Württemberg erfreulicherweise nicht. Das ist u. a. darauf zurückzuführen, dass schon vor Betriebsbeginn klar war, dass es hier landesweit nur einen einzigen datenschutzrechtlich Verantwortlichen (im Sinne des Artikels 4 Nummer 7 DS-GVO) gibt: das Sozialministerium Baden-Württemberg.

Somit hatten wir von Anfang an in Gestalt des Ministeriums einen zentralen und kompetenten Ansprechpartner zur Erörterung und Klärung der beachtlichen Anzahl einzelner Datenschutzfragen, die mit der Errichtung und dem Betrieb der komplexen Struktur baden-württembergischer Impfzentren verbunden waren.

Ein kleiner Wermutstropfen dabei war, dass sich das Sozialministerium erst kurz vor Weihnachten 2020 mit der Bitte um Beratung an uns gewandt hat. Daher musste innerhalb der somit verbliebenen knappen Zeitpanne bis zum Betriebsbeginn der ersten Impfzentren am 27. Dezember 2020 unter Hochdruck und mit „Mut zur Lücke" an der Klärung bestimmter Fragen gearbeitet werden, zuletzt noch an Heiligabend und den Weihnachtsfeiertagen. Gegenstand der Erörterungen waren u. a. die Fragen, ob und in welcher Form und auf welcher Rechtsgrundlage eine Qualitätssicherung bei den Gesprächen zur telefonischen Terminvereinbarung stattfinden solle (hier entschied sich das Sozialministerium aufgrund unserer Beratung zu einer Aufzeichnung und Kontrolle von Gesprächen ausschließlich auf Basis von Einwilligungen), welche Daten wie und auf welcher Rechtsgrundlage zur Terminvereinbarung, zur Durchführung der Impfung und zu deren Dokumentation, zum Impfquotenmonitoring und im Rahmen der Impfsurveillance verarbeitet werden, wie die Betroffenen über die Datenverarbeitungen gemäß Artikel 13 und ggf. Artikel 14 DS-GVO informiert werden und welche datenschutzrechtlich relevanten Verträge (etwa zur Auftragsdatenverarbeitung) durch wen abzuschließen seien.

Zur Vermeidung eventueller Missverständnisse: Wir scheuen vor engagierter Arbeit keineswegs zurück. Aber diese besondere Belastung des ohnehin stark geforderten Personals beim Sozialministerium und anderswo wäre möglicherweise durch rechtzeitige Vorbereitung vermeidbar gewesen. Wir hatten

INFOKASTEN

Nach Artikel 4 Nummer 7 DS-GVO ist „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

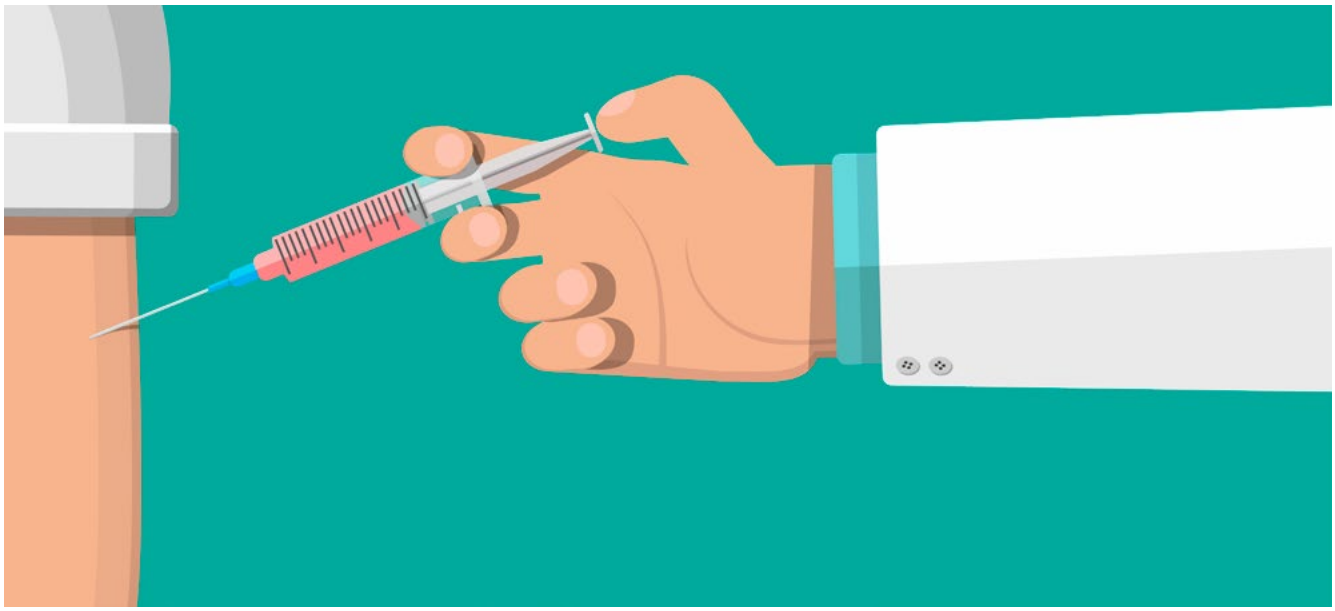
uns jedenfalls bereits im November 2020 mit dem Angebot an das Sozialministerium gewandt, es bezüglich der datenschutzrechtlichen Fragen im Zusammenhang mit der Einrichtung der Impfzentren zu beraten und zu unterstützen.

Ganz grundlegende Fragen, etwa nach der datenschutzrechtlichen Verantwortung, den Rechtsgrundlagen, den nach Artikel 13 DS-GVO anzubietenden Informationen sowie nach bestimmten Anforderungen des technischen und organisatorischen Datenschutzes, konnten rechtzeitig vor Betriebsbeginn geklärt werden.

Einige Problemstellungen, etwa die Abgrenzung der datenschutzrechtlichen Verantwortungssphäre des Sozialministeriums einerseits und der Kassenärztlichen Bundesvereinigung andererseits (nämlich mit Blick auf die Interessierten für die telefonische Buchung von Impfterminen eröffnete Möglichkeit, die „116117-Dienste“ der Kassenärztlichen Bundesvereinigung zu nutzen, und die Möglichkeit, eine solche Buchung über eine von der Kassenärztlichen Bundesvereinigung betriebene Homepage vorzunehmen, von der aus in die Systeme des Landes verwiesen wurde) sowie nach der Erfüllung aller datenschutzrechtlichen Anforderungen hinsichtlich einer Auftragsverarbeitung (im Sinne des Artikels 28 DS-GVO), etwa von bestimmten baden-württembergischen Kommunen und Kreisen für das Sozialministerium, konnten zwar angesprochen, aber leider nicht mehr rechtzeitig vor Betriebsbeginn abgearbeitet werden.

Zur Klarstellung sei anmerkt: Bei verständiger Würdigung der auch von Fachleuten immer wieder betonten überragenden Bedeutung des Impfens bei der Pandemiebekämpfung einerseits sowie der vergleichsweise untergeordneten Bedeutung der bei Betriebsbeginn ungeklärten datenschutzrechtlichen Fragen andererseits standen diese datenschutzrechtlichen Defizite dem Betrieb der Impfzentren unseres Erachtens nicht entgegen. Wir haben allerdings darauf hingewiesen, dass diese Defizite zumindest im weiteren Verlauf aufzulösen sind.

Es kam, wie nicht anders zu erwarten, auch beim Betrieb der Impfzentren zu einigen Datenpannen. Diese hatten, nach den Datenpannenmeldungen, die wir erhalten haben, u. a. den Versand von E-Mails an eine Vielzahl (in einem Fall beispielsweise mehr als 800) von Adressat_innen mit so genanntem offenen Verteiler zum Gegenstand. Zumindest hatten diese E-Mails keine höchst sensiblen Inhalte, etwa mit Angaben über individuelle Nebenwirkungen einzelner geimpfter Menschen. Sie betrafen „nur“, dies ist aber schlecht genug, allgemeine Informationen zum Registrierungsprozedere und zur Terminkoordinierung, eine Umfrage zum Impfstoff sowie eine Terminverschiebung. Es ist für uns ohne Weiteres nachvollziehbar, dass



© Grafik_absent84 – stock.adobe.com

Nicht nur Testzentren, sondern auch Impfzentren haben es mit dem Datenschutz nicht ganz so genau genommen.

sich eine nicht unerhebliche Anzahl insofern Betroffener auch mit Beschwerden (vgl. Artikel 77 DS-GVO) an uns gewandt hat. Ebenso nachvollziehbar erscheint es, dass sich einige Beschwerdeführer verärgert geäußert haben. Schließlich gehört es mittlerweile zum kleinen Einmaleins des Datenschutzes, beim Versand von E-Mails an mehr als eine Adressatin oder einen Adressaten, bei Bedarf den offenen Verteiler zu vermeiden und mit dem Instrument „bcc" (die Abkürzung für „blind carbon copy") zu arbeiten: Alle Empfänger_innen, die im Header einer E-Mail unter „bcc" eingetragen sind, erhalten eine so genannte Blindkopie; keine_r von ihnen kann erkennen, an wen die jeweilige E-Mail sonst noch versandt wurde. Wenn wir die Zahl der uns gemeldeten derartigen Datenpannen mit der für uns kaum schätzbaren Vielzahl insgesamt von baden-württembergischen Impfzentren versandten E-Mails ins Verhältnis setze, erkennen wir, dass insofern wohl ganz überwiegend korrekt gearbeitet worden ist.

Eine weitere Datenpanne hatte den Versand von Impfzertifikaten in einem Sammelumschlag nach mobilem Impfen an den falschen Empfänger zum Gegenstand. In verschiedenen Zusammenhängen, etwa auch mit Blick auf die Corona-Testzentren, haben wir auf die herausragende Bedeutung der Informationen nach Artikel 13 DS-GVO hingewiesen, insbesondere auch hinsichtlich der Namen und Kontaktdaten des Verantwortlichen. Der Text dieser Informationen wurde zwar bereits im Dezember 2020 zwischen dem Sozialministerium und uns sorgfältig abgestimmt. Danach wurde allerdings mehrfach deutlich, dass dieser Text, auch für mit der Materie und Verwaltungsangelegenheiten vertraute Menschen, erst Recht für insofern Außenstehende und Ungeübte, im Internet sowie in der „realen Welt" sehr schwer und im Ergebnis manchmal gar nicht zu finden war. Da fragte sich der eine oder die andere: Was nützt der schönste Text, wenn man ihn sich als interessierter Mensch in typischen Situationen nicht mit zumutbarem Aufwand vor Augen führen kann? Wir gehen davon aus, dass diese Probleme in künftigen vergleichbaren Situationen mit einfachen Mitteln vermieden werden können, etwa durch hinlänglich deutliche Platzierung des anzubietenden Textes im Internetangebot sowie durch Aushängen und / oder Auslegen entsprechender Dokumente im Eingangsbereich der jeweiligen Einrichtungen. Nach mehrmaligem Nachhaken unsererseits hat das Sozialministerium jedenfalls auch im Fall der Impfzentren die Datenschutzinformationen in das Internet gestellt. Ein Blick hierauf lohnt sich nicht nur für diejenigen, die sich ein Bild von der Verarbeitung der Daten in den Impfzentren machen wollen, sondern auch für Verantwortliche, die ihrerseits Datenschutzinformationen erstellen müssen, kann die Lektüre dieses Beispiels durchaus sinnvoll sein.

>> Mehr Informationen:

Datenschutzinformationen Impfzentren:
https://sozialministerium.baden-wuerttemberg.de/fileadmin/redaktion/m-sm/intern/downloads/Downloads_Gesundheitsschutz/Corona_SM_Information_Datenschutz_Termin_Impfung.pdf <<

1.6 Apotheken in der Corona-Pandemie: Schutzmasken, Corona-Tests und COVID-19-Impfzertifikate

Auch die Apotheken wurden in unterschiedlicher Weise in die Bewältigung der Corona-Pandemie einbezogen. Sie haben insbesondere Schutzmasken gemäß der Coronavirus-Schutzmasken-Verordnung kostenfrei beziehungsweise kostengünstig an den berechtigten Personenkreis ausgegeben, sie führten und führen Corona-Tests durch und stellen digitale COVID-19-Impfzertifikate aus. Mit allen diesen Tätigkeiten von Apotheken waren auch wir befasst. Darüber hinaus behandelten wir auch eine Beratungsanfrage in Bezug auf die Ausstellung von Ausweisen im Scheckkartenformat mit dem aufgedruckten QR-Code über das digitale Impfzertifikat durch Apotheken.

Ausgabe von Corona-Schutzmasken nach der Coronavirus-Schutzmasken-Verordnung

Nach der Coronavirus-Schutzmasken-Verordnung hatten verschiedene berechtigte Personengruppen längstens bis zum 15. April 2021 Anspruch auf eine bestimmte Anzahl von qualifizierten Schutzmasken (des Typs FFP 2 oder eines anderen im Anhang der Verordnung aufgelisteten Typs). Die Apotheken gaben diese Schutzmasken nach der Prüfung der Berechtigung im Rahmen ihrer jeweiligen Kapazitäten aus. Hier gab es wiederholt Schwierigkeiten bei der Prüfung der Anspruchsberechtigung durch

Apotheken. So wurde insbesondere bei der Personengruppe, bei der die Anspruchsberechtigung auf dem Lebensalter (über 60 Jahre) beruhte (§ 2 Absatz 1 Nummer 1 der Verordnung) und bei der die Abgabe nach dem Text der Verordnung ausschließlich gegen Vorlage des Personalausweises hätte erfolgen sollen (§ 4 Absatz 1 Satz 2 der Verordnung), die Geltendmachung des Anspruchs wiederholt von weiteren Voraussetzungen oder Bedingungen abhängig gemacht. Verschiedene Apotheken verlangten etwa, dass die Anspruchssteller_innen ihre Gesundheitskarte einlesen lassen müssten, eine Datenschutzerklärung unterschrieben oder sich zunächst als Kundin und Kunde bei der Apotheke registrierten. Oder die Apotheken fertigten statt einer bloßen Einsichtnahme in den Personalausweis eine Kopie von diesem an. Hier schritten wir ein.

Über die Bearbeitung von solchen Einzelfalleingaben hinaus haben wir uns deswegen auch an das Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg, die Landesapothekerkammer Baden-Württemberg (LAK) und den Landesapothekerverband Baden-Württemberg e.V. (LAV) mit der Bitte gewandt, im Rahmen ihrer Möglichkeiten durch sachgerechte Maßnahmen die datenschutzrechtskonforme Ausgabe der Schutzmasken sicherzustellen. Dazu gehörte der Hinweis, dass die Apotheken die Anspruchsberechtigten über die Verarbeitung personenbezogener Daten nach Maßgabe von Artikel 12-14 DS-GVO zu informieren haben. Insbesondere war unseres Erachtens die Anfertigung einer Kopie des Personalausweises weder zur Zweckerreichung (nämlich der Feststellung der Berechtigung des Anspruchsstellers oder der Dokumentation des Geschäftsvorfalls und Abrechnung) erforderlich noch lagen die Voraussetzungen aus § 20 Absatz 2 des Personalausweisgesetzes hierfür vor.

Durchführung von Corona-Tests durch Apotheken

Nach der Coronavirus-Testverordnung (zunächst vom 8. März 2021) konnten auch Apotheken kostenlose Bürger-Tests auf SARS-Cov-2 anbieten. Dabei ist es grundsätzlich auch unter Datenschutzgesichtspunkten begrüßenswert, wenn solche gesundheitsbezogenen Leistungen von Leistungserbringern angeboten werden, die Erfahrung im Umgang mit den nach der DS-GVO besonders zu schützenden Gesundheitsdaten haben und die einer gesetzlichen Pflicht zur Wahrung des Berufsgeheimnisses unterfallen (vgl. insbesondere Artikel 9 Absatz 2 Buchstabe i und Absatz 3 DS-GVO). Gleichwohl stellten sich auch hier einige Fragen – wie etwa die nach der Rechtsgrundlage für die Verarbeitung personenbezogener Daten und der Speicherdauer – die wir gemeinsam mit der LAK und dem LAV zu klären versuchten. Nachdem die Coronavirus-Testverordnung am 24. Juni 2021 auch mit unserer Unterstützung neu gefasst wurde, haben sich einige dieser Fragen – etwa auch zur Speicherdauer zu

© Andrea Tosi – stock.adobe.com

FFP2-Masken gab es für eine kurze Zeit kostenlos in der Apotheke – aber nur für bestimmte Personengruppen. Also musste die Apotheke kontrollieren, ob die Person, die kostenlos Masken haben wollte, auch anspruchsberechtigt war.

Dokumentations- und Abrechnungszwecken, für die es nunmehr in § 7 Absatz 5 der neu gefassten Coronavirus-Testverordnung eingehendere Regelungen gibt – überholt (wegen weiterer Einzelheiten hierzu empfehlen wir unseren Beitrag: „Datenschutz in Corona-Testzentren").

Ausstellung digitaler Impfzertifikate durch Apotheken

Die Apotheken stellen auch digitale Impfzertifikate (COVID-19-Impfzertifikate) nach § 22 Absatz 5 des Infektionsschutzgesetzes (IfSG) aus. Um ein digitales Impfzertifikat zu erhalten, muss die geimpfte Person nach dem Gesetzestext der Apotheke eine Impfdokumentation in Papierform, z. B. den gelben Impfpass, über eine Schutzimpfung gegen das Coronavirus SARS-CoV-2 vorlegen.

Die Apotheke hat dann „geeignete […] Maßnahmen zur Vermeidung der Ausstellung eines unrichtigen COVID-19-Impfzertifikats, insbesondere, um die Identität der geimpften Person und die Authentizität der Impfdokumentation nachzuprüfen," treffen. Aus der Begründung des zuständigen Bundestagsausschusses zu der Neuregelung des § 22 Absatz 5 IfSG ging hierzu hervor, dass die Überprüfung der vorgelegten Dokumentation, eine ordnungsgemäße Belehrung über die Konsequenzen der Vorlage einer unrichtigen Impfdokumentation und die Ausstellung des Impfzertifikates zu dokumentieren seien (vgl. Deutscher Bundestag Drucksache 19/29870, S. 32). Dies und verschiedene Äußerungen in der öffentlichen Diskussion hierzu führten möglicherweise zu einer gewissen Verunsicherung bei den Apotheken, so dass diese teilweise wohl von der Notwendigkeit ausgingen, personenbezogene Dokumentationen vorzunehmen, insbesondere Kopien von vorgelegten Unterlagen anzufertigen.

Daher sind wir nach der Einführung dieser Regelung im Juli 2021 an die LAK und den LAV herangetreten und haben unsere Rechtsauffassung mitgeteilt, dass die Apotheken für die Ausstellung des Impfzertifikats keine personenbezogenen Daten speichern dürften. Der gelbe Impfausweis sei vielmehr durch die Geimpften nach § 22 Absatz 5 Satz 2 IfSG nur vorzulegen. Daher genüge etwa eine bloße optisch-mechanische Prüfung durch die Apotheker_innen ohne weitere Speicherung oder personenbezogene Dokumentation. Auch die Bundesvereinigung deutscher Apothekerverbände e. V. (ABDA) vertrat in ihrer „Handlungshilfe zur nachträglichen Erstellung der COVID-19 Impfzertifikate durch Apotheker" vom 11. Juni 2021 die Auffassung, dass Apotheken insoweit keine personenbezogenen Daten zu speichern hätten. Der LAK und der LAV teilten unsere Rechtsauffassung, dass für die Nachprüfung des gelben Impfausweises allein eine „Sichtprüfung" zu erfolgen habe. Auch teilten die LAK und der LAV unsere Rechtsauffassung, dass nach § 22 Absatz 5 IfSG eine weitergehende personenbezogene Dokumentation nicht erforderlich und daher nicht zulässig sei. Soweit Apotheken für den Ausdruck pdf-Dateien mit den QR-Codes zum digitalen Impfzertifikat zwischenspeichern, seien sie gehalten, diese sogleich – auch etwa im Browsercache – zu löschen. Bei Anfragen und in Einzelfällen legen wir daher nunmehr diese mit der LAK und dem LAV abgestimmte Rechtsauffassung zugrunde. Durch die fundierte inhaltliche Prüfung der rechtlichen Grundlagen konnten wir somit Klarheit sowohl für die Apotheken als auch für die Bürger_innen schaffen. Davon profitieren alle Beteiligten, schließlich auch wir, die nun fortan auch davon ausgehen können, dass es künftig zu weniger Datenschutzverstößen in diesem Bereich kommt. Das hoffen wir zumindest.

Zur Ausstellung des Zertifikats müssen die Apotheken nach § 22 Absatz 2 Satz 1, Absatz 4, Absatz 5 Satz 3 IfSG einen bestimmen Satz personenbezogener Daten (u. a. das Datum der Schutzimpfung, die Bezeichnung des Impfstoffes, Name der Krankheit, gegen die geimpft wurde, Name der geimpften Person und deren Geburtsdatum) an das Robert Koch-Institut (RKI) übermitteln, welches das CO-

© keBu.Medien – stock.adobe.com

Das digitale Impfzertifikat erspart das Vorzeigen des gelben Impfpasses.

VID-19-Impfzertifikat technisch generiert. Hierzu stellt ihnen der Deutsche Apothekerverband e. V. (DAV) ein Portal zur Verfügung, in das die Daten zwecks Übermittlung einzutragen sind. Zu dieser Datenverarbeitung informierte der DAV in den Datenschutzinformationen seiner Homepage ursprünglich folgendermaßen:

„Um ein Zertifikat auszustellen, müssen die folgenden Daten auf Wunsch des Patienten angegeben werden: Vor- und Nachnamen, Geburtsdatum, Zielkrankheit oder -erreger, Impfarzneimittel, Nummern der Erst- und Wiederimpfung, Datum der Impfungen. Diese Daten werden an das Robert-Koch-Institut übermittelt, damit durch letzteres das Impfzertifikat in Form eines QR-Codes erstellt und an die Apotheke übermittelt werden kann. Es erfolgt keine Speicherung der Patientendaten, diese werden nur kurzfristig zur Übermittlung benötigt. Ebenso wird auch das Impfzertifikat nicht in der Anwendung gespeichert. Wir [der DAV] verarbeiten diese Daten auf der Grundlage von Art. 6 Abs. 1 lit. f DSGVO in dem Interesse, Ihnen die Ausstellung von Covid-19-Impfzertifikaten zu ermöglichen und auf Grundlage von Artikel 6 Abs. 1 lit. b DSGVO (Serviceleistung der Anwendung zur Covid-19-Impfzertifikatserstellung).“

Nach dieser Darstellung schien sich also der DAV für datenschutzrechtlich verantwortlich für die Übermittlung der Patientendaten an das RKI zu halten und diese Verarbeitung auf Artikel 6 Absatz 1 Buchstaben b und f DS-GVO zu stützen. Hierzu teilten wir der LAK und dem LAV mit, wir sähen weder eine Befugnis der Apotheker_innen noch des RKI, die Patientendaten an den Deutschen Apothekerverband (als datenschutzrechtlich Verantwortlichen) zu übermitteln. Auch seien die vom DAV hier geltend gemachten Befugnisnormen zur eigenverantwortlichen Datenverarbeitung durch diesen nicht einschlägig (zumal auf Artikel 9 DS-GVO trotz der Verarbeitung von Gesundheitsdaten nicht eingegangen werde). Nach § 22 Absatz 5 IfSG hätten die Übermittlungen vielmehr unmittelbar zwischen den jeweiligen Apotheker_innen und dem RKI zu erfolgen. Wir hielten das Verfahren trotz der nach den Angaben nur kurzfristigen Datenverarbeitung im Portal nur für datenschutzrechtlich zulässig, wenn zwischen den jeweiligen Apotheker_innen und dem Deutschen Apothekerverband ein Auftragsverarbeitungsvertrag im Sinne von Artikel 28 DS-GVO abgeschlossen werde.

Der LAV und die LAK teilten auch insoweit unsere Ansicht. Es sei zutreffend, dass zwischen DAV als Auftragsverarbeiter und den Apotheken als Verantwortlicher ein Auftragsverarbeitungsvertrag geschlossen werden müsse. Der DAV sehe sich nicht als datenschutzrechtlich verantwortlich für die Übermittlung der Patientendaten an das RKI. Die von uns zitierten Angaben in den Datenschutzhinweisen des Portals seien missverständlich. Die demnach erforderlichen Prozesse seien bereits in die Wege geleitet: Der Auftragsverarbeitungsvertrag werde online auf dem Portal hinterlegt und mit den Apotheken geschlossen. Entsprechend wurden auch in der Folgezeit die Datenschutzhinweise – sowohl auf der Webseite des DAV als auch die Musterdatenschutzhinweise für die Apotheken in der oben bereits zitierten Handlungshilfe des ABDA – überarbeitet.

Ausstellung von Ausweisen im Scheckkartenformat mit aufgedrucktem QR-Code (digitales Impfzertifikat)

Verschiedene Unternehmen bieten – ggf. unter Einbindung von Apotheken – Geimpften gegen Entgelt an, den QR-Code mit dem Impfzertifikat des RKI auf eine Kunststoffkarte zu drucken, um ihn so ohne Einspeicherung in ein Smartphone haltbarer zu machen. Diesen QR-Code können die Apotheken (ggf. nebst weiteren personenbezogenen Daten) an einen Anbieter von Kunststoffkarten weitergeben oder unter Verwendung bestimmter Software der Anbieter die Kunststoffkarte selbst vor Ort erstellen. Zur Frage der datenschutzkonformen Ausgestaltung erhielten wir eine Beratungsanfrage.

>> Mehr Informationen:

Coronavirus-Schutzmasken-Verordnung: https://www.gesetze-im-internet.de/schutzmv/SchutzmV.pdf

„Handlungshilfe zur nachträglichen Erstellung der COVID-19 Impfzertifikate durch Apotheker“ vom 11.6.2021 https://www.mein-apothekenportal.de/downloads/COVID-19-Zertifikate_Handlungshilfe.pdf

Onlineportal des Deutsche Apothekerverband e. V. (DAV) https://www.mein-apothekenportal.de/ <<

Im Rahmen dieser Beratung wiesen wir insbesondere auf Folgendes hin: Zunächst ist in solchen Konstellationen zu klären, wer wofür datenschutzrechtlich im Sinne von Artikel 4 Nummer 7 DS-GVO verantwortlich sein soll. Soweit in diesem Zusammenhang eine Auftragsverarbeitung oder eine gemeinsame Verantwortung vorliegen soll, sind entsprechende Verträge abzuschließen, die den Anforderungen aus Artikel 26 bzw. 28 DS-GVO genügen.

Den Geimpften sind den Anforderungen nach Artikel 12 und 13 DS-GVO entsprechende Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erteilen.

Die Rechtsgrundlagen für die Verarbeitung sind zu klären. Dabei ist zu beachten, dass der Impfstatus einer Person ein Gesundheitsdatum im Sinne von Artikel 9 DS-GVO ist. Seine Verarbeitung wird daher in der hier vorliegenden Konstellation nur aufgrund einer ausdrücklichen Einwilligung der betroffenen Person (Artikel 9 Absatz 2 Buchstabe a DS-GVO) zulässig sein. Insoweit sahen die Verfahrensabläufe der Anbieter_innen teilweise vor, dass die Apotheke lediglich elektronisch eine mündliche „Zustimmung" der geimpften Person „zu den Datenschutzinformationen" dokumentieren soll. Das ist nicht zuletzt vor dem Hintergrund, dass der Verantwortliche nach Artikel 5 Absatz 2 DS-GVO für die Rechtsmäßigkeit der vorgenommenen Datenverarbeitung rechenschaftspflichtig ist (und damit u. a. die informierte und freiwillige Erteilung der Einwilligung nachweisen können muss), durchaus bedenklich; ausreichende Vorkehrungen zur Sicherung einer informierten, freiwilligen und ausdrücklichen Einwilligung der betroffenen Personen konnten wir hierin nicht erkennen.

Zuweilen sahen die Anbieter_innen eine Reihe von Verarbeitungen vor, die zur Erstellung der Scheckkarte nicht erforderlich erscheinen. So wurde etwa teilweise von den Apotheken verlangt, dass diese den Personalausweis der betroffenen geimpften Person kopieren und die Kopie dem/der Anbieter _in übersenden oder eine E-Mail-Adresse der geimpften Person „für Updates" erheben und dem Anbieter mitteilen sollten. Hierfür erschienen uns der Zweck und die Rechtsgrundlage der Verarbeitungen zweifelhaft. Ebenfalls stellte sich uns die Frage nach dem Zweck und der Rechtsgrundlage, wenn die personenbezogenen Daten zu der Scheckkarte im Warenwirtschaftssystem der Apotheke hinterlegt werden sollen. Soweit von Seiten des Anbieters weitere Unterauftragnehmer eingesetzt und deswegen eine Datenverarbeitung auch außerhalb des Geltungsbereichs der DS-GVO erfolgt, sind die besonderen Anforderungen aus Kapitel V der DS-GVO zu beachten.

Bei dem Verfahren zur Erstellung der mit dem QR-Code bedruckten Scheckkarte sind außerdem nach Artikel 25, 32 DS-GVO in Verbindung mit § 22 Absatz 2 des Bundesdatenschutzgesetzes die erforderlichen technischen und organisatorischen Maßnahmen umzusetzen. Dabei ist ebenfalls zu berücksichtigen, dass der Impfstatus einer Person (ebenso wie die Einzelinformationen hierzu) ein besonders schutzwürdiges Gesundheitsdatum ist. Daher muss beispielsweise die eingesetzte Software diesen besonderen Anforderungen genügen. Etwaige elektronische Mitteilungen zwischen Apotheker_innen und Anbieter_innen mit Bezug auf Gesundheitsdaten der betroffenen Personen müssen Ende-zu-Ende verschlüsselt erfolgen. Soweit die bedruckte Scheckkarte postalisch versandt werden soll, ist mit Blick auf die darin enthaltenen Gesundheitsdaten zu empfehlen, dass der Versand nachverfolgt wird.Schließlich ist in Anbetracht der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten eine Datenschutz-Folgenabschätzung nach Artikel 35 Absatz 3 Buchstabe b DS-GVO vorzunehmen.

Insgesamt enthält die Scheckkarte dieselben Informationen wie der QR-Code in der Corona-Warn-App oder der CovPass-App. Für die eigentliche Erstellung des digitalen Impfzertifikats wird keine Speicherung personenbezogener Daten vorgenommen, und zwar weder von Seiten der Apotheke noch von Seiten des Robert-Koch-Instituts, das die Daten unmittelbar nach Erstellung des Zertifikats wieder löscht. Auch bei Hinterlegung des Impfzertifikats z. B. in der CovPass-App (aber auch in anderen Apps wie z. B. der Corona-Warn-App) werden die Daten nur lokal auf dem eigenen Handy gespeichert. Wenn Anbieter Kunststoff-Scheckkarten mit dem QR-Code anbieten möchten, sollten sie sicherstellen, dass die Bürger_innen gut informiert darüber entscheiden können, ob sie diese Leistung in Anspruch nehmen wollen. Auch müssen Anbieter_

innen sicherstellen, dass die Datenverarbeitung, die umfangreicher ist als bei der Hinterlegung in der CWA, auch rechtmäßig ist.

1.7 Die Verpflichtung zur Kontaktdatenverarbeitung, Luca App und Corona-Warn-App

Als ein Mittel zur Eindämmung der Pandemie gilt die Kontaktnachverfolgung durch die Gesundheitsämter. Um diese Nachverfolgung bei Veranstaltungen, dem Besuch von Gaststätten und bei verschiedenen anderen Gelegenheiten zu erleichtern, bei denen mehrere Personen mit höherem Ansteckungsrisiko zusammenkommen, wurde schon ab Mai 2020 darauf gesetzt, Veranstalter, Gastwirte und andere Verantwortliche zu einer Erfassung und vierwöchigen Speicherung von Anwesenheits- und Kontaktdaten zu verpflichten (siehe hierzu schon unseren Tätigkeitsbericht 2020, S. 10 ff.). Die daraus resultierende Zettelwirtschaft führte – wie wir schon im letzten Tätigkeitsbericht (2020, S. 12 ff.) geschildert haben – zu zahlreichen Datenschutzverstößen. Diverse Apps versuchten diesen Prozess zu digitalisieren, scheiterten aber zumeist bereits daran, dass die Hersteller der Apps die Angaben der Gäste zumeist noch nicht einmal einer rudimentären Plausibilitätsprüfung unterzogen, Zugriff auf die Kontakt- und Anwesenheitsdaten der Gäste zuließen oder solche Daten gar an Werbekonzerne wie Facebook und Google weitergaben.

Einen anderen, freiwilligen Ansatz verfolgte und verfolgt die Corona-Warn-App (CWA): Deren Anwender können sich warnen lassen, wenn sie sich in der Nähe anderer CWA-Nutzer aufgehalten haben und diese eine eigene Infektion via App mitteilen. Freiwillig sind dabei die Nutzung der App, das Einstellen eines (positiven) Tests und die eigene Isolation beziehungsweise Testung bei Benachrichtigung von einem potentiell ansteckenden Kontakt. Die CWA arbeitet dabei datensparsam und ohne zentrale Sammlung von Kontaktdaten, ermöglicht aber nach ihrer Konzeption – ganz bewusst – nicht die hoheitliche Anordnung von Maßnahmen durch die Gesundheitsämter gegenüber Kontaktpersonen von positiv Getesteten. Zudem verlief die Weiterentwicklung der App anfangs schleppend, im Laufe der 2. und 3. Corona-Welle wurden nur kleinere Aktualisierungen vorgenommen und die wichtige Möglichkeit zur Registrierung von Veranstaltungen stand erst Ende April 2021 zur Verfügung. Da blieben wichtige Chancen ungenutzt.

© Koonsiri – stock.adobe.com

Die digitale Kontaktnachverfolgung etwa in Cafés hat die „Zettelwirtschaft" weitgehend beendet.

Kontaktnachverfolgung und die Luca App

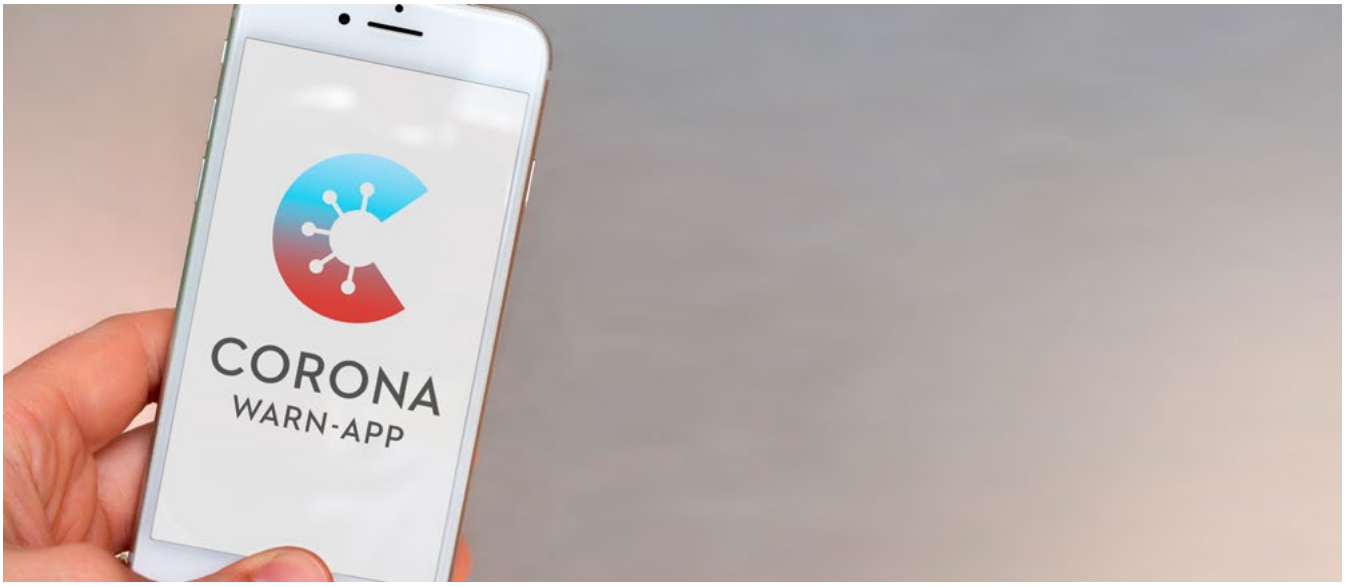
In dieser Situation wurden wir im Januar 2021 auf die Luca App aufmerksam. Diese speichert die Anwesenheitsdaten mit Hilfe von Verschlüsselung so, dass weder der Betreiber des Dienstes noch die Veranstalter oder Gastwirte (oder die anderen nach der Corona-Verordnung zur Erhebung und Speicherung von Anwesenheits- und Kontaktdaten Verpflichteten, im folgenden „Veranstalter") Zugriff auf die Daten haben, die Gesundheitsämter diese aber dennoch nach Freigabe durch die Veranstalter abfragen können. Erste technische Analysen hatten diese Arbeitsweise bestätigt. Und die App bietet die Möglichkeit, die Telefonnummer der Teilnehmenden durch die Zusendung eines Codes per SMS (jedenfalls rudimentär) zu verifizieren.

Schwierigkeiten sahen wir zwar bei der häufigen Übermittlung von sogenannten Trace-IDs, die daraus resultierenden Probleme waren aber nicht unüberwindbar. Einzelne Kritikpunkte wie die Einbindung von Google Analytics auf der „Marketing"-Website behob der Hersteller schnell. In rechtlicher Hinsicht empfahlen wir dem Hersteller, dass hinsichtlich der verarbeiteten Daten zu unterscheiden sein dürfte: Ein Teil der Daten – z. B. die Daten, die für die zusätzliche Funktion der Führung eines Kontakttagebuchs für den Nutzer oder die Nutzerin gespeichert werden – sollte aufgrund des Nutzungsvertrages oder einer Einwilligung zwischen Nutzer_in und App-Betreiber in der Ver-

antwortung durch diesen verarbeitet werden. Die Anwesenheitsdaten selbst sollten dagegen nach unserer Empfehlung durch den App-Betreiber als Auftragsverarbeiter für die „zur Datenverarbeitung Verpflichteten", also die Veranstalter, Gastronomen etc. als Verantwortliche verarbeitet werden. Mit einem Autragsverarbeitungsvertrag zwischen App-Betreiber und Veranstalter konnte u. a. sichergestellt werden, dass die Anwesenheitsdaten während der aus Sicht des Verordnungsgebers erforderlichen Frist von vier Wochen unabhängig vom Bestand des Nutzungsvertrages zwischen Besucher_innen und App-Betreiber_innen oder einer Einwilligung des/der Besucher_in gespeichert bleiben durften. Auch wenn es kurios klingen mag, dass die Veranstalter für die Verarbeitung von Daten verantwortlich sein sollen, die sie gar nicht im Klartext lesen können (weil sie auch ihnen gegenüber verschlüsselt gespeichert werden), so schien uns diese zulässige Konstruktion doch der Zielrichtung der Corona-Verordnung am nächsten zu kommen.

Im Rahmen unserer Beratung der Landesregierung haben wir eine rechtliche und technische Analyse und Bewertung durchgeführt. In unserer Stellungnahme vom 2. März 2021 kamen wir zu dem Schluss, dass die Luca App – vorbehaltlich noch gewisser vom Anbieter zugesagter Anpassungen – datenschutzkonform eingesetzt werden kann. Wie üblich haben wir dabei nur Datenschutz-Themen berücksichtigt und z. B. keine Bewertung des Geschäftsmodells des Herstellers durchgeführt. Die technische Bewertung ergab, dass Luca die Verarbeitung der Kontakt- und Anwesenheitsdaten prinzipiell gut geschützt durchführt und keine Anhaltspunkte dafür bestehen, dass die Daten vom Anbieter eingesehen werden können. Dabei haben wir allerdings darauf hingewiesen, dass unsere Untersuchungen keine Sicherheitsaudits ersetzen, zumal wir – zeitlich bedingt – keine Analyse des Quellcodes hatten vornehmen können. Wir empfahlen daher, solche Audits durchzuführen. In rechtlicher Hinsicht wiesen wir die Landesregierung darauf hin, dass für den Einsatz die Corona-Verordnung geändert werden müsse. Denn diese ging zum damaligen Zeitpunkt noch davon aus, dass der Veranstalter die Kontaktdaten lesen könne, indem u. a. von ihm eine Vollständigkeitskontrolle und in gewissem Rahmen eine Plausibilitätsprüfung erwartet wurde, was er bei der ihm gegenüber verschlüsselten Verarbeitung nicht leisten konnte.

Insgesamt überwogen aber mit Blick auf den Datenschutz die Vorteile des Einsatzes der Luca App gegenüber einer papiergestützten Verarbeitung. Dabei sahen wir insbesondere folgende Vorteile: Durch die Verschlüsselung kann der Veranstalter die Daten nicht lesen, so dass sowohl ein Missbrauch durch Beschäftigte des Veranstalters als auch eine unbefugte Kenntnisnahme durch Dritte wie etwa andere Teilnehmende an der Veranstaltung (und den App-Betreiber selbst) ausgeschlossen werden kann.



Die Corona-Warn-App hilft bei der Pandemie-Bekämpfung.

Die App ermöglicht eine sichere Übermittlung der Anwesenheits- und Kontaktdaten vom Veranstalter an das Gesundheitsamt, wenn dieses die Daten anfordert und der Veranstalter sie freigibt. Bei Nutzung der App kann die datenschutzkonforme Vernichtung der durch die Veranstalter zu speichernden Anwesenheits- und Kontaktdaten nach Ablauf der vorgeschriebenen Speicherfrist von vier Wochen sichergestellt werden. Weitere Empfehlungen, wie eine Veröffentlichung des Programmcodes unter einer Open Source Lizenz und von Muster-Datenschutzinformationen für Veranstalter, wurden vom Hersteller im Laufe der nächsten Wochen umgesetzt.

Die Landesregierung ist unserer Stellungnahme gefolgt und hat sich in der Folge entschlossen, die Lizenzen für den flächendeckenden Einsatz der Luca App in Baden-Württemberg zu beschaffen. Bei der erforderlichen Umformulierung der Corona-Verordnung unterstützten wir sodann die Landesregierung. Dabei war uns u. a. wichtig, dass Menschen, welche die Luca App (z. B. mangels Smartphones) nicht nutzen können oder wollen, nicht vom Besuch von Veranstaltungen (und anderen Angeboten und Einrichtungen) ausgeschlossen werden, sondern dass ihnen immer auch eine nicht-digitale Alternative zur Verarbeitung der Kontaktdaten vom Veranstalter angeboten werden muss.

Auch im weiteren Verlauf haben wir uns immer wieder mit der (immer wieder auch in Kritik geratenen) Luca App beschäftigt und auch deren weitere Verbesserung gefördert. Insbesondere haben wir uns an der Entwicklung einer gemeinsamen „Stellungnahme zu Kontaktnachverfolgungssystemen – insbesondere zu ‚Luca' der culture4life GmbH" der Datenschutzkonferenz (DSK), dem Gremium der unabhängigen deutschen Datenschutzaufsichtsbehörden der Länder und des Bundes, beteiligt und mit der DSK gemeinsam eine „Orientierungshilfe zum Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurant- und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19" erstellt.

Mehrfach haben wir in der Folge auch Anfragen erhalten, in denen Stellen die Luca App einsetzen wollten, die nicht zur Kontaktdatenverarbeitung (nach Infektionsschutzrecht) verpflichtet waren. Der Einsatz zur Kontaktdatenerfassung durch nicht gesetzlich hierzu verpflichtete Stellen war indes nicht der eigentliche Zweck der Entwicklung und Einführung der Luca App und erwies sich in mehrfacher Hinsicht als problematisch: Zwar ist grundsätzlich auch denkbar, dass eine nicht verpflichtete Stelle Kontaktdaten etwa auf Basis einer Einwilligung verarbeitet. Grundvoraussetzung für eine wirksame Einwilligung ist indes, dass diese freiwillig erteilt wird. Wenn aber etwa Behörden den Zugang von der Erteilung einer solchen Einwilligung abhängig machen, wird die Freiwilligkeit vielfach nicht gegeben sein (vgl. hierzu auch schon den Beitrag „Zugang zum Rathaus nur gegen Daten", S. 16 f. in unserem Tätigkeitsbericht 2020).

Aber auch speziell die Nutzung der Luca App auf Basis einer Einwilligung gegenüber einem nicht verpflichteten „Veranstalter" wies zum damaligen Zeitpunkt verschiedene rechtliche Herausforderungen auf, insbesondere:

>> Mehr Informationen:

Stellungnahme des LfDI Baden-Württemberg zur App „Luca": https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/04/Stellungnahme-LfDI-BW-Luca-App.pdf

Pressemitteilung des SM „Baden-Württemberg setzt auf die Luca-App" https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/baden-wuerttemberg-setzt-auf-die-luca-app/

Stellungnahme der DSK zu „Kontaktnachverfolgungssystemen – insbesondere zu ‚Luca' der culture4life GMBH" https://www.datenschutzkonferenz-online.de/media/st/20210429_DSK_Stellungnahme_LUCA.pdf

Stellungnahme der DSK zu „Kontaktnachverfolgung in Zeiten der Corona-Pandemie: Praxistaugliche Lösungen mit einem hohen Schutz personenbezogener Daten verbinden"https://www.datenschutzkonferenz-online.de/media/st/20210329_DSK_Stellungnahme.pdf

Stellungnahme der DSK „Einsatz von digitalen Diensten zur Kontaktnachverfolgung anlässlich von Veranstaltungs-, Einrichtungs-, Restaurant-und Geschäftsbesuchen zur Verhinderung der Verbreitung von Covid-19": https://www.datenschutzkonferenz-online.de/media/oh/20210429_DSK_OH_Kontaktnachverfolgung.pdf <<

- die Einbindung der Einwilligungserklärung in den Eincheck-Vorgang (hier werden Nutzer_innen häufig nicht nachvollziehen können, warum sie/er bei einzelnen Eincheckvorgängen einwilligen muss und bei anderen nicht);

- die Dokumentation der Einwilligung mit Blick auf die Rechenschaftspflicht des Verantwortlichen (Art. 5 Abs. 2 DS-GVO) bei gleichzeitiger Aufrechterhaltung des Vorteils der Ende-zu-Ende-Verschlüsselung auch gegenüber dem Zugriff des Veranstalters;

- die Ermöglichung der Löschung bei Widerruf.

Die Betreiber der App haben später für diese speziellen Probleme bei Verwendung der Luca-App durch nicht verpflichtete „Veranstalter" auf Basis von Einwilligungen der Besucher Lösungen entwickelt; allerdings hatten wir bislang noch keinen Anlass, diese später entwickelten Lösungen zu bewerten.

Kontaktnachverfolgung und Corona-Warn-App

Auch wenn durch die Einführung der Ende-zu- Ende verschlüsselnden Luca-App schon ein wesentlicher Fortschritt gegenüber der ausschließlichen „Zettelwirtschaft" erreicht war, haben wir die Landesregierung wiederholt darum gebeten, vor dem Hintergrund der jeweils aktuellen Entwicklungen, insbesondere der Infektionsrate einerseits und der tatsächlichen Nutzung der Kontaktdaten durch die Gesundheitsämter andererseits, zu prüfen, inwieweit es noch sachgerecht ist, an dem Prinzip uneingeschränkt festzuhalten, die hoheitliche Kontaktnachverfolgung durch die Gesundheitsämter (ggf. mit Quarantäneanordnungen) im Wege der zwingenden Kontaktdatenverarbeitung durch zahlreiche Verpflichtete (der Privatwirtschaft) sicherzustellen. Aus unserer Sicht müsse (so etwa im vergangenen Sommer) bei geringen Infektionszahlen daran gedacht werden, auf die Kontaktdatenverarbeitung auch – zumindest nach und nach – wieder zu verzichten oder zumindest die freiwillige Teilnahme an der Corona-Warn-App als gleichwertig zu akzeptieren. Seit Ende August 2021 kam der Umstand hinzu, dass das Sozialministerium in der öffentlichen Debatte einen Strategiewechsel bei der Kontaktnachverfolgung ankündigte: Demnach sollten die Gesundheitsämter künftig nicht mehr bei jedem Corona-Fall die Kontakte – etwa in Kinos oder Gaststätten – nachverfolgen müssen. Die Lage habe sich insofern geändert, als dass es eine zunehmende Zahl von Geimpften und Genesenen gebe; wer aber geimpft oder genesen sei, müsse in aller Regel – auch als Kontaktperson – nicht in Quarantäne. Der öffentliche Gesundheitsdienst wolle daher die Kräfte auf eine intelligente Schwerpunktnachverfolgung von herausragenden Ereignissen konzentrieren.

Auch dieser Strategiewechsel stellte nach unserer Einschätzung die Notwendigkeit und Angemessenheit der massenhafte Kontaktdatenverarbeitung in Frage. Wir baten das Sozialministerium daher zu prüfen, ob es nicht angesichts dieser Umstände angemessen sei, auch die Nutzung der Corona-Warn-App alternativ zur verpflichtenden Kontaktdatenverarbeitung genügen zu lassen – wie dies andere Länder bereits zuvor zugelassen hatten. Denn die CWA stellt eine datensparsamere Möglichkeit zur Benachrichtigung über kritische Kontakte mit positiv Getesteten dar. Zwar ist es mit der Corona-Warn-App nicht möglich, verpflichtende Quarantäne-Anordnungen zu verschicken, sie hat aber einen starken Vorteil in der Geschwindigkeit, da sie direkt und ohne den Umweg über die Abfrage durch die Gesundheitsämter warnen kann. Zur näheren Begründung konnten wir auf eine Entschließung der DSK verweisen, die in diesem Sinne bereits unter dem 29. April 2021 aufgefordert hatte, die Chancen der Corona-Warn-App 2.0 zu nutzen.

Die Landesregierung hat dankenswerter Weise diese Prüfung vorgenommen. Zwar konnte sie sich bislang noch nicht dazu entschließen, die vielfältigen Verpflichtungen zur Kontaktdatenverarbeitung zu reduzieren, was durch die steigenden Inzidenzen nachvollziehbar begründet sein mag. Sie hat aber mit der Änderungsverordnung vom 13. Oktober 2021 den Willen zum Ausdruck gebracht, das Einchecken mit der Corona-Warn-App durch den Nutzenden anstelle der verbindlichen Kontaktdatenverarbeitung durch den Veranstalter genügen zu lassen. Rechtstechnisch kam dieser Wille freilich im Text der Verordnung zunächst nur unvollkommen (und eindeutig vor allem aus der Begründung der Änderungsverordnung) zum Ausdruck, indem der Verordnungstext, der die Verwendung der Luca-App gestattete, nur geringfügig geändert wurde.

Der Verordnungstext, der die Verwendung der Luca zuließ, lautete zuvor wie folgt:

„Die Erhebung und Speicherung [der Anwesenheits- und Kontaktdaten] kann auch in einer für den zur Datenverarbeitung Verpflichteten nicht lesbaren Ende-zu-Ende-verschlüsselten Form nach dem Stand der Technik erfolgen, solange sichergestellt ist, dass das zuständige Gesundheitsamt die Daten im Falle einer Freigabe durch den zur Datenverarbeitung Verpflichteten im Wege einer gesicherten Übermittlung in einer für das Gesundheitsamt lesbaren Form erhält. Die Ende-zu Ende-verschlüsselte Form muss die Übermittlung der Daten an das Gesundheitsamt für einen Zeitraum von vier Wochen ermöglichen."

Nach der Neufassung durch die Änderungsverordnung vom 13. Oktober 2021 lautete der Verordnungstext insoweit nur noch:

„Die Erhebung und Speicherung kann auch in einer für den zur Datenverarbeitung Verpflichteten nicht lesbaren Ende-zu-Ende-verschlüsselten Form nach dem Stand der Technik erfolgen.

In der Begründung zur Änderungsverordnung wurde dabei ausgeführt:

„Durch die Streichung des 2. Halbsatzes von Satz 1 [Anm. LfDI: Hinzuzudenken war wohl „und des Satzes 2"] erfolgt eine Anpassung an die geänderte Nachverfolgungspraxis. Es können fortan entsprechend weitere wirkungsvolle digitale Applikationen, wie z. B. die Corona-Warn-App für die Kontaktnachverfolgung genutzt werden. Aufgrund der zuletzt stabilen Infektionslage ist es unter Verhältnismäßigkeitsgesichtspunkten geboten, auch solche Applikationen zuzulassen, welche keine direkte Nachverfolgung durch das Gesundheitsamt ermöglichen."

Auch wenn die beabsichtigte Änderung sehr zu begrüßen war, konnte der Normentext insoweit kaum als normenklar bezeichnet werden. Bei der Formulierung wurde insbesondere nicht bedacht, dass bei Nutzung der Corona-Warn-App – anders als bei der Luca-App – nicht der zur Datenverarbeitung Verpflichtete (also der Veranstalter) für die Datenverarbeitung verantwortlich ist, sondern dass Robert-Koch-Institut (als Betreiber der Corona-Warn-App), zu dem der Verpflichtete in keinerlei datenschutzrechtlicher (Vertrags-)Beziehung steht, so dass insoweit schon gar nicht mehr von einer Erhebung und Speicherung der Daten durch den zur Datenverarbeitung Verpflichteten die Rede sein kann.

Unserer Kritik auch an dieser zwar gut gemeinten, aber rechtstechnisch wenig gelungenen Formulierung stieß dankenswerter Weise nicht auf taube Ohren. Mit unserer Unterstützung formulierte die Landesregierung (mit der Änderungsverordnung vom 17. Dezember 2021) die Passage neu (fügte insbesondere einen neuen Absatz in den hier einschlägigen Paragraphen ein), so dass nunmehr aus unserer Sicht normenklar hervorgeht, dass die

>> Mehr Informationen:

Bericht Stuttgarter Zeitung vom 25.8.21: „Verzicht auf massenhafte Kontaktverfolgung geplant" https://www.stuttgarter-zeitung.de/inhalt.coronavirus-in-baden-wuerttemberg-verzicht-auf-massenhafte-kontaktverfolgung-geplant.5e7cae1f-918a-46b5-8630-6921041b344c.html

Stellungnahme der DSK zu „Chancen der Corona-Warn-App 2.0 nutzen" https://www.datenschutzkonferenz-online.de/media/en/20210429_DSK_Entschlie%C3%9Fung_Chancen_der_CWA_2.0_nutzen.pdf

Verordnung derLandesregierungzur Änderung der Corona-Verordnung vom 13.10.2021: https://www.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Coronainfos/211013_VO_der_LReg_zur_Aenderung_der_CoronaVO.pdf

Begründung zur ersten Änderungsverordnung vom 13. Oktober 2021 zur Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2 (Corona-Verordnung –CoronaVO) vom 15. September 2021: https://www.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Coronainfos/211013_Begruendung_zur_1.Aenderungs-VO_zur_11.CoronaVO.pdf

Sechste Verordnung derLandesregierung zur Änderung derCorona-Verordnung: https://www.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Coronainfos/211217_Sechste_VO_der_LReg_zur_Aenderung_der_CoronaVO.pdf <<

Pflicht des Veranstalters zur Verarbeitung der Kontaktdaten entfällt, wenn eine Besucherin/ein Besucher mit der Corona-Warn-App (ordnungsgemäß) eincheckt. Die Passage lautet:

„Die Pflicht zur Datenverarbeitung nach Absatz 1 entfällt in Bezug auf solche Anwesende, die das Angebot des zur Datenverarbeitung Verpflichteten zur Nutzung einer digitalen Anwendung annehmen, die ohne Speicherung personenbezogener Daten durch den zur Datenverarbeitung Verpflichteten eine Benachrichtigung der Nutzerinnen und Nutzer dieser Anwendung im Falle eines positiven Testergebnisses bei einer anderen, gleichzeitig anwesenden Person ermöglicht."

Somit wurde wieder mehr Rechtsklarheit geschaffen für die Bürgerschaft – wir Datenschützer_innen helfen, wo wir können. Trotz der Verbesserungen und Erleichterungen, welche die Landesregierung mit dem Angebot der Luca-App und der alternativen Zulassung der Nutzung der Corona-Warn-App bereits ermöglicht, wird sie auch weiterhin immer wieder anhand des aktuellen Pandemiegeschehens zu prüfen haben, inwieweit die massenhafte Erfassung und Speicherung von Kontakt- und Anwesenheitsdaten der Bürger_innen bei den unterschiedlichen Gelegenheiten des Alltags überhaupt noch geeignet, erforderlich und angemessen ist. Dabei ist zu sehen, dass nach der gesetzlichen Verordnungsermächtigung (§ 28a Absatz 1 Nummer 17 und Absatz 4 bzw. Absatz 7 Satz 1 Nummer 8 und Satz 3 des Infektionsschutzgesetzes (IfSG) in Verbindung mit § 28 Absatz 1 Und § 32 IfSG) die Anordnung der Verarbeitung von Kontaktdaten nur erfolgen darf, „um nach Auftreten einer Infektion mit dem Coronavirus SARS-CoV-2 mögliche Infektionsketten nachverfolgen und unterbrechen zu können" und die Verarbeitung auch nur soweit erfolgen darf, als „dies zur Nachverfolgung von Kontaktpersonen zwingend notwendig ist".

Die Pflicht zur Kontaktdatenverarbeitung bei vielen Gelegenheiten des öffentlichen Lebens stellt dabei einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht dar, den es zu beenden gilt, soweit die Kontaktdaten daher nicht mehr zur Pandemiebewältigung benötigt werden.

Insgesamt gesehen ist es uns durchaus gelungen, die unpraktische und überzogene Zettelwirtschaft und die daraus resultierende massenhafte Offenlegung von personenbezogenen Daten bei der Kontaktnachverfolgung auf ein Mindestmaß zu reduzieren. Zugleich hat die CWA einen Entwicklungsschub erfahren, der hoch erfreulich ist. Technische Mittel gegen die Pandemie sind durchaus wirkungsvoll – für sich genommen aber sicherlich keine „Problemlöser". Auch das müssen wir lernen.

Wir leisten mit unserer Expertise gerne einen Beitrag dazu, dass technische Möglichkeiten der Digitalisierung wirksam und rechtssicher genutzt werden können. Zentrales Problem bleibt die mangelnde technische Infrastruktur und der fehlende Wille, sich technisch auf ein angemessenes Sicherheitsniveau zu bringen sowie die korrekte Nutzung der digitalen Systeme zu fördern. Beschäftigte in den Verwaltungen brauchen Unterstützung bei Einführung, Etablierung und Nutzung von digitalen Technologien und bei der digitalen Transformation. Auch brauchen die öffentliche Stellen IT-Wissen im Haus, direkt vor Ort. Insbesondere mit Blick auf IT-Sicherheit ist es ohnehin allen öffentlichen Stellen zu empfehlen, sorgfältig und professionell den Austausch mit Fachleuten der IT-Infrastruktur zu pflegen. Mehr dazu im Kapitel IT-Sicherheit.

Endlich wieder einmal unbeschwert und ohne Check-in einen Espresso trinken gehen – irgendwann wird das wieder möglich.

2. Bildungsplattform des Kultusministeriums

Die Beratung des Kultusministeriums zur Digitalen Bildungsplattform beschäftigte die Behörde des Landesbeauftragten auch im Jahr 2021 sehr intensiv. Mit Blick auf das Ziel, dass die Schulen eine passende und datenschutzkonforme Lösung erhalten, haben wir diese Beratung sehr gerne wahrgenommen.

Bereits seit dem vergangenen Jahr steht den Schulen als Teil dieser Bildungsplattform mit dem vom Kultusministerium angebotenen und von uns in dieser Version datenschutzrechtlich geprüften Dienst Threema (siehe Seite 51 f., Tätigkeitsbericht 2020) ein datenschutzkonformer Messenger-Dienst zur Verfügung.

Das Kultusministerium plant, die Digitale Bildungsplattform um weitere Komponenten zu erweitern. Hierzu gehören insbesondere

- ein E-Mail-Dienst für Lehrkräfte mit einer Büro-Arbeitsplatzumgebung samt Online-Speicher, Textverarbeitungs- und Tabellenkalkulationssoftware,
- ein weiteres Lernmanagementsystem (LMS) neben der den Schulen bereits zur Verfügung stehenden Lernplattform Moodle und
- ein Identity and Access Managementsystem (IdAM).

Die Umsetzung dieser weiteren Komponenten stand im Jahr 2021 insoweit im Fokus unserer Beratungen gegenüber dem Kultusministerium.

E-Mail-Dienst und Arbeitsplatz für Lehrer_innen

Für E-Mail, Online-Speicher, Textverarbeitung, Tabellenkalkulation etc. hatte das Ministerium, wie wir bereits in unserem letzten Tätigkeitsbericht (a. a. O.) ausgeführt haben, den Dienst Microsoft 365 vorgesehen. Hierzu wurde vom Ministerium ausgehend von den vielfältigen Varianten von Microsoft 365, mit Unterstützung durch die Landesoberbehörde IT Baden-Württemberg (BITBW) und des Software- und Dienste-Anbieters, jene Variante gewählt, welche den Datenschutz am besten gewährleisten konnte. Dies spiegelte sich auch in der Konfiguration des Systems wieder, da alle Einstellungen möglichst datenschutzkonform vorgenommen wurden. Um dies auch am laufenden System zu untersuchen, hatten wir 2020 einem Pilotbetrieb an einigen Schulen zugestimmt. Dabei erhielten an den teilnehmenden Schulen nur Lehrkräfte einen Zugang, nicht jedoch Schülerinnen und Schüler. Auch wir erhielten Zugänge für eine eigene Testschule, damit wir das System technisch prüfen konnten. Während unserer Beratung standen wir in regelmäßigem Austausch mit dem Kultusministerium und Vertreter_innen des Software- und Dienste-Anbieters.

Zum Ende des Pilotprojekts konnten wir im April 2021 eine Empfehlung gegenüber dem Kultusministerium abgeben. Wenngleich unsere Prüfungen aufgrund des Umfangs und der Weiterentwicklung der Dienste nicht abschließend sein können, hatten sie hinreichend klar ergeben, dass aus unserer Sicht die Risiken beim Einsatz der nun erprobten Microsoft-Dienste im Schulbereich als inakzeptabel hoch zu bewerten waren. Wir rieten deswegen davon ab, diese im Schulbereich zu nutzen.

Verantwortliche – und das sind im Schulbereich die Schulen (vgl. Artikel 4 Nr. 7 DS-GVO und § 1 des Schulgesetzes für Baden-Württemberg) – haben beim gewählten System keine vollständige Kontrolle über das Gesamtsystem und den US-amerikanischen Auftragsverarbeiter Microsoft. Sie können nach unserer Bewertung bei Verwendung dieses Dienstes derzeit nicht ausreichend nachvollziehen, welche personenbezogenen Daten wie und zu welchen Zwecken verarbeitet werden, und nicht nachweisen, dass die Verarbeitung auf das für diesen Zweck notwendige Minimum reduziert ist. All das müssten sie aber, um ihrer Rechenschaftspflicht aus Artikel 5 Absatz 2 DS-GVO und dem Prinzip der Datenminimierung aus Artikel 5 Absatz 1 Buchstabe c DS-GVO gerecht zu werden. Zudem sind für einige Übermittlungen personenbezogener Daten an Microsoft keine Rechtsgrundlagen erkennbar, was nach der Datenschutz-Grundverordnung aber erforderlich wäre. Und teilweise konnten wir

>> Mehr Informationen:

LfDI-Empfehlung zum Pilotprojekt zur Nutzung MS 365 an Schulen: https://www.baden-wuerttemberg.datenschutz.de/empfehlung-lfdi-online/<<

Übermittlungen personenbezogener Daten auch in Regionen außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung feststellen, für die wir nicht erkennen konnten, dass die hierfür (unter Berücksichtigung der Ergebnisse des Schrems-II-Urteils des Europäischen Gerichtshofs aus dem Jahr 2020) zu beachtenden besonderen Bedingungen nach Kapitel 5 der Datenschutz-Grundverordnung eingehalten würden. Für den Schulbereich haben wir daher ein hohes Risiko der Verletzung von Rechten und Freiheiten betroffener Personen beim Einsatz von Microsoft 365 festgestellt, das sich auch nicht kurzfristig abstellen lässt. Dies gilt für die ins Auge gefasste Erweiterung des Systems um Konten für die Schülerinnen und Schüler umso mehr. Der Staat hat eine Garantenstellung für die überwiegend minderjährigen Schülerinnen und Schüler, welche zudem der staatlichen Schulpflicht unterliegen und daher der Verwendung ihrer persönlichen Daten nicht ausweichen können. In dieser Konstellation bewerten wir das Risiko als inakzeptabel hoch.

Dabei ist es nicht etwa generell unmöglich, Cloud-Dienste mit dem Funktionsumfang von Microsoft 365 datenschutzkonform zu betreiben. Microsoft als Hersteller und Diensteanbieter hat sich aber dazu entschieden, eine intransparente Anzahl an Verarbeitungen auch zu eigenen Zwecken durchzuführen und zahlreiche nicht ausreichend dokumentierte Datenflüsse zu implementieren. Die geschilderten Schwierigkeiten sind also nicht etwa systemimmanent für Cloud-Dienste, vielmehr hängen sie von der konkreten Gestaltung des jeweiligen Dienstes ab.

Im Juli 2021 teilte das Kultusministerium mit, dass die Teile der Digitalen Bildungsplattform, welche im Pilotbetrieb mir Microsoft 365 eingesetzt wurden, neu ausgeschrieben werden. Wir unterstützen diese Entscheidung ausdrücklich und werden das Kultusministerium auch in diesem weiteren Verfahren gerne weiter beraten. Ein erster Workshop mit den Interessenvertretungen fand hierzu bereits im November 2021 unter unserer Beteiligung statt.

Lernmanagementsystem

Um den Schulen im Rahmen der digitalen Bildungsplattform (neben dem bereits bislang angebotenen System Moodle) ein weiteres Lernmanagementsystem (LMS) zur Verfügung stellen zu können, hatte das Kultusministerium bereits im Jahr 2019 eine Ausschreibung gestartet. Dabei hatte es uns jedoch leider nicht an der Erstellung der Ausschreibungsunterlagen beteiligt. In den Bieterrunden ab 2020 konnten wir uns jedoch beratend einbringen und so – wenngleich leider nur begrenzt – unsere fehlende Einbindung bei der Erstellung der Ausschreibungsunterlagen teilweise ausgleichen. Dabei legten wir insbesondere Wert auf die Frage der Einhaltung

Das Kultusministerium hat entschieden: Eine datenschutzkonforme digitale Bildungsplattform kommt.

der Bedingungen des Kapitels 5 der DS-GVO, soweit es zu Datentransfers in Drittstaaten kommen sollte, sowie auf die Vermeidung von Verarbeitungen zu Zwecken des Anbieters. Bei der Entscheidung im Spätherbst 2020 zum Zuschlag für itslearning und den anschließenden Vertragsabschlüssen waren wir dann aber leider nicht mehr beteiligt. Die datenschutzrechtlich erforderlichen Dokumente (Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DS-GVO, Vertrag zur Auftragsdatenverarbeitung nach Artikel 28 DS-GVO, Datenschutzerklärungen nach Artikel 13 DS-GVO) wurden uns in der Folge zwar auf unsere Nachfrage hin vom Kultusministerium übermittelt, eine Beratung jedoch nicht mehr gewünscht. Erst im weiteren Verlauf des Jahres 2021 änderte sich dies, und es wurden uns die überabeiteten datenschutzrechtlichen Unterlagen mit der Bitte um Beratung zugesandt, nun ergänzt um eine Datenschutz-Folgenabschätzung.

Nach Prüfung der Unterlagen sahen wir zwar noch datenschutzrechtliche Probleme, vor allem in Bezug zur zwar vertraglich ausgeschlossenen, aber dennoch stattfindenden Verarbeitung personenbezogener Daten in Drittsaaten, der Verarbeitung zu Zwecken von Auftragsverarbeitern und Prüfungen der technisch-organisatorischen Maßnahmen, hielten diese jedoch für überwindbar. Mit Schreiben vom 20. November 2021 haben wir vor diesem Hintergrund dem Ministerium mitgeteilt, dass wir zwar empfehlen, die aufgezeigten Probleme zunächst zu beheben, es aber angesichts der aktuellen pandemischen Situation auch für vertretbar hielten, den Dienst schon jetzt auszurollen, wenn die Probleme sodann zügig in Angriff genommen würden. Soweit sich die Probleme nur auf einzelne Werkzeuge beziehen, sollte in jedem Fall deren Freischaltung erst nach Behebung der Probleme erfolgen.

Das Kultusministerium ist dieser letzten Variante gefolgt und hat mit dem Ausrollen begonnen. Bei der ausgerollten Version war dabei – wie uns das Kultusministerium mitteilte – bereits eine wesentliche Verbesserung vorgenommen worden: Ursprünglich war nach den uns vorgelegten Unterlagen vorgesehen, dass für die Office-Anwendungen zunächst eine Microsoft Office Online-Version eingebunden werde, zu welcher der Support von Microsoft bereits eingestellt war (und die daher unter Umständen Sicherheitsrisiken hätte bergen können); erst im weiteren Verlauf sollte stattdessen ein Open-Source-Produkt implementiert werden. Erfreulicher Weise war diese Umstellung jedoch nach Bericht des Kultusministeriums bereits zu Beginn des Ausrollens erfolgt.

Identitäts- und Zugangsmanagement

Zum Identity and Access Managementsystem (IdAM), dem dritten Baustein der Digitalen Bildungsplattform, beraten wir das Kultusministerium schon seit Anfang 2020. In diesem System sollen jene personenbezogenen Daten abgelegt werden, welche für den Zugang zum System der Bildungsplattform und zu deren Komponenten erforderlich sind, d. h. Name, Vorname, Schule, Klasse, etc.

Da hier vor allem Daten abgelegt werden, um eine Person eindeutig zu identifizieren, und auch der Authentifizierungsmechanismus darüber gesteuert wird, ist neben der Festlegung der hier erforderlichen Datenarten auch die Sicherheit des technischen Systems besonders wichtig. Vor allem hier – aber auch für die weiteren Teile der Bildungsplattform – empfehlen wir deswegen dem Kultusministerium systematische Audits, IT-Sicherheitsanalysen und Penetrationstests durchführen zu lassen, bevor mit realen Daten gearbeitet wird.

Das Kultusministerium geht mit diesem Teil der digitalen Bildungsplattform derzeit in eine erste Pilotierung (noch ohne echte personenbezogene Daten). Auch hierbei und bei der weiteren Entwicklung des Identity and Access Managemenssystems werden wir das Ministerium weiter beraten.

Im Herbst 2021 hat mich das Kultusministerium gebeten, dem Lenkungskreis des Kultusministeriums zur Digitalen Bildungsplattform als regelmäßiges Mitglied beizutreten. Diese Aufgabe habe ich gerne angenommen. Dies wird den Informationsfluss und die Möglichkeiten der Zusammenarbeit zwischen Kultusministerium und meiner Behörde entscheidend verbessern. Auf diese Weise können wir noch unmittelbarer dem Kultusministerium unsere Unterstützung anbieten und die Zusammenarbeit erfolgreicher gestalten, um für die Schulen wesentliche und von ihnen dringend benötigte digitale Mittel datenschutzkonform zu entwickeln und bereitzustellen.

Für eine Übergangszeit bis zur Komplettierung der digitalen Bildungsplattform wurden uns von Seiten

des Landtages Ende 2021 dankenswerter Weise weitere Stellen bewilligt, um den Datenschutz an den Schulen deutlich zu stärken und insbesondere eine erhebliche Anzahl von Schulungen für Lehrkräfte, Schulleitungen, Datenschutzbeauftragte, Eltern und Schülervertretungen über unser Bildungszentrums Datenschutz und Informationsfreiheit Baden-Württemberg (BIDIB) anzubieten. Auch diese sinnvolle Aufgabe werden wir gerne übernehmen und die Schulen auf diese Weise bei der Bewältigung der datenschutzrechtlichen Herausforderungen, vor die sie sich nicht zuletzt wegen der rasant zunehmenden Digitalisierung im Schulbereich gestellt sehen, noch besser unterstützen. Wir danken zudem dem Kultusministerium für die nun etablierte sehr konstruktive und kooperative Zusammenarbeit in Bezug auf die Bildungsplattform.

Unsere Beratung rund um die digitale Bildungsplattform bringt noch einen weit darüber hinausgehenden Aspekt zutage: Während Projekte, die an externe Anbieter vergeben wurden, tendenziell besondere datenschutzrechtliche Herausforderungen mit sich bringen oder gar daran scheitern, sind diese Probleme bei den vom Land selbst betriebenen Diensten wie Moodle und BigBlueButton nicht festzustellen. Diese funktionieren insgesamt sehr zuverlässig und geräuschlos. Es ist daher empfehlenswert, mittel- und langfristig die eigenen Kompetenzen, Fähigkeiten und Möglichkeiten des Landes im Aufbau und Betrieb von IT-Infrastruktur weiter zu stärken.

Unsere Beratungen zur Digitalen Bildungsplattform werden andauern, damit die Schulen in Baden-Württemberg datenschutzkonforme Anwendungen erhalten. Das wird die Schulen sicherlich entlasten, damit sie sich ihren ureigenen Aufgaben der Erziehung und Bildung widmen können, ohne dabei die Rechte der Schüler_innen (und der weiteren am Schulbetrieb beteiligten Personen) auf informationelle Selbstbestimmung zu missachten.

Konkret und wirksam zu helfen nützt hier allen Beteiligten: Schulen können effektiv arbeiten, Eltern, Schüler- und Lehrerschaft erhalten Wissen und Unterstützung und können davon ausgehen, dass das Recht auf informationelle Selbstbestimmung bestmöglich gewahrt wird. Zugleich leisten wir unseren Beitrag dazu, dass an Schulen Fähigkeiten bei der Digitalisierung, IT-Sicherheit, Softwarekonfiguration und Anwendung intensiver eingeübt werden können. Für uns bedeutet dies, dass wir strukturiert und langfristig mehr Sicherheit und Expertise an den Schulen erkennen können und somit erfolgreich an der datenschutzkonformen Digitalisierung der Schulen mitwirken.

Die DS-GVO schützt die Verarbeitung von personenbezogenen Daten von Kindern besonders.

3. Proctoring

Studierende mussten in der Pandemie nahezu ihr gesamtes Unileben ändern. Kaum noch Treffen vor Ort, Lese- und Arbeitsgruppen sowie gemeinsame Prüfungsvorbereitungen verlagerten sich ins Digitale. Die Pandemie warf und wirft dabei auch im Bereich der Hochschulen neue datenschutzrechtliche Fragen auf. Eine besondere Fragestellung ergab sich für die Unis aus der Notwendigkeit, Prüfungen auch zu Zeiten anzubieten, in denen die Hochschulräume aus Gründen des Infektionsschutzes nicht oder nur in geringen Auslastungen betreten werden durften und damit Präsenzprüfungen nur noch sehr eingeschränkt zulässig waren.

Die Hochschulen gingen deswegen vermehrt dazu über, Online-Prüfungen unter Videoaufsicht durchzuführen. Dies bedingt erhebliche Eingriffe in das informationelle Selbstbestimmungsrecht der Prüfungskandidat_innen. Hierzu hat der Landesgesetzgeber eine gesetzliche Grundlage geschaffen, bei deren Anwendung und Auslegung das Ziel, einen angemessenen Ausgleich zwischen dem Schutz des Grundrechts auf informationelle Selbstbestimmung und der Verhinderung von Täuschungsversuchen herzustellen, im Auge zu behalten ist.

Vor dem Hintergrund der eingeschränkten Möglichkeiten zur Abhaltung von Prüfungen in Präsenz hatte der Landesgesetzgeber bereits Ende des Jahres 2020 die Notwendigkeit erkannt, die Zulässigkeit von Online-Prüfungen gesetzlich zu regeln. Dank der kooperativen Vermittlung des Wissenschaftsministeriums hatten wir bei der Formulierung der diesbezüglichen Regelungen in den neu eingefügten § 32a und § 32b des Landeshochschulgesetzes datenschutzrechtliche Aspekte einbringen können. Damit stand den Hochschulen seit Anfang des Jahres eine gesetzliche Grundlage zur Verarbeitung von Daten der Studierenden im Rahmen von Online-Prüfungen zur Verfügung. Auf die zuvor teilweise in Anspruch genommene, aber letztlich (u. a. wegen ihrer Widerruflichkeit) wenig passende datenschutzrechtliche „Krücke", die Datenverarbeitung bei Online-Prüfungen auf eine Einwilligung der Prüflinge zu stützen, waren die Hochschulen seitdem nicht mehr angewiesen.

Gleichwohl erhielten wir noch in der Folgezeit Hinweise und Beschwerden, dass von den Hochschulen mitunter Software und Prüfungsregeln angewandt würden, die zu sehr in die Rechte von Studierenden eingreifen würden.

Das nahmen wir zum Anlass, Online-Prüfungen an Hochschulen im Land in tatsächlicher und rechtlicher Hinsicht näher zu betrachten. Wir unternahmen eine Rundfrage unter den staatlichen Hochschulen, in welcher Form sie Onlineprüfungen durchführen. Außerdem sprachen wir mit Betroffenen, Hochschulvertretungen, Vertretungen des Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg sowie Softwareanbietenden und machten in der öffentlichen Diskussion auf die Gefahr zu weitgehender Eingriffe in die Privatsphäre der Studierenden aufmerksam.

Präsenzprüfungen und Online-Prüfungen bieten jeweils andere Möglichkeiten, die Studierenden zu kontrollieren. Beispielsweise ist es etwas anderes, ob die Aufsicht im Prüfungssaal Studierende überwacht oder ob eine Software – unter Umständen auch unter Einsatz sogenannter „Künstlicher Intelligenz" (KI) – die/den einzelne_n Studierenden über eine Webcam direkt in die Augen sieht und im Zweifel jede Regung wahrnehmen und auswerten kann. Auch gewährt die Online-Prüfung unter Videoaufsicht – je nach ihrer Ausgestaltung – unter Umständen tiefe Einblicke in die Wohnung und Privatsphäre der Prüfungskandidatinnen und -kandidaten, die sie im Falle einer Prüfung vor Ort nicht nehmen könnte. Hier gilt es, auf der Basis der rechtlichen Grundlage einen angemessenen Ausgleich herzustellen zwischen dem prüfungsrechtlichen Ziel der Vermeidung von Täuschungshandlungen und dem Recht auf informationelle Selbstbestimmung der Studierenden.

Dies hat uns veranlasst, eine Handreichung zur Durchführung von Online-Prüfungen an Hochschulen herauszugeben. Sie dient Hochschulen und Studierenden und setzt auf Grundlage des novellierten Landes-Hochschulgesetzes einen neuen Standard. Die Handreichung bezieht sich auf die einschlägigen rechtlichen Grundlagen und nennt übersichtlich Eckpunkte, die wir auf der Grundlage der genannten Gespräche mit Studierenden, Hochschulvertretungen, Softwareanbietenden und dem Wissenschaftsministerium sowie der bei uns eingegangenen Beschwerden und der Hochschulumfrage entwickelt haben.

Die Handreichung soll dazu beitragen, dass einerseits Studierende sich nicht – etwa unter dem Druck, ihren Abschluss auch in der Pandemie zeitnah zu erreichen – Online-Prüfungen unterziehen, die datenschutzrechtlich unzulässig sind, etwa weil sie Studierende durch technische Tools dauerhaft kontrollieren oder zu stark in die räumliche und technische Privatsphäre der Studierenden eingreifen. Studierende müssen ihre Rechte nicht aufgeben, um zeitnah an einer Prüfung teilnehmen zu können. Andererseits ist nachvollziehbar, dass die Hochschulen, auch bei Online-Prüfungen Betrugsversuche unterbinden müssen; Online-Prüfungen stehen, ebenso wie Präsenzprüfungen, unter dem Gebot der Chancengleichheit und Fairness.

Einige Punkte der Handreichung: Aufzeichnungen und Screenshots von Prüfungen oder Teilen hiervon sind unzulässig. Hochschulen dürfen nicht verlangen, dass Studierende ihre Kamera zur Kontrolle durch ihren Privatraum schwenken, in dem sie die Online-Prüfung ablegen. Der „Denkprozess" der Studierenden – der auch ihre Textentwürfe umfasst – soll geschützt bleiben. Jede individuelle Überwachungsmaßnahme, zum Beispiel das Aufrufen eines Einzelbildes eines Studierenden, muss diesem auch optisch angezeigt werden. Besonders eingriffsintensive Tools von Videokonferenz-Systemen, wie das Aufmerksamkeits-Tracking und Tracking von Augen-, Kopf- und Körperbewegungen sind nicht erlaubt. Die Videoaufsicht selbst ist zulässig. Der Einsatz von Software, die den Rechner des Prüflings scannt und unverhältnismäßig in die Vertraulichkeit und Integrität dieses IT-Systems eingreift, ist allerdings unzulässig.

>> Mehr Informationen:

Handreichung des LfDI zu online-Prüfungen an Hochschulen: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/07/20210715_Handreichung-Online-Pruefungen.pdf <<

Wir stehen mit Hochschulen, den Studierenden und ihren Vertretungen sowie dem Wissenschaftsministerium weiterhin im Gespräch und beraten bei der Suche nach passgenauen, datenschutzkonformen Lösungen. Denn die gesetzliche Rechtsgrundlage ist zwar aufgrund der besonderen Herausforderungen während der pandemischen Verhältnisse geschaffen worden; ihre Anwendbarkeit ist aber nicht auf die Zeit der Pandemie begrenzt. Es ist vielmehr davon auszugehen, dass die Hochschulen auch darüber hinaus Online-Prüfungen anbieten und durchführen werden. Aus unseren gemeinsamen Gesprächen haben wir den Eindruck gewonnen, dass die Notwendigkeit der datenschutzkonformen Nutzung von Software bei den Verantwortlichen anerkannt ist. Im weiteren Verlauf werden wir auch auf Beschwerden eingehen und wenn nötig stichprobenartige Kontrollen vornehmen.

© bongkarn – stock.adobe.com

Die Rechte der Studierenden müssen auch bei Online-Prüfungen gewahrt werden.

4. Videokonferenzsysteme datenschutzkonform betreiben

Seit Beginn der Pandemie sind Videokonferenzdienste und andere Online-Kommunikationsdienste stark nachgefragt. Verantwortliche fragen sich und uns häufig, ob ein bestimmter Dienst datenschutzkonform eingesetzt werden kann und was beachtet werden muss.

Aus diesem Grund haben wir im Sommer und Herbst 2021 eine umfangreiche Handreichung zum Thema Videokonferenzsysteme erstellt und im Oktober veröffentlicht, in der sieben Videokonferenzsysteme sowohl rechtlich als auch technisch untersucht und beschrieben werden: Alfaview, BigBlueButton, Cisco WebEx, GoToMeeting, Jitsi, MS Teams und Zoom. In einer Übersicht listen wir auf, worauf zu achten ist, wenn man ein Videokonferenzsystem nutzt – datenschutzrechtlich und technisch. Zugleich gibt sie Hinweise zu verbreiteten Videokonferenzsystemen. Diese Handreichung mit übersichtlicher Tabelle steht nun zum Download auf der Homepage des Landesbeauftragten bereit. Dabei können wir keine detaillierten Hinweise zu allen möglichen Konfigurationen und Vertragsgestaltungen geben – aber dabei helfen, das passende System zu finden und einzurichten. Denn die richtige Software-Einstellung kann oftmals bereits entscheidend helfen, datenschutzrechtliche Risiken zu reduzieren. Und es nützt natürlich, sich etwas ausführlicher über den passenden Anbieter für die eigenen Zwecke und über die richtige Konfiguration Gedanken zu machen.

Schwierigkeiten bereitet bei einigen Diensten, dass diese personenbezogene Daten zu eigenen Zwecken verwenden. Denn eine Verwendung personenbezogener Daten der Nutzenden zu eigenen Zwecken des Anbieters schließt den Einsatz eines Videokonferenzsystems im öffentlichen Dienst (insbesondere an Schulen) aus. Die neben einer Einwilligung nach Artikel 6 Absatz 1 Buchstabe a DS-GVO, welche nach Erwägungsgrund 43 gegenüber Behörden grundsätzlich nicht freiwillig abgegeben werden kann, einzig verbleibende Rechtsgrundlage des berechtigten Interesses nach Artikel 6 Absatz 1 Buchstabe f DS-GVO ist für Behörden nicht einschlägig (vgl. Artikel 6 Absatz 1 Satz 2 DS-GVO). Der datenschutzrechtlich Verantwortliche im Sinne von Artikel 4 Nr. 7 DS- GVO hat grundsätzlich drei

>> Mehr Informationen:

Handreichung des LfDI zu Videokonferenzsystemen: https://www.baden-wuerttemberg.datenschutz.de/videokonferenzsysteme/ <<

Möglichkeiten, ein Videokonferenzsystem (VKS) zu betreiben: Entweder er betreibt das System auf Basis eigener Infrastruktur und Software vollständig selbst, oder er greift dabei auf einen Dritten zurück, der die Videokonferenz (VK) als externer IT-Dienstleister mitsamt Hard- und/oder Software anbietet. Aktuell greifen die meisten Verantwortlichen auf die dritte Möglichkeit, einen Online-Dienst (Software as a Service) zurück. Diese Fallgestaltung untersucht die Handreichung näher und gibt Empfehlungen zu den einschlägigen rechtlichen und technischen Fragestellungen.

Bestehen aus Sicht des Verantwortlichen besondere Anforderungen an das Videokonferenzsystem, etwa wegen der besonderen Sensibilität der verarbeiteten Daten (z. B. bei der Verarbeitung von besonderen Kategorien personenbezogener Daten nach Artikel 9 DS-GVO oder bei Sicherheitsbehörden) oder der besonderen Schutzbedürftigkeit der Nutzer_innen (z. B. im Schulbereich), so wird das selbst (ggf. auf Basis von Open Source Software wie BigBlueButton oder Jitsi) oder von einem sorgsam ausgewählten IT-Dienstleister betriebene Videokonferenzsystem vorzugswürdig oder sogar alternativlos sein.

5. Ohne Datenschutz und IT-Sicherheit schließt der Fortschritt Bürger_innen aus

Auch 2021 hat sich der Trend zu immer mehr und immer schwereren IT-Sicherheitsvorfällen fortgesetzt. Was sich anhört, als ob Naturkatastrophen ohne Möglichkeit der Kontrolle hereinbrechen, ist oftmals ein Prozess, der als Folge von mangelnder IT-Sicherheit und fehlendem Sicherheitsbewusstsein entsteht.

2021 haben uns mehrere schwere und breitflächige IT-Sicherheits-Vorfälle, bei denen viele Verantwortliche betroffen waren, beschäftigt. Diese gingen mit einer hohen Zahl an Meldungen von Verletzungen des Schutzes personenbezogener Daten nach Artikel 33 DS-GVO (sogenannte Datenpannen-Meldungen) einher.

So wurde im März eine Sicherheitslücke in Microsoft Exchange bekannt, mit der Angreifer_innen beliebigen Code auf ungesicherten Systemen ausführen und so z. B. Daten auslesen konnten. Selbst wer die Sicherheitsupdates von Microsoft frühzeitig eingespielt hat, konnte betroffen sein. Die Lücke erreichte eine große Aufmerksamkeit, was es umso erstaunlicher macht, dass einige Verantwortlichen ihre Systeme erst mit mehrwöchiger Verzögerung aktualisiert haben. Im Dezember 2021 wurde in der häufig verwendeten Komponente log4j für die Programmiersprache Java eine schwerwiegende Sicherheitslücke bekannt, die ebenso für das Ausführen von beliebigem Code genutzt werden kann. Da zahlreiche Softwares log4j nutzen und eine Aktualisierung nicht immer ganz einfach ist, ist in der Folge mit zahlreichen Datenpannen bis ins Jahr 2022 hinein zu rechnen.

Daneben gab es tagtäglich zig Meldungen über Angriffe von diversen Ransomware-Gangs mit Verschlüsselungstrojanern. Da betroffene Unternehmen immer häufiger Backups vorhalten und zurückspielen, verlegen sich die Angreifer auf ein zweites Standbein ihres Geschäftsmodells: Sie kopieren in großem Stil Daten und drohen, diese zu veröffentlichen. Betroffene Personen sind oftmals Kunden, Geschäftspartner_innen, Patient_innen oder Mandant_innen der angegriffenen Unternehmen – oder alle Bürger_innen, wenn Behörden und öffentliche Stellen angegriffen wurden. Diese haben dann kaum noch Möglichkeiten, sich zu schützen und können nur die Folgen eindämmen – die je nach Art der Daten unterschiedlich sein können. Die meisten Vorfälle haben gezeigt, dass bereits wenige einfache Maßnahmen das Risiko, Opfer eines großflächigen Angriffs zu werden, deutlich reduzieren können:

1. Sicherheitsupdates müssen schnell eingespielt werden, um ein häufiges Einfallstor zu schließen.

2. Es müssen Maßnahmen ergriffen werden, um im Falle eines erfolgreichen Angriffs mit einer zweiten Verteidigungslinie den Schaden zu minimieren – zum Beispiel indem verschiedene interne Dienste voneinander abgeschottet sind und das Backup nicht an der gleichen zentralen Authentifizierung hängt.

3. Interne Dienste sollten möglichst nicht von außen erreichbar sein, sondern via VPN, mit Client-Zertifikaten oder auf bestimmte IP-Bereiche beschränkt.

4. Fernwartungssysteme aller Art müssen besonders gut abgesichert werden.

5. Das Deaktivieren von Office-Makros verhindert eine häufige Angriffsmethode. Sollten Makros unbedingt notwendig sein, sollten ausschließlich von einer vertrauenswürdigen Instanz signierte Makros erlaubt sein.

6. Bei der Nutzung von Cloud-Diensten sollte eine Zwei-Faktor-Authentifizierung (2FA) genutzt werden, um das Risiko für das Abgreifen von Passwörtern zu reduzieren. Es gab 2021 aber auch zahlreiche Berichte darüber, dass Angreifer_innen auch diese Hürde genommen haben.

Die Liste ist nicht vollständig, sondern führt einige der am häufigsten fehlenden Maßnahmen mit hohem Risiko auf. Verantwortliche sind aufgerufen, dringend mehr Wert auf IT-Sicherheit zu legen. Die Exchange-Lücke zu Beginn des Jahres und die Sicherheitslücke Ende des Jahres in der häufig verwendeten Komponente log4j haben in der öffentlichen Diskussion nicht nur in einschlägigen Fachzeitschriften oder netzpolitisch fokussieren Portalen viel Raum eingenommen – was ihrer Relevanz endlich gerecht wird. Die Themen rutschen immer häufiger aus den Technik-Ressorts „nach vorne“, und das völlig zu recht. Privatpersonen, Unternehmen und Behörden müssen sich im eigenen Interesse und im Interesse ihrer Kund_innen und Bürger_innen intensiver mit dem Schutz ihrer Daten und ihrer IT-Infrastruktur befassen. Eine 100-prozentige Sicherheit wird es nicht geben, aber sie kommen nicht aus dem Nichts. Man muss nach einem Angriff nicht verzweifelt sein, man muss reagieren können. Man kann das Sicherheitsniveau erhöhen, man kann mehr investieren in Expert_innen, die sich mit IT-Sicherheit auskennen und die dieses vermeintliche #Neuland besser verstehen als andere.

Es ist ein bedauernswerter Zustand, wenn von einem Datenklau betroffenen Personen nur noch mitgeteilt werden kann, dass neben einer Anzeige bei der Polizei, sie spätere Schäden durch einen Identitätsdiebstahl beziehungsweise die Bestellung von Waren Dritter unter falschem Namen (d. h. der betroffenen Person) vermutlich unumgänglich ins Auge blicken müssen und Löschungen auf einschlägigen Webseiten (z. B. im Darknet) vermutlich wenig Aussicht auf Erfolg haben. Nun könnte

man meinen, dass es in der heutigen Zeit längerfristig, angesichts einer stetig wachsenden Zahl von Datenlecks und nicht ausreichender IT-Sicherheit, wohl absehbar wäre, dass jeder von Datenlecks betroffen sein wird.

Auf https://sec.hpi.de/ilc/ und https://haveibeenpwned.com/PwnedWebsites finden betroffene Personen bei der Prüfung ihrer E-Mailadresse häufig unerwartet nicht nur über eine, sondern gleich mehrere Datenpannen, von der sie betroffen sind. Es ist nicht schwierig oder gar einer/einem Privatnutzenden tatsächlich vorzuwerfen, Opfer einer missbräuchlichen Erhebung zu werden, denn für Angreifer_innen bieten sich zahlreiche Gelegenheiten.

Hierzu gehört es auch zu betrachten, dass bestimmte Formen der digitalen Kommunikation anfälliger sind für Angriffe, andere weniger. An einzelnen Beispielen soll dies verdeutlicht werden. In E-Mails von großen Handels- oder Finanzplattformen werden Themen gerne „angeteasert". Sie bieten über große Buttons dann den Verweis auf ihre Webseite und bieten einen notwendigen Login an. Das ist mittlerweile gewöhnlich. Ein_e Angreifer_in kann diese Gewohnheit auch ausnutzen um täuschungsähnliche E-Mails zu versenden, die Links enthalten.

Häufig haben wir 2021 im Rahmen von Art. 33 DS-GVO Meldungen von Verantwortlichen über Datenpannen in Form von erfolgreichen Phishing-Angriffen erhalten, in der Nutzer so z. B. zur Eingabe ihrer Zugangsdaten auf der täuschungsähnlichen Webseite der/des Angreiferin/Angreifers verleitet wurden und so Angreifer_innen über die abgefangenen Zugangsdaten Zugriff auf Systeme des Arbeitsgebers erhalten haben. Dabei handelt es sich häufig um Webseiten mit der Mitarbeiter Zugriff auf E-Mails, Kalender und Kontakte erhalten sollen (und in denen häufig auch sensible Daten verarbeitet werden). Müssen deshalb Links in E-Mails verboten werden? Nein, aber es ist so derzeit unklar, wie allein Schulungen bei täuschungsähnlichen E-Mails helfen sollen, Anmeldedialoge auf gefälschten Webseiten von den richtigen zu unterscheiden. Hier fehlt es an technischen Mitteln und Knowhow, die das Risiko minimieren können. Auch auf gefälschte Jobannoncen wurden wir in der Vergangenheit hingewiesen, die über täuschungsechte, professionell wirkende Webseiten für eine Bewerbung zu einem Hochladen des eigenen Personalausweises verleitet haben und bei der selbst die Angabe im Impressum auf eine nicht beteiligte Person verwiesen hatte. Manche Menschen bekommen erst mit, dass Unbefugte Zugriff auf ihre Daten genommen haben, wenn sie über die nach Art. 34 DS-GVO erforderliche Meldung des Verantwortlichen über eine Verletzung des Schutzes personenbezogenen Daten bei hohem Risiko von einer Datenpanne informiert werden. Dies ist etwa vorgekommen bei einer Beschäftigten die zur Beantragung von Elternzeit bei einem Arbeitgeber eine Geburtsurkunde und weitere Informationen einreichen musste und diese bei dem Arbeitgebenden bei einem großangelegten Angriff auf seine IT-Systeme mutmaßlich kopiert wurden.

Wir mussten auch sehen, dass Telefonnummern, die nur als Zwei-Faktor-Authentifizierung angefragt worden waren, bei einer großen Social-Media-Plattform Angreifer_innen zugänglich wurde. Dies hat im Jahr 2021 die neue Angriffsform „Smishing" beflügelt. Hierbei werden betroffenen Personen regelmäßig per SMS-Links zu angeblichen Sendungsverfolgungen, angeblich wartenden Sprachnachrichten oder angeblichen Bestellbestätigungen beschert, die im nächsten Schritt, durch Telefonanrufe oder in gleicher Weise wie bei Phishing Personen in das Unglück führen.

Betroffenen Personen kann in diesem Fall nur empfohlen werden, ggf. bei der Bundesnetzagentur die Absender_innen zu melden und – sofern man nur Mitteilungen von bekannten Rufnummern erhält – im Smartphone einen Filter für unbekannte Rufnummern zu aktivieren und ansonsten einen ruhigen Finger zu bewahren. Durch einen Klick auf den individualisierten Link wird den Angreifer_innen zumindest bekannt, dass die Rufnummer aktiv genutzt wird und der Aufruf der Webseite kann möglicherweise problematisch sein kann. Die Täuschungs- und Angriffsmöglichkeiten sind vielfältig. Wir beraten und weisen als Aufsichtsbehörde verantwortliche Stellen darauf hin, geeignete technische und organisatorische Maßnahmen einzusetzen. Wir haben auch verschiedene Publikationen zum Thema, z. B. zum sicheren Umgang mit Passwörtern veröffentlicht. Verantwortliche Stellen müssen für die Verarbeitung personenbezogener Daten nach Art. 5 Abs. 1 lit. f, Art. 24ff., Art. 32 DS-GVO geeignete technische und organisatorische Maßnahmen treffen. Diese müssen so beschaffen

sein, dass der Verantwortliche für das Risiko durch die Verarbeitung personenbezogenen Daten für die Rechte und Freiheiten betroffener Personen ein dem Risiko angemessenes Schutzniveau gewährleistet. Das BSI bietet verschiedene praktische Tipps für Verbraucher_innen. Auch Verbraucherzentralen informieren zum Thema Identitätsdiebstahl. Die Polizei informiert auf verschiedenen Webseiten über das Phänomen Identitätsdiebstahl/Phishing. Es kann nach unserem Verständnis für betroffene Personen hilfreich sein, durch eine Anzeige bei der Polizei den Vorgang zu dokumentieren, z. B. um später, bei einer Bestellung durch Dritte unter falschem Namen einen Nachweis zu haben und die Diskussion mit dem Versandhändler hinsichtlich der unberechtigten Forderung möglicherweise abzukürzen.

>> Mehr Informationen:

Bericht auf wired.com vom 4.6.2021 „What Really Caused Facebook's 500M-User Data Leak?": https://www.wired.com/story/facebook-data-leak-500-million-users-phone-numbers/

LfDI-Hinweise zum Umgang mit Passwörtern: https://www.baden-wuerttemberg.datenschutz.de/hinweise-zum-umgang-mit-passwoertern/

Bundesamt für Sicherheit in der Informationstechnik (BSI): „‚Smishing' – SMS-Phishing im Herbst 2021 mit neuen Betrugsmaschen": https://www.bsi.bund.de/DE/Home/home_node.html;jsessionid=499148A1B3B5506B08C01B7BC9D81645.internet482

Bundesnetzagentur: „Ärger mit Rufnummern und Anrufen": https://www.bundesnetzagentur.de/DE/Home/home_node.html;jsessionid=6EC2B6C7DDED4CCBB3B5A3964B230E0D

„Blockieren, Filtern und Melden von Nachrichten auf dem iPhone": https://support.apple.com/de-de/guide/iphone/iph203ab0be4/ios

Bundesamt für Sicherheit in der Informationstechnik (BSI): Verbraucherinnen und Verbraucher: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/verbraucherinnen-und-verbraucher_node.html

Identitätsdiebstahl
Verbraucherzentrale Baden-Württemberg: https://www.verbraucherzentrale-bawue.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750

Polizeiliche Kriminalprävention der Länder und des Bundes: https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing/

Bundeskriminalamt: https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/ECSM/ecsm_node.html <<

Sicherlich hilft es, digitale Kompetenzen der Technik-Nutzenden zu fördern, um digitale Angriffe zu verteidigen. Wir beraten Betroffene nach Möglichkeit immer sehr gerne, wir organisieren Veranstaltungen, um über Digitalisierung zu sprechen. Es gehört aber dazu, dass Verantwortliche in ihrem Bereich, wo sie dies zu entscheiden haben, Wert auf höhere Sicherheitsstandards legen. Ansonsten verharrt Digitalisierung als ökonomische Technik und Möglichkeit für Dritte, Menschen zu attackieren und im Zweifel zu schädigen. Der Schutz der personenbezogenen Daten und IT-Sicherheit sind die notwendigen Voraussetzungen dafür, dass sich Menschen im digitalen Zeitalter unter Wahrung ihrer Bürgerrechte bewegen können. Die Anstrengung, mehr für IT-Sicherheit zu tun und datenschutzrechtliche Vorgaben zu beachten, wird künftig nötig sein, und diese Anstrengung dauerhaft zu leisten sein. Auf Landesebene leistet hier die jüngst gegründete Cybersicherheitsagentur Baden-Württemberg (CSBW) ihren Beitrag, gerne auch im Austausch mit uns.

Ein Wesenskern des technischen Fortschritts ist es, dass das er sehr schnell voranschreitet und man stets versuchen sollte, auf der Höhe der Zeit zu sein, um seine Systeme bestmöglich im Griff zu haben. Um dafür ein Selbstverständnis zu entwickeln, verstehen wir Digitalisierung als eine Kulturtechnik. Das meint, dass wir als Gemeinschaft die kulturelle Praxis des digitalen Zusammenlebens praktizieren. Der Chaos Computer Club und andere Organisationen haben seit den 80er Jahren schon sehr viel dazu beigetragen, dass wir von der Technik mehr verstehen. Dennoch braucht es mehr Zeit und Willen, Digitalisierung gesellschaftlich so zu verankern, dass sie als kulturelle Praxis eingeübt ist und Menschen Wissen zur Verfügung haben, was der Technikeinsatz für Folgen haben kann.

6. Bildungszentrum – Ein Forum für Datenschutz und Informationsfreiheit wächst, gedeiht und erfreut sich großer Nachfrage

Mit Vorfreude blickten wir Ende 2020 wenige Monate nach Gründung des Bildungszentrums auf das neue Jahr. Nach der Gründungsphase hatten wir uns für die Aufbauphase im Jahr 2021 viel vorgenommen. Vor allem freuten wir uns darauf, Gäste und Teilnehmende bei uns vor Ort in Präsenz begrüßen zu dürfen. Erwartungsvoll blickten wir auch auf den für Sommer vorgesehenen Umzug in ein anderes Gebäude mit eigenen Seminarräumen und entsprechender Ausstattung und Technik sowie die damit verbundenen neuen Möglichkeiten. Jedoch wurde der Verlauf des Jahres dann stark von der Corona-Pandemie geprägt. Dies erforderte eine größere Flexibilität und verursachte einen deutlich erhöhten Aufwand, um Veranstaltungen zumindest in digitaler Form anbieten zu können.

In den ersten Monaten konnten wir Veranstaltungen zunächst nur online durchführen. Im Juli erfolgte dann der lang erwartet Umzug in neue Räumlichkeiten. Damit kamen wir unserem Ziel näher, sowohl ein digitaler wie auch ein Treffpunkt in Präsenz zu sein, an dem man sich über alle Aspekte von Datenschutz und Informationsfreiheit austauschen kann. Auch die Corona-Lage stellte sich kurzzeitig deutlich besser dar. Doch die pandemische Entwicklung erlaubte es nicht allzu lange, das Bildungszentrum für Interessierte vor Ort offen zu halten. Schließlich musste den erneut steigenden Corona-Fallzahlen Tribut gezollt und zu unserem Bedauern wie im Jahr davor auf reine Online-Veranstaltungen umstellt werden.

Trotz widriger Umstände konnten wir im Jahr 2021 – dem ersten vollständigen Bildungsjahr seit Bestehen – mehr als 50 Veranstaltungen durchführen. Dies schließt auch solche Veranstaltungen ein, die nicht öffentlich ausgeschrieben wurden. Das sind insbesondere Veranstaltungen, die ausschließlich für anfragende Stellen (Inhouse-Schulungen) oder mit Blick auf Seminarinhalte und Zielgruppe nur für bestimmte Bereiche angeboten wurden, wie etwa Schulungen für Polizeibehörden. Das Interesse an den Angeboten des Bildungszentrums war in aller Regel groß. Insgesamt haben sich zu allen Veranstaltungen über 2.000 Interessierte angemeldet.

Darüber hinaus haben wir zahlreiche Videos rund um Datenschutz und Informationsfreiheit erstellt. Sie sind in aller Regel in unserer Mediathek abrufbar. Einzelne Medien sind integraler Bestandteil von Veranstaltungen und daher nur bei einer Anmeldung zu diesen zugänglich.

Bildungszentrum für Datenschutz und Informationsfreiheit (BIDIB)

Reges Interesse an Veranstaltungen

Für klein- und mittelständige Unternehmen haben wir unter anderem Veranstaltungen angeboten, die vermittelten, was bei der Erstellung einer Datenschutz-Folgenabschätzung und beim Umgang mit Datenpannen zu beachten ist und wie durch organisatorische und technische Maßnahmen Bußgelder vermieden werden können. Zudem haben wir gemeinsam mit der IHK Region Stuttgart eine Veranstaltung durchgeführt, die sich kritisch mit der DS-GVO auseinandergesetzt hat und bei der von Referierenden unserer Dienststelle Tipps und Hinweise zu unterschiedlichen Themen für die unternehmerische Praxis gegeben wurden. Diese erfolgreiche Kooperation möchten wir weiterführen und noch mehr Unternehmer_innen und Verantwortliche in den Betrieben beraten und auch hören, wo es in der alltäglichen Praxis hakt, um passgenaue Angebote wie digitale Tools, Handreichungen und Schulungen anzubieten. Unser Programm umfasste im Jahr 2021 auch mehrere Veranstaltungen für Vereine. Zum einen ging es hierbei allgemein um Grundlagen des Datenschutzrechts im Vereinswesen. Zum anderen wurde das LfDI-Tool „DS-GVO. clever“ vorgestellt und aufgezeigt, wie die meisten Vereine mit diesem Programm ihrer rechtlichen Informationspflicht recht einfach nachkommen können, wenn sie personenbezogene Daten verarbeiten. Das Tool wurde im Laufe des Jahres um eine Version für kleine Unternehmen, Gewerbetreibende und Handwerksbetriebe erweitert und in der Folge auch für diese Zielgruppe entsprechende Schulungen angeboten. Das Tool steht auf der Homepage des Landesbeauftragten bereit und erfreut sich bundesweit einiger Beliebtheit.

Für Interessierte aus dem kommunalen Bereich gab es die Möglichkeit, an Veranstaltungen zum datenschutzgerechten Umgang mit sozialen Netzwerken, dem Datenschutz im Baurecht oder den Anwendungsbereichen von DS-GVO und JI-Richtlinie sowie dem Beschäftigtendatenschutz teilzunehmen. Auch die Veranstaltungen zum Umgang mit Datenpannen und der Erstellung von Datenpannenmeldungen standen den Kommunen offen.

Veranstaltungen, die wir nicht öffentlich ausgeschrieben haben, sind etwa Seminare zur Videoüberwachung im privaten Bereich für Polizeibehörden oder eine Schulungsreihe für alle Jugendmannschaften des VfB-Nachwuchsleis-

© LfDI BW

Pandemiebedingt konnte die erste BIDIB-Ausstellung nicht vor Ort stattfinden. Nach schneller Umplanung stand ein paar Tage später ein zweiteiliges Ausstellungsvideo online.

tungszentrums einschließlich der Teilnahme an einem Elternabend.

Für die interessierte Öffentlichkeit gab es die Möglichkeit, an einer Veranstaltung teilzunehmen, die sich mit der Frage auseinandergesetzt hat, was Freiheit in einer digitalen Gesellschaft bedeutet. In einer weiteren Veranstaltung wurde über den Umgang mit Messenger-Diensten aus Sicht des Datenschutzes informiert. Zudem haben wir erstmalig eine Ausstellung mit einer eigens dafür konzipierten Veranstaltungsreihe in unserer Dienststelle organisiert. Die Ausstellung und die Veranstaltungen befassten sich mit Olympiateilnehmenden aus der ehemaligen DDR und Leistungssportler_innen im Allgemeinen.

Mit der Ausstellung und den begleitenden Veranstaltungen haben wir die Erfolge von zum Teil vergessenen Sportheld_innen gewürdigt und zugleich die Art und Weise hinterfragt, wie an sie erinnert wird. Als Aufsichtsbehörde, die sich für die Belange von Freiheits- und Bürgerrechten stark macht, haben wir uns intensiv mit der innerdeutschen Sportgeschichte, Persönlichkeitsrechten von Leistungssportler_innen und den aktuellen Entwicklungen im Sportbereich auseinandergesetzt.

Eine Ausstellung zu organisieren war für uns neu. Wie kamen wir dazu? So einfach wie idealtypisch wünschenswert: Ein Mitarbeitender unserer Dienststelle hatte diese Idee. Er hat erfreulicherweise auch vorgeschlagen, diese Idee einmal auszuformulieren. Einige Kolleg_innen haben sich dazugesetzt, unser Bildungszentrum hat seine Erfahrung in die Veranstaltungsorganisation eingebracht und alsbald stand das Programm – eines, dass weniger juristisch ausgerichtet, dafür aber sehr konkret und praktisch ausgestaltet wurde und somit niederschwellig war. Wir konnten am Beispiel der Spitzensportler_innen der Frage nachgehen, wie viel Freiheit man von sich preisgeben muss, um seiner Leidenschaft zu folgen. Hier sind unmittelbar datenschutzrechtliche Aspekte und etwa die freie Ausübung des Berufs tangiert: Olympiateilnehmende unterschreiben Verträge, die teilweise festlegen, welchen Arzt man zu konsultieren habe, dass man sich nicht politisch äußern darf bei Olympia, und dass man bestimmte Sponsoren bewerben muss. Zugleich wird über den Gesundheitszustand eines Sportstars öffentlich diskutiert, ob er oder sie will oder nicht.

Als Spitzensportler wird man auch Teil des Anti-Doping-Systems, welches extrem auf Kontrolle ausgelegt ist. Die Teilnahme am Anti-Doping-System ist für Spitzensportler_innen Voraussetzung für die Ausübung ihres Berufes. Sie geben für ein Kontrollsystem viel von sich preis, und ertragen eine lückenlose Kontrolle durch die Nationale Anti-Doping Agentur Deutschland (NADA). Und sie – nicht etwa die NADA – müssen, sobald eine erste Probe positiv ausfällt, beweisen, dass sie nicht gedopt haben. Oftmals beginnen dann auch die öffentliche mediale Auseinandersetzung und die Diskussion über den Fitness-Zustand und die Gesundheit der Betroffenen.

Leistungssport ist beliebt, wirkt in den Breitensport hinein und viele Menschen haben eine Meinung zu Sportler_innen. Wir haben die Gelegenheit genutzt, um gerade in einem so viel beachten Bereich wie dem Sport für Themen des Datenschutzes zu sensibilisieren und inhaltlich zu diskutieren.

Aufgrund der Corona-Lage mussten wir vorgesehenen Führungen durch die Ausstellung letztlich auf ein zweiteiliges Video begrenzen, welches in der Mediathek steht, und das reduzierte Veranstaltungsprogramm online streamen. Aber wir werden ausgefallene Veranstaltungen im Jahr 2022 nachholen.

Mehr Hybridveranstaltungen

Wir haben bei der Umstellung unseres Veranstaltungsangebots auf Online- beziehungsweise Hybridveranstaltungen darauf geachtet, dass wir künftig konsequent digitale Formate anbieten können. Wir sehen beides nicht als Zwischenlösung in Zeiten der Pandemie. Auch nach der Pandemie – wann immer das sein wird, hoffentlich bald – wird es nach unserer Einschätzung dabei bleiben, dass viele Menschen die digitalen Möglichkeiten des Zusammenkommens nutzen werden.

Wir mussten uns technisch für Online- und Hybridveranstaltungen neu ausrichten. Inhaltlich haben wir unsere Formate versucht, interaktiver zu gestalten. Wir sind noch nicht am Ende dieser Entwicklung, wir lernen weiter, wie wir möglichst vielen online-Interessierten künftig noch passendere Angebote machen können. Online-Angebote bieten für uns zudem die Möglichkeit, weiter in die Fläche zu kommen.

Im Jahr 2021 starteten wir mit einer zweiteiligen Schulungsreihe zu Grundlagen der Informationsfreiheit. Im ersten Teil können sich Interessierte im Selbststudium anhand von verschiedenen Videos grundlegendes Wissen aneignen. Im zweiten Teil werden in Veranstaltungen Fragen von Teilnehmenden erörtert, aktuelle Entwicklungen aufgegriffen und einzelne Punkte vertieft. Dieses Format wird bislang gut angenommen und soll im Jahr 2022 auch für den Datenschutzbereich umgesetzt werden. Zunächst sollen Module zu grundlegenden Themen wie Rechtsgrundlagen, Informationspflichten oder Betroffenenrechte erstellt werden. Dann wird das Angebot sukzessive um weitere Module erweitert.

Ein großes Vorhaben wird eine umfassende, zweijährige Schulungsreihe für den Schul- und Kultusbereich im Zusammenhang mit einer Bildungsplattform für Schulen sein, die im Jahr 2022 beginnt. Hier soll es eine Vielzahl von Schulungen für Schulleitungen, Lehrende, Datenschutzbeauftragte sowie Schüler_innen und Eltern geben. Für dieses wichtige Schulungsprojekt hat der Landtag befristet drei Stellen zur Verfügung gestellt. Zudem wird das Bildungszentrum im Jahr 2022 zwei weitere Stellen erhalten, mit denen die Bereiche Medienproduktion und -gestaltung sowie Verwaltung, Haushalt und Organisation verstärkt werden. Wir wollen damit unsere multimedialen Angebote ausbauen. Zudem hoffen wir, dass es die Rand- und Rahmenbedingungen zulassen, als Standard hybride Veranstaltung weiter zu etablieren, also wahlweise die Möglichkeit der Teilnahme vor Ort in Präsenz oder digital online. Für Interessierte außerhalb Stuttgarts wird es somit leichter, an einer unserer Veranstaltungen teilzunehmen.

Wir wünschen uns aber, dass das Bildungszentrum nicht nur ein überwiegend digitales Forum ist, sondern auch ein Treffpunkt vor Ort sein wird, wo sich alle an den modernen Bürgerrechten Datenschutz und Informationsfreiheit Interessierten treffen und austauschen können. Deshalb soll unser Angebot auch Formate wie Workshops, beispielsweise zu technischen und organisatorischen Maßnahmen, oder Veranstaltungsreihen, auch mit externen Expert_innen, etwa zum Thema Künstliche Intelligenz umfassen. Zudem werden wir nach Möglichkeit auch einzelne Präsenz-Veranstaltungen außerhalb des Bildungszentrums dezentral in Baden-Württemberg anbieten.

© LfDI BW

Zu Besuch in Stuttgart: Harald Welzer und Stefan Brink diskutierten über Möglichkeiten und Grenzen der Digitalisierung.

7. Kultur

7.1 Datenschutz kinderleicht

Wie bereits im vergangenen Tätigkeitsbericht angekündigt, haben wir uns daran gewagt, ein Sensibilisierungsprojekt für die Kleinsten zu entwickeln. Unter dem Motto „Datenschutz – kinderleicht" sensibilisieren wir Kindergartenkinder im Vorschulalter auf Basis von Grimms Märchen. In Teil 1 der neuen Reihe wird den Kleinen dabei die Bedeutung des eigenen Namens vermittelt. Und wer, wenn nicht Rumpelstilzchen, wäre dazu besser geeignet? Mit „Datenschutz kinderleicht – Teil 1 – Rumpelstilzchen" haben wir für die Großen und Kleinen zu Ostern eine Toolbox mit vielen bunten Werkzeugen, wie beispielsweise ein Musikvideo, ein Hörspiel und verschiedene Interviews auf unserer Homepage bereitgestellt. In Weihnachtszeit wurde Teil 2 – „Schneewittchen" veröffentlicht. Mit diesem Märchen wollen wir den Kindern die Bedeutung ihrer Wohnadresse nahebringen. Denn hätte nicht der geschwätzige Spiegel verraten, wo Schneewittchen wohnt – hinter den sieben Bergen, bei den sieben Zwergen – dann wäre die Geschichte womöglich besser für Schneewittchen ausgegangen.

7.2 „ALICE – lost and found"

Im Rahmen unserer Spotlights, die wir 2021 präsentiert haben, ist eine Kooperation mit den Theatermachern Meinhardt & Krauss entstanden, die wir in diesem Jahr mit einem weiteren Kinderprojekt fortgesetzt haben. „ALICE – lost and found" knüpft in spielerischer Form an das Kinder-Theaterprojekt „ALICE lost in cyberland" an.

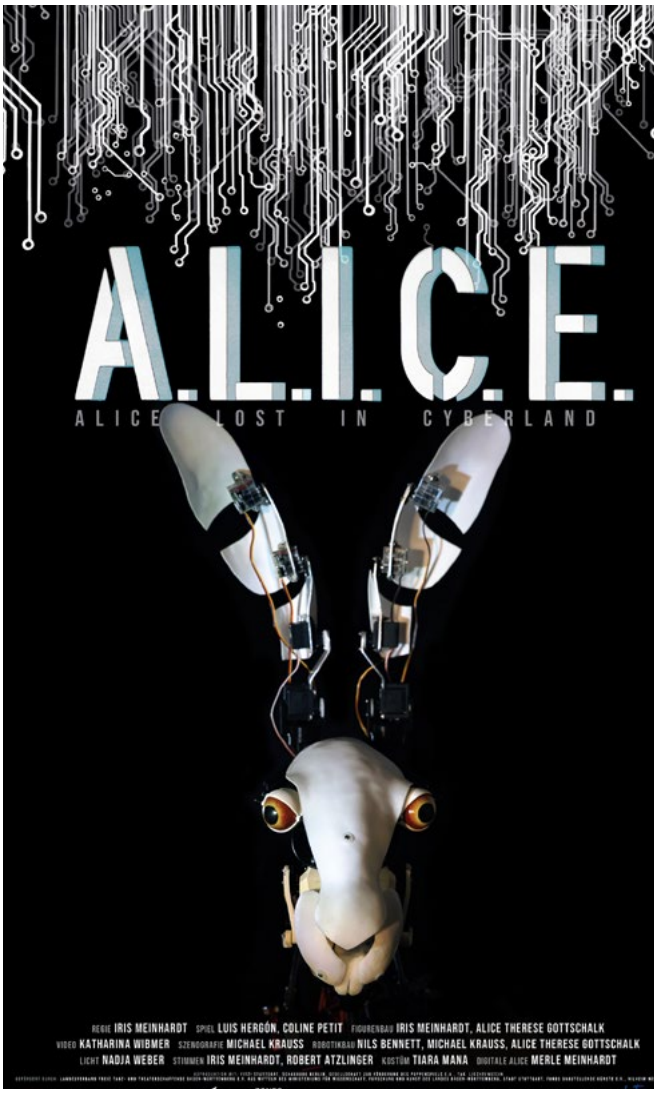
Alice ist verloren, und will nun gefunden werden

Die Theatermacher Meinhardt & Krauss inszenieren das Online-Live-Event nach Motiven von Alice im Wunderland als Escape-Room- und digitales Rätselspiel. „ALICE – lost und found" spielt und rätselt mit Kindern im Grundschulalter und deren Familien und allen, die am Rätseln Freude haben. Die Figurenspielerin und Regisseurin Iris Meinhardt, der Robotik- und Videokünstler Michael Krauss und der Komponist und Musiker Thorsten Meinhardt gewähren uns dabei einen weiteren Einblick in ihre künstlerische Arbeit und die Welt des modernen Figurentheaters.

7.3 Datenschutz geht zur Schule und Videoclips „Datenschutz – leicht erklärt"

In diesem Sinn unterstützen wir die Initiative „Datenschutz geht zur Schule" des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V. nicht nur, wir bauen diese aktiv gemeinsam aus. Als im letzten Jahr absehbar wurde, dass uns die Thematik der Pandemie und die damit verbundenen Einschränkungen bei Präsenzveranstaltungen noch einige Zeit begleiten werden, haben wir der Initiative „Datenschutz geht zur Schule" vorgeschlagen, gemeinsam eine digitale Version von „Datenschutz geht zur Schule" zu produzieren.

Mit diesem Projekt konnten wir unsere bisherige länderübergreifende Zusammenarbeit der Aufsichtsbehörden auch in digitaler Form fortsetzen bzw. sogar einige Aufsichtsbehörden dafür neu



© Meinhardt & Krauss

Veranstaltungsplakat zu „Alice – lost and found".

gewinnen. Unter dem Titel „Datenschutz – leicht erklärt“ haben wir hierfür im November 2021 rund 20 Videoclips produziert, die das bisherige Angebot von „Datenschutz geht zur Schule“ ergänzen werden. Die Veröffentlichung der Clips ist für den Europäischen Datenschutztag im Januar 2022 geplant. Ab diesem Zeitpunkt können die Clips für alle kostenfrei genutzt werden.

Die Initiative „Datenschutz geht zur Schule“ sensibilisiert Schüler_innen für einen bewussten Umgang mit dem Internet und den sozialen Medien.

7.4 Hörspiel „Spione wie wir. Tracking in der Familie“

Was bedeutet Tracking? Und was bedeutet es, das eigene Kind zu tracken? Ist es ok, wenn Eltern ihre Kinder tracken? Und wie stellt sich die Situation vielleicht umgekehrt dar? Und wer muss eigentlich wieviel von wem wissen? Insbesondere innerhalb einer Familie? Wo verläuft die Grenze zwischen Sicherheit und Privatsphäre? Diesen Fragen haben wir uns gestellt und in Kooperation mit der Hochschule der Medien zu diesem Themenfeld ein Hörspiel für Heranwachsende und Erwachsene produziert.

7.5 „Vergiss mich einmal mehr“ – Koproduktion mit Daniela Flickentanz

Und nicht zuletzt ist der Landesbeauftragte als Songwriter aktiv. Bereits im Jahr 2019 hatten wir einen Songtext gemeinsam mit Daniela Flickentanz geschrieben. Im September 2021 wurde ein weiterer Song veröffentlicht, den der Landesbeauftragte getextet und Daniela Flickentanz komponiert hat.

7.6 Märchenhafter Abend

Zum Abschluss des Jahres hatten wir im Dezember 2021 zu einem „märchenhaften Abend“ eingeladen – einer Veranstaltung, die wir in Kooperation mit der Hochschule der Medien konzipiert und gemeinsam in der Jungen Staatsoper Stuttgart durchgeführt haben. In Anlehnung an unser Projekt „Datenschutz – kinderleicht“, das Jüngere und Ältere im Hinblick auf ihre Privatsphäre und den Umgang mit personenbezogenen Daten sensibilisiert, haben wir uns mit der Frage der zeitgenössischen Bedeutung von Märchen und Geschichten aus ethischer, datenschutzrechtlicher und künstlerischer Sicht auseinandergesetzt.

>> Mehr Informationen:

Datenschutz – kinderleicht: „Rumpelstilzchen“ und „Schneewittchen“: https://www.baden-wuerttemberg.datenschutz.de/datenschutz-kinderleicht/

ALICE lost and found (digitales Rätselspiel): https://www.meinhardt-krauss.com/galerie/33515/alice-lost-and-found-(digitales-r%C3%A4tselspiel).html

„Spione wie wir. Tracking in der Familie“: https://www.baden-wuerttemberg.datenschutz.de/mediathek

„Datenschutz geht zur Schule“: https://www.bvd-net.de/datenschutz-geht-zur-schule/

Songs mit Daniela Flickentanz: https://www.youtube.com/watch?v=1z8Qs19JPzc ; https://www.flickentanz.at/texte ; https://www.youtube.com/watch?v=WB-8trK1Ldro <<

© Alexas_Fotos – pixabay

Datenschutz ist eine Kulturaufgabe.

Nicht juristisch, sondern erzählerisch in einem Hörspiel können Datenschutzthemen einfach zugänglich sein.

Irgendwas mit Algorithmus? Digitalisierung ist mehr als eine komplexe Berechnung. Sie hat auch mit europäischen Werten, der Ökonomie, dem Recht und mit Kultur zu tun.

8. Koordinierte Prüfung zum Drittstaatentransfer

Wir haben uns im Berichtszeitraum an einer länderübergreifenden Kontrolle der deutschen Datenschutzaufsichtsbehörden bezüglich der Umsetzung der Anforderung der Schrems-II-Entscheidung des Europäischen Gerichtshofs bei Datenübermittlungen aus der EU und dem europäischen Wirtschaftsraum an Stellen außerhalb der EU und des europäischen Wirtschaftsraums beteiligt. Ziel dieser Kontrolle war es, die breite Durchsetzung der Anforderungen des Europäischen Gerichtshofs in seiner Schrems-II-Entscheidung vom 16. Juli 2020 (Rs. C-311/18) zu sichern. In diesem Urteil stellte der EuGH fest, dass Übermittlungen in die USA nicht länger auf Basis des sogenannten Privacy Shields erfolgen können und die Zugriffsmöglichkeiten staatlicher Stellen auf personenbezogene Daten in Drittstaaten und der hiergegen mögliche Rechtsschutz für Betroffene aus Europa im Zusammenhang mit der Zulässigkeit der Übermittlung personenbezogener Daten in unsichere Drittstaaten nicht unberücksichtigt bleiben können.

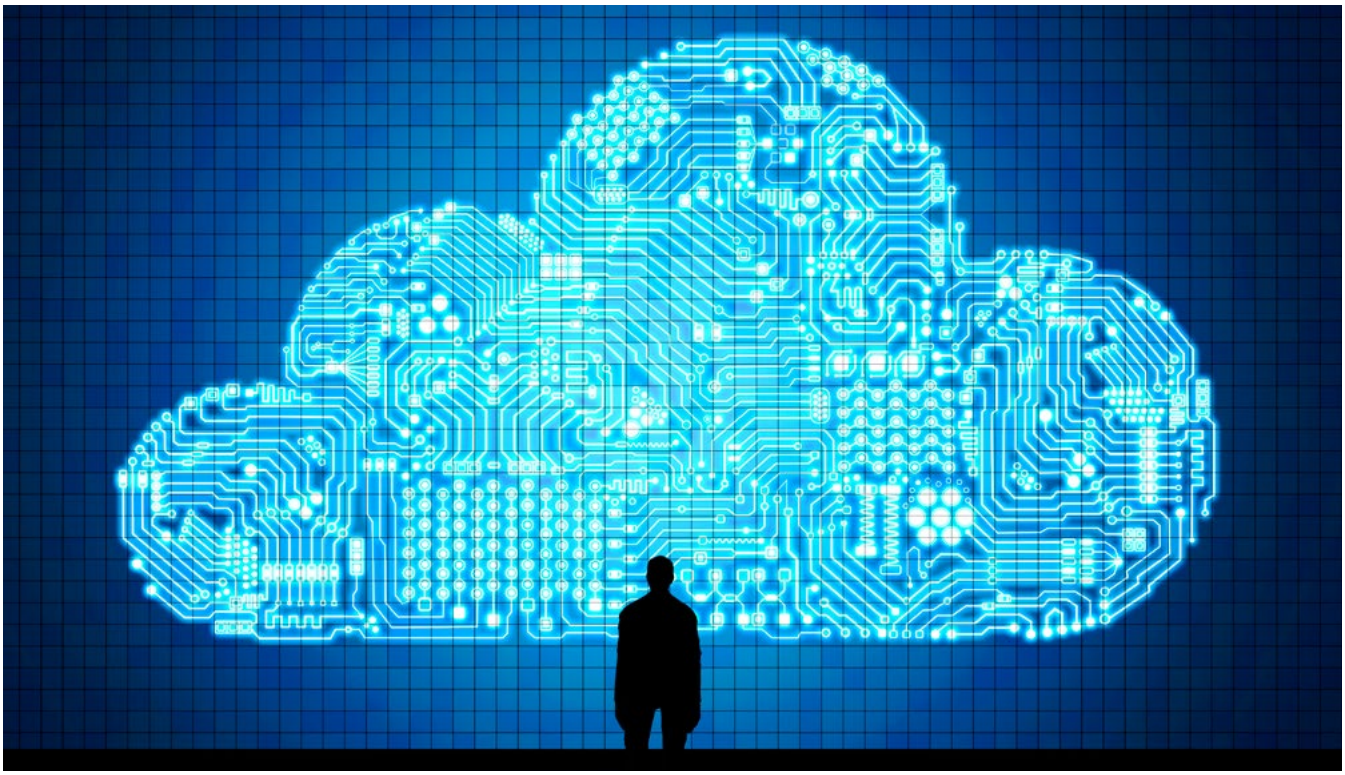
Dazu hat eine Task Force unter Vorsitz des Hamburger Landesdatenschutzbeauftragten fünf Fragebögen entwickelt, die die teilnehmenden Behörden ausgewählten Unternehmen und öffentlichen Stellen zukommen lassen konnten. Die Fragebögen befassten sich mit dem Einsatz von Dienstleister_innen zum E-Mail-Versand, zum Hosting von Internetseiten, zum Web-Tracking, zur Verwaltung von Bewerber_innendaten sowie dem konzerninternen Austausch von Kund_innen- und Beschäftigtendaten. Neben dem LfDI Baden-Württemberg beteiligten sich auch die Landesdatenschutzaufsichtsbehörden aus Bayern, Berlin, Bremen, Brandenburg, Hamburg, Rheinland-Pfalz, dem Saarland und Niedersachsen an der Prüfung. Jede Aufsichtsbehörde entschied hierbei individuell, in welchen der genannten Themenfelder sie tätig werden wollte.

Besonderes Interesse hatten wir an dem Bereich des Einsatzes von Dienstleister_innen in Drittstaaten bei der Verwaltung für Berwerber_innendaten. Nachdem wir uns einen Überblick über relevante öffentliche und nicht-öffentliche Stellen im Land verschafft hatten, kristallisierte sich schnell eine Gruppe relevanter Stellen bei der Verwaltung von Bewerber_innendaten heraus. Diese Stellen baten wir um Beantwortung des übersandten Fragebogens. Der Fragebogen erfragte in 16 Fragen, ob externe Dienstleister mit der Speicherung und/oder Verwaltung von Bewerber_innendaten beziehungsweise der Kommunikation mit Bewerber_innen eingesetzt werden, es dabei zu einer Datenübermittlung in ein Land außerhalb des EWR kommt und die hierfür geltenden rechtlichen Vorgaben (insbesondere das Erfordernis einer speziellen Rechtsgrundlage nach Kapitel 5 der DS-GVO) eingehalten werden. Die angeschriebenen Stellen haben alle innerhalb der gesetzten Frist alle Fragen verständlich und im erforderlichen Umfang beantwortet.

Das Ergebnis der Prüfung kann als durchaus erfreulich bezeichnet werden: Nur in einem Fall wurden Unregelmäßigkeiten im Rahmen der Drittstaatenübermittlung festgestellt. Das betreffende Unternehmen hatte einen Dienstleister in der EU mit der Verarbeitung von Bewerber_innendaten beauftragt. Dieser Dienstleister hatte wiederum einen Unterauftragsverarbeiter in einem unsicheren Drittstaat eingesetzt, ohne dass dabei den sich aus der Schrems-II-Entscheidung des EuGH ergebenden Prüfpflichten im Einzelfall ausreichend Genüge getan worden wäre. Damit konnte das Unternehmen nicht darlegen, dass die in seinem Auftrag im Drittstaat verarbeiteten personenbezogenen Daten keinem unverhältnismäßigen Zugriff durch Behörden des Drittstaates unterlagen und Betroffenen im Fall eines Zugriffs ausreichende Rechtsschutzmöglichkeiten hiergegen zur Verfügung stehen würden. Das betreffende Unternehmen hat uns zugesichert, den Anbieter zu wechseln und künftig nur noch solche Dienstleistungen von Auftragsverarbeitern in Anspruch zu nehmen, die in keiner Form mit einem Transfer personenbezogener Daten außerhalb Europas oder des europäischen Wirtschaftsraums verbunden sind. Wir behalten diesen Vorgang im Blick.

9. Der europäische Blick

Auch im Jahr 2021 hat die Corona-Pandemie natürlich weiterhin die Arbeit auf europäischer Ebene und in unserer Stabsstelle Europa erheblich beeinflusst. Die Sitzungen sowie die Arbeiten an Projekten der Arbeitsgruppen des Europäischen Datenschutzausschusses waren weiterhin (fast) ausschließlich in den digitalen Bereich verlagert. Ein Ausbau der Online-Möglichkeiten wie beispielsweise eines Forums für einen direkten Austausch hat jedoch die Kommunikation mit anderen euro-



Auch für Cloud-Anbieter gilt die DS-GVO. Wer in Europa Geschäfte machen will, muss sich an europäisches Recht halten.

päischen und deutschen Aufsichtsbehörden zu Einzelthemen verstärkt möglich gemacht. Daneben haben wir sowohl den Auftritt auf unserer Homepage hinsichtlich des neuen Formats von Grundlagen-Schulungs-Videos, mit denen wir Interessierten die Möglichkeit zur Online-Information geben, ausgebaut, als auch durch eine erhöhte Anzahl an Online-Inhouse-Schulungen die eigenen Kolleg_innen über aktuelle Entwicklungen aus allen Themenbereichen auf dem Laufenden gehalten.

9.1 Gemeinsame Verantwortlichkeit und Auftragsverarbeitung

Ein Thema, das uns nach wie vor mit am häufigsten begegnet, ist die gemeinsame Verantwortlichkeit nach Artikel 26 DS-GVO. Dies bestätigt über unsere tägliche Arbeit hinaus auch die erhöhte Nachfrage zu Schulungen in diesem Bereich. Spätestens durch die aktuelle Rechtsprechung des Europäischen Gerichtshofs zur Figur und den möglichen Formen der gemeinsamen Verantwortlichkeit sind viele Fragen zur Rollenverteilung, den Rechten und Pflichten der verantwortlichen Stellen sowie zur Vertragsgestaltung in diesem Bereich aufgekommen.

Bereits vor einiger Zeit konnten wir durch das erste europäische Muster zur Erstellung eines Vertrages über die gemeinsame Verantwortlichkeit die komplexen Vorgaben der DS-GVO umsetzbar machen. Anhand eines konkreten Projekts von öffentlichen und privaten Stellen des Landes war es uns möglich, die im Rahmen gemeinsamer Verantwortlichkeit relevanten Aspekte herauszuarbeiten und die zugehörigen Schwerpunkte für die Vertragsgestaltung zu identifizieren. In dem Vertragsmuster werden die verschiedenen Verarbeitungsprozesse im Einklang mit der aktuellen Rechtsprechung des Europäischen Gerichtshofs in sogenannte Wirkbereiche aufgeschlüsselt und Hilfestellung für die konkrete Zuordnung der Pflichten der einzelnen Verantwortlichen sowie die transparente Bereitstellung aller notwendigen Informationen an die betroffenen Personen gegeben.

Nicht zuletzt spielt in diesem Zusammenhang auch die Abgrenzung zur Auftragsverarbeitung (Artikel 28 DS-GVO) eine große Rolle. Auch hierzu war es uns möglich, ein Vertragsmuster zu erstellen, das praktische Tipps für die Gestaltung von Auftragsverarbeitungsverträgen im Sinne der DS-GVO gibt. Es enthält neben Regelungen zur Festlegung der Leistungen des Auftragnehmers auch solche zu den Rechten und Pflichten beider Parteien sowie hilfreiche Passagen für die Inanspruchnahme von Subunternehmen.

Beide Vertragsmuster zur gemeinsamen Verantwortlichkeit sowie zur Auftragsverarbeitung, die wir erstellt haben, erfreuen sich als praktische Hilfestellung erfreulicherweise auch weiterhin größter Aufmerksamkeit.

Der Europäische Datenschutzausschuss hatte außerdem bereits im September 2020 weitere Abhilfe geschaffen, indem er die „Guidelines on the concepts of controller and processor in the GDPR" – sprich „Leitlinien über die Abgrenzung der Verantwortlichkeiten und des Konzepts der Auftragsverarbeitung" – verabschiedet hat. Diese wurde im Rahmen einer öffentlichen Konsultation einer erneuten großen Überprüfung unterworfen, in der sich aus Anmerkungen zum Inhalt des Papiers seitens Unternehmen, Verbänden, Privaten, etc. insbesondere der Wunsch nach (noch) konkreteren Definitionen und Abgrenzungen der Verantwortlichkeiten und praktischen Beispielsfällen zur Veranschaulichung ergeben hat. Infolge der Analyse dieser Äußerungen hat der Europäische Datenschutzausschuss im Juli 2021 eine überarbeitete Version der Leitlinien veröffentlicht. Das hat die Stabsstelle Europa unverzüglich zum Anlass genommen, die bereits vor einiger Zeit erstellten FAQs zu den Leitlinien, in denen die Kernaussagen zusammengefasst werden, ebenfalls anzupassen. Der Inhalt der FAQs wurde insgesamt erweitert und aktualisiert, insbesondere wurden die neuen anschaulichen Beispielsfälle aus der Leitlinie ergänzt. Durch die umfassenden, teils ergänzenden Erläuterungen sowie Querverweise auf das Dokument des Europäischen Datenschutzausschusses geben die FAQs nun einen noch besseren Überblick über die komplexen Rechtsfragen zu den Verantwortlichkeiten.

9.2 Internationaler Datentransfer – „Schrems II" und Standarddatenschutzklauseln

Am 4. Juni 2021 hat die Europäische Kommission neue Standardvertragsklauseln für den Drittstaatentransfer (Standarddatenschutzklauseln nach Artikel 46 Abs. 2 Buchstabe c DS-GVO) erlassen, um den Änderungen durch die DS-GVO Rechnung zu tragen. Zudem sollen die neuen Standarddatenschutzklauseln im Unterschied zu den bisherigen auch für den Fall der Beteiligung einer Vielzahl von Importeur_innen und Exporteur_innen und lange und komplexe Verarbeitungsketten gelten. Die neuen Standarddatenschutzklauseln sind modular aufgebaut und gelten für Übermittlungen zwischen einem Verantwortlichen oder Auftragsverarbeiter, der der DS-GVO unterliegt, und einem Verantwortlichen oder Auftragsverarbeiter, der nicht der DS-GVO unterliegt. Insgesamt gibt es also vier Module. Erfasst ist damit auch ein Transfer innerhalb eines Drittstaats oder von einem Drittstaat an einen anderen Drittstaat, wenn der „Exporteur" gemäß Artikel 3 Absatz 2 der DS-GVO dieser unterfällt. Bei den Modulen ist allerdings Obacht geboten: Einige (Teil-)Klauseln gelten für alle Modulvarianten, während bei anderen Klauseln jeweils zu prüfen ist, ob sie für das gewünschte Modul einschlägig sind.

Die neuen Standarddatenschutzklauseln enthalten eine Übergangsregelung, wonach Übermittlungen auf der Grundlage der alten Standardvertragsklauseln 2001/497/EG und 2010/87/EU noch bis zu einem Jahr nach Inkrafttreten der neuen Standardverträge möglich sind. In dieser Zeit sind nachträgliche Vertragsänderungen – mit Ausnahme der Vereinbarung notwendiger zusätzlicher Maßnahmen zur Erreichung eines angemessenen Schutzniveaus im Sinne von Artikel 45, 46 der DS-GVO – für die bereits vor Inkrafttreten der neuen Standarddatenschutzklauseln abgeschlossenen Verträge allerdings ausgeschlossen. Die alten Standardvertragsklauseln dürfen neue abzuschließenden Vereinbarungen jetzt auch nicht mehr zugrunde gelegt werden.

Neben den Modulerweiterungen enthalten die neuen Klauseln auch weitere inhaltliche Neuerungen. Die neuen Standarddatenschutzklauseln setzen dabei – jedenfalls zum Teil – einige der Forderungen um, die wir in unserer Orientierungshilfe „Was jetzt in Sachen internationaler Datentransfer?" bereits kurz nach dem Schrems- II-Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 aufgestellt hatten. Daher stellen die neuen Klauseln aus unserer Sicht bereits eine Verbesserung dar. Wir empfehlen, baldmöglichst auf die neuen Klauseln umzusteigen. Wir haben den Erlass der neuen Standarddatenschutzklauseln auch zum Anlass genommen, unsere Orientierungshilfe zu aktualisieren. Darin raten wir, die neuen Klauseln zum Teil zu ergänzen (ab S. 9 der 4. Auflage der Orientierungshilfe detailliert beschrieben). Außerdem weisen wir darauf hin, dass bei Klausel 14 im höchsten Maße Vorsicht geboten ist. Diese sieht die Möglichkeit vor, zur Bestimmung des Datenschutzniveaus im Drittland auch dortige

Gepflogenheiten heranzuziehen. Laut EU-Kommission können dazu auch (einschlägige und dokumentierte) praktische Erfahrungen herangezogen werden, ob es in der Vergangenheit Ersuchen um Offenlegung personenbezogener Daten seitens öffentlicher Drittlandsbehörden gab. Wir empfehlen Datenexporteuren aber, sich nicht nur auf solche praktischen Erfahrungen zurückzuziehen, sondern sich an praktischen Beispielen zu möglichen zusätzlichen Garantien zu orientieren und diese umzusetzen. Solche praktischen Beispiele sind in der Empfehlung des Europäischen Datenschutzausschusses in Anhang 2 enthalten.

Hinweis – nicht verwechseln: Neben den Standarddatenschutzklauseln für den Drittstaatentransfer hat die EU-Kommission auch Standardvertragsklauseln gemäß Artikel 28 Abs. 7 DS-GVO als Alternative zur individuellen Auftragsverarbeitungsvereinbarung erlassen. Diese gelten für den Datenverkehr innerhalb der EU.

9.3 Die neue KI-Verordnung

Die EU-Kommission erweitert derzeit das rechtliche Rahmenwerk für digitale Anwendungen mit einer Verordnung für Künstliche Intelligenz (KI). Dazu wurde von der EU-Kommission am 21. April 2021 ein Verordnungsentwurf für KI-Anwendungen vorgestellt.

Im Rahmen einer Stellungnahme des Europäischen Datenschutzausschusses (EDSA) beteiligte sich die Stabsstelle Europa, den Verordnungs-Entwurf der EU-Kommission zur Regulierung von Anwendungen der Künstlichen Intelligenz (KI) in Bezug auf datenschutzrelevante Themen kritisch zu prüfen. In der Stellungnahme wurden einige für den Datenschutz wesentliche Punkte und Problemstellen erörtert.

So versäumt es der Verordnungsentwurf bislang, ausdrücklich die Vorgaben der DS-GVO hervorzuheben, wo KI-Anwendungen personenbezogene Daten verarbeiten. Die KI-Verordnung muss rechtlich auf einer Stufe mit der DS-GVO stehen. Eine Anpassung dahingehend durch die EU-Kommission ist unerlässlich, da andernfalls für Hersteller und Nutzende von KI-Anwendungen eine Rechtsunsicherheit entsteht.

Dem Entwurf fehlt es außerdem an effektiven Rechten und Rechtsbehelfen für betroffene Personen oder Interessensverbände. Diese sind elementarer Bestandteil in der DS-GVO und bieten betroffenen Personen eine effektive Möglichkeit, einer Einschränkung ihrer (Grund-)Rechte zu begegnen. Der Europäische Gerichtshof hat unter anderem mit seiner Schrems II-Entscheidung erneut klargestellt, dass betroffenen Personen in der Wahrnehmung ihrer Rechte größtes Gewicht beizumessen ist.

Ein sensibler Kritikpunkt besteht auch in dem Verbot für besonders kritische KI-Anwendungen, das die Verordnung vorsieht. Dazu zählt insbesondere die biometrische Fernidentifizierung im öffentlichen Raum, beispielsweise die biometrische Gesichtserkennung an Bahnhöfen oder auf öffentlichen Plätzen. Aber auch die unterschwellige Beeinflussung von Personen, Auswertung von Emotionen, Bewertung des sozialen Verhaltens (Social Scoring) sowie die Kategorisierung nach biometrischen Merkmalen, etwa nach ethnischer Herkunft, Geschlecht, politischer oder sexueller Orientierung oder sonstigen Diskriminierungsgründen nach Art. 21 der Charta der Grundrechte der Europäischen Union. Diese Verbote sind soweit sehr begrüßenswert.

Aus Sicht des EDSA enthalten die Regelungen jedoch zu weitgehende Ausnahmen, etwa bei Nichteintritt physischer oder psychischer Schäden, oder wenn Anwendungen nur über einen bestimmten Zeitraum durch Behörden oder in deren Auftrag erfolgen. Die europäischen Aufsichtsbehörden fordern, KI-Anwendungen zur automatischen Erkennung von personenbezogenen Merkmalen im öffentlichen Raum allgemein zu verbieten. Zudem sollten KI-Anwendungen zur biometrischen Kategorisierung oder zur Ermittlung des emotionalen Zustands von Personen allgemein verboten oder zumindest nur für eng umgrenzte Anwendungsfälle, etwa zu Gesundheits- oder Forschungszwecken, zugelassen werden.

Weiterhin sieht der Entwurf für viele KI-Anwendungen, die voraussichtlich mit einem hohen Risiko für betroffene Personen einhergehen, lediglich eine Selbstprüfung durch die Hersteller vor, ohne (auch) eine datenschutzrechtliche Prüfung zu fordern. Die dadurch ausgelöste Gefahr, dass eine KI-Anwendung im Rahmen der KI-Verordnung dann umsetzbar ist, aber nicht datenschutzkonform eingesetzt werden kann, ist nicht hinnehmbar. Hersteller sollten vielmehr immer auch eine

>> Mehr Informationen:

Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten vom 10.11.2020: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf

Empfehlung des Europäischen Datenschutzausschusses in Anhang 2: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_de.pdf

Die 4. Auflage der Orientierungshilfe „Was jetzt in Sachen internationaler Datentransfer?": https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf

Die neuen Standarddatenschutzklauseln nach Artikel 46 Abs. 2 Buchstabe c DS-GVO: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0914

Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915

Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz vom 21.4.2021: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52021PC0206

Gemeinsame Stellungnahme zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 18.6.2021: https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_de.pdf <<

Risikoabschätzung unter Berücksichtigung der angedachten Anwendungsfälle durchführen und das Unternehmen oder die Behörde, die das KI-System anwenden möchten, sollten bei KI-Anwendungen mit voraussichtlich hohen Risiken verpflichtend eine Datenschutz-Folgenabschätzung (DSFA) mit dem spezifischen Kontext der Anwendung durchführen müssen. Zudem fordert der EDSA, dass Hersteller einer KI-Anwendung mit hohen Risiken die Konformitätsbewertung immer durch unabhängige Dritte durchführen lassen.

Schließlich setzt sich der EDSA dafür ein, die bestehenden Datenschutz-Aufsichtsbehörden auch als Aufsichtsbehörden für KI-Anwendungen vorzusehen. Da sensible KI-Anwendungen mehrheitlich auch mit der Verarbeitung personenbezogener Daten einhergehen, ist die Expertise der Datenschutz-Aufsichtsbehörden für die Aufsicht der KI-Verordnung unerlässlich.

Dazu gehört insbesondere die Bereitstellung eines KI-Reallabors durch die (Datenschutz-)Aufsichtsbehörden, mittels denen insbesondere kleinen und mittleren Unternehmen ohne entsprechende finanzielle Möglichkeiten ein Verfahren angeboten wird, KI-Anwendungen in einer sicheren Umgebung zu testen und einer Konformitätsbewertung unterziehen zu können. Innovationen im Bereich KI sollen dadurch auch in kleinen und mittleren Unternehmen gefördert werden.

Es gehört zu unseren Aufgaben, die Umsetzung der KI-Verordnung in Baden-Württemberg zu begleiten. Wir werden uns in Zukunft sehr intensiv mit KI befassen. Ich bin dem Landtag sehr dankbar, dass er uns mit der Bewilligung von zwei neuen Stellen substanziell stärkt, sodass wir unsere Aufgaben gerade in diesem zukunftsträchtigen Bereich wirksamer wahrnehmen können. Dieses vorausschauende Handeln des Landtags hilft uns, Start-ups und Unternehmen in für Baden-Württemberg wichtigen Wirtschaftssektoren wie dem Gesundheitssektor gut zu beraten. Dies nützt wiederum den Unternehmen und dem Wirtschaftsstandort – und letztlich allen Bürger_innen.

Die weitere Entwicklung der KI-Verordnung ist für Unternehmen und Behörden in Baden-Württemberg von großer Bedeutung. Wir werden uns auch in Zukunft für eine datenschutzkonforme und da-

mit rechtssichere Ausgestaltung des rechtlichen Rahmenwerks einsetzen.

9.4 DS-GVO.clever 2.0

Vereine sind nach der DS-GVO genauso wie Unternehmen, Behörden und alle anderen Verantwortlichen verpflichtet, Datenschutzinformationen bereitzustellen. Korrekte Datenschutzerklärungen zu formulieren fällt jedoch insbesondere kleineren Unternehmen und Vereinen schwer, da sie nicht über die Ressourcen verfügen, externe Datenschutzbeauftrage einschalten oder mit der eigenen Rechtsabteilung tätig werden zu können.

Daher haben wir im vergangenen Jahr ein Projekt angestoßen, das Anfang 2021 in die Praxis überführt wurde. Mit „DS-GVO.clever" steht ein Tool auf der Homepage des Landesbeauftragten zur Verfügung, mit dem Vereine einfach und schnell Datenschutzhinweise generieren und für die eigenen Zwecke nutzen können. Das Tool ist mit zahlreichen Info-Buttons und Hinweisen auf weitere Hilfestellungen des LfDI, wie Erklärvideos oder Praxisratgeber, versehen.

Zudem führte das Bildungszentrum 2021 vier Online-Veranstaltungen durch, bei denen rund 200 Teilnehmende eine Schritt-für-Schritt-Anleitung für die Nutzung von „DS-GVO.clever" erhielten. Neben Vereinen haben wir weitere Zielgruppen von Verantwortlichen in den Blick. Die Weiterentwicklung führte im Herbst 2021 zum Launch von „DS-GVO.clever 2.0", begleitet von zwei BIDIB-Schulungen, die speziell für kleine Unternehmen, Gewerbetreibende und Handwerksbetriebe entwickelt wurden. Um auf deren Bedarfe einzugehen, wird unter anderem auch die Verarbeitung von Kund_innendaten in den Blick genommen. Auch in der neuen Version finden sich selbstverständlich hilfreiche Info-Buttons und Hinweise.

„DS-GVO.clever" ist modular aufgebaut und datensparsam: Es wurde in TypeScript basierend auf React entwickelt. Besonders hervorzuheben ist die Möglichkeit, gleichzeitig Änderungen einzugeben und das Ergebnis direkt zu sehen. Bei der Entwicklung wurde eine modulare Struktur kreiert, um Erweiterungen mit Templates zu ermöglichen. Ebenso wurde darauf geachtet, dass – im Sinne größtmöglicher Datensparsamkeit – keine der eingegebenen Daten auf dem Server gespeichert werden, sondern nach dem Laden die Eingaben nur lokal im Browser verarbeitet werden. Mit der Weiterentwicklung wurden beide Versionen mit der Möglichkeit versehen, offene Punkte beim Generieren der Datenschutzhinweise effektiver zu bearbeiten, in dem Nutzer_innen direkt zu offenen Eingabefeldern geleitet werden. Da keine Daten gespeichert werden, erhalten Nutzer_innen bei Schließen des Tabs oder der Seite nun außerdem eine Warnung im Browser, um ein ungewolltes Nutzungsende zu verhindern.

Auch im Jahr 2022 sind wieder Schulungen zu „DS-GVO.clever" geplant. Die Termine werden auf der Seite des BIDIB bekanntgegeben.

Anregungen und Feedback zu „DS-GVO.clever" nimmt der Landesbeauftragte gerne unter dem speziell dafür eingerichteten Postfach DS-GVO.clever@lfdi.bwl.de entgegen.

>> Mehr Informationen:

DS-GVO.clever für Vereine und kleinere Unternehmen:

https://www.baden-wuerttemberg.datenschutz.de/ds-gvo.clever/#vereine

https://www.baden-wuerttemberg.datenschutz.de/ds-gvo.clever/#ku

Veranstaltungen des Bildungszentrums: https://www.baden-wuerttemberg.datenschutz.de/offene-veranstaltungen/

„Datenschutz und Social Media: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/11/BvD-Herbstkonferenz-2021_Datenschutz-und-Social-Media-Aktuelle-Entwicklungen.pdf

Leitlinien über die gezielte Ansprache von Nutzer_innen sozialer Medien: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf

Weitere Leitlinien und Stellungnahmen des Europäischen Datenschutzausschusses: https://edpb.europa.eu/edpb_de <<

9.5 Gremienarbeit

Auch auf europäischer Ebene setzen wir uns in den Arbeitsgremien des Europäischen Datenschutzausschusses (EDSA) weiterhin tatkräftig für den Datenschutz ein. Der EDSA besteht aus Vertreter_innen der nationalen Datenschutzbehörden und dem Europäischen Datenschutzbeauftragten (EDSB). Deutschland ist dort mit einem Sitz vertreten. Den Sitz des Gemeinsamen Vertreters der deutschen Aufsichtsbehörden nimmt aktuell der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) wahr. Am 25. Juni 2021 wählte der Bundesrat den Bayerischen Landesbeauftragten für den Datenschutz (BayLfD), Professor Thomas Petri, zum Stellvertreter im Europäischen Datenschutzausschuss. Dieser Stellvertreter nimmt das Stimmrecht in Sachen wahr, in denen die Länder allein das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen. Daher begrüßen wir es sehr, dass der Bundesrat dieses Versäumnis nun nachgeholt hat und unterstützen Thomas Petri bei der Ausübung dieses Amtes. So nehmen wir unter anderem an den vorbereitenden Sitzungen der deutschen Aufsichtsbehörden im Vorfeld der Plenarsitzungen des EDSA teil.

In den Arbeitsgremien des Europäischen Datenschutzausschusses haben wir eine feste Position als Ländervertreter im Coordinated Supervision Committee sowie in der Social Media Expert Subgroup inne. Außerdem haben wir im Jahr 2021 eine weitere verantwortungsvolle und spannende Aufgabe auf europäischer Ebene übernommen: Die Koordinierung der Social Media Expert Subgroup. Die Koordinator_innenschaft wird ebenfalls von der Stabsstelle Europa wahrgenommen und umfasst die Organisation und Moderation der Sitzungen der Subgroup, in enger und vertrauensvoller Zusammenarbeit insbesondere mit dem Sekretariat des EDSA.

Die Subgroup ist unter anderem für die Analyse sozialer Medien und deren bestehender und neu entstehender Funktionen zuständig. Außerdem werden dort Leitlinien, Empfehlungen und Best Practices in Bezug auf die Nutzung sozialer Medien erstellt. In diesem Rahmen wurden die „Guidelines 8/2020 on the targeting of social media users“ aus der Social Media Expert Subgroup im Anschluss an die öffentliche Konsultation im April 2021 endgültig vom Europäischen Datenschutzausschuss angenommen. Wir waren als einfacher Berichterstatter an der Erstellung dieser Leitlinien über die gezielte Ansprache von Nutzer_innen sozialer Medien beteiligt.

Veriene und kleinere Unternehmen können mit dem LfDI-Tool DS-GVO.clever einfach und schnell Datenschutzhinweise erstellen.

Ende Oktober 2021 erhielten die Teilnehmenden der BvD-Herbstkonferenz beim Thema „Datenschutz und Social Media: aktuelle Entwicklungen" einen Überblick zum Inhalt der Leitlinien. Die Präsentation stellt der Landesbeauftragte auf seiner Homepage zur Verfügung. In zwei weiteren Social Media-Themen setzen wir uns als federführender beziehungsweise einfacher Berichterstatter weiterhin für die Erstellung europäischer Leitlinien zu aktuellen Fragen ein.

Außerdem haben wir in weiteren Bereichen die Berichterstatterschaft für die Erstellung europäischer Leitlinien übernommen. Die einfache Berichterstatterschaft für Leitlinien zu einem aktuellen Thema in Grundsatzfragen der DS-GVO üben wir in der Key Provisions Expert Subgroup gemeinsam mit dem Bundesbeauftragten und Mecklenburg-Vorpommern aus. Die „Leitlinien über die Abgrenzung der Verantwortlichkeiten und des Konzepts der Auftragsverarbeitung" wurden vom EDSA in diesem Jahr endgültig angenommen. Hier teilten wir uns mit Schleswig-Holstein die Position des einfachen Berichterstatters.

In der für Fragen der aufsichtsbehördlichen Zusammenarbeit zuständigen Cooperation Expert Subgroup wurde 2021 die federführende Berichterstatterschaft des LfDI an einem internen Papier zu einem aktuellen Thema rund um das Kooperationsverfahren nach der DS-GVO erfolgreich abgeschlossen.

9.6 Wegweiser durch den Info-Dschungel: Icons helfen

Wer kennt das nicht: gerade angekommen in einer neuen Stadt, muss man sich erst mal zurechtfinden und mit den Örtlichkeiten und lokalen Gepflogenheiten vertraut machen. Hilfreich sind dabei Wegweiser, z. B. in Form von Straßen- oder Verkehrsschildern, die uns schnell Orientierung geben. Die gleiche Funktion übernehmen die Datenschutz-Icons, die im Rahmen des Wettbewerbs: „Icons entwerfen und Datenschutz mitgestalten" als Gewinner-Icons im Oktober 2021 prämiert wurden. Wer personenbezogene Daten verarbeitet, muss erklären, wofür. Datenschutzhinweise sind manchmal lang und auch unübersichtlich. Wir stoßen tagtäglich auf diese: bei jedem Cookie-Banner, jedem App-Download oder jedem Besuch auf der Webseite von Unternehmen oder Behörden. Nutzer_innen von solchen Angeboten, die diese Erklärungen lesen, verlieren nicht selten den Überblick und damit das Verständnis für die darin enthaltenen wichtigen Informationen – obwohl Artikel 12 Abs. 1 DS-GVO Verantwortliche verpflichtet, die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Im Ausgust und September 2021 waren alle Kreativen aufgefordert, beim Wettbewerb „Datenschutz-Icons" mitzumachen und Vorschläge einzureichen. Es wurden Lösungen gesucht, die Datenschutzinformationen mithilfe von Icons, Symbolen oder anderen grafischen Elementen einfacher, klarer und sofort verständlich machen. Denn nur wer versteht, worum es geht, kann seine Rechte informiert ausüben, z. B. die Einwilligung in den Newsletterversand widerrufen, Privatsphäreneinstellungen am Browser vornehmen oder weitere Betroffenenrechte geltend machen.

Folgende Begriffssymbole wurden gesucht und von der Expertenjury Florian Mehnert (Konzeptkünstler), Cornelia Tausch, Vorstand der Verbraucherzentrale Baden-Württemberg, und mir ausgewählt:

- (personenbezogene) Daten,
- Zweck,
- Rechtsgrundlage, mit Icons zu Einwilligung und deren Widerruf, sowie zu Vertrag, rechtliche Verpflichtung und berechtigtes Interesse,
- Schutz, mit Icons zu den Betroffenenrechten Auskunft, Berichtigung, Einschränkung, Löschung sowie Beschwerde (bei der Aufsichtsbehörde),
- Datenschutzbeauftragte_r,
- Aufsichtsbehörde,
- Weitergabe mit Icons zu Empfänger und Übermittlung in Drittstaaten,

Die feierliche Verleihung der Auszeichnungen für die Plätze 1 bis 3 fand Ende Oktober 2021 im Rahmen des Abendprogramms der BvD-Herbstkonferenz in München statt. Nach einem einführenden Überblick über die europäische Grundlage für die Erstellung von Datenschutz-Icons – die gibt es nämlich ausdrücklich! –, bekamen bei der Preisverleihung alle drei Prämierten die Gelegenheit, sich selbst sowie die Beweggründe für ihre Teilnahme

an dem Projekt vorzustellen. Besonderer Hingucker war die Inszenierung des Zweitplatzierten, der sich per Videokonferenz zugeschaltet hatte und für sein Gespräch einen auf aktuelle Themen abgestimmten Datenschutz-Newsticker über seinen Bildschirm laufen ließ. Prämiert wurden Stefan Behringer (Platz 1), Gustav Blaß (Platz 2) und Sabine Sonneborn (Platz 3). Ein Sonderpreis wurde an Claudia Lobmeier für ihre prägnanten Ideen vergeben. Die prämierten Icons werden nun grafisch überarbeitet und vereinheitlicht. Wenn sich solche Icons etablieren, nützt das sehr vielen Menschen, sich im Informationsdschungel besser zurechtzufinden und informieren zu können. Die vielen Einreichungen sendeten ein positives Signal: Die Bereitschaft, Datenschutz mitzugestalten, ist groß!

9.7 Schulungen

Zur fortlaufenden Fortbildung des Hauses hat die Stabsstelle Europa auch im Jahr 2021 wieder stetig Inhouse-Schulungen für alle Mitarbeitenden angeboten, die aufgrund der Pandemiesituation weiterhin im Online-Format angeboten wurden. Die insgesamt 18 Schulungen gaben den Beschäftigten Einblicke in die aktuelle Arbeit der verschiedenen Abteilungen des LfDI und erfreuten sich eines breiten Publikums, zu dem glücklicherweise auch viele der neu hinzugekommenen Beschäftigten zählten. Daneben halten die Referent_innen der Stabsstelle Europa regelmäßig Vorträge im Rahmen des Programms des Bildungszentrums BIDIB. Zu Letzterem soll auch das von der Stabsstelle entworfene Format der Online-Schulungen noch erweitert werden, um in Zukunft noch mehr datenschutzinteressierte Personen unterstützen und begeistern zu können.

Icons können dabei helfen, Datenschutzhinweise einfacher zu gestalten.

10. Aktuelles aus der Bußgeldstelle

Vom 01. Januar 2021 bis 31.Dezember 2021 wurden bei der Bußgeldstelle insgesamt 129 neue Verfahren anhängig. Auch in diesem Jahr machte sich die Corona-Pandemie – ähnlich wie im vergangenen Jahr – bei der Anzahl der Neueingänge bemerkbar.

Im Berichtszeitraum hat die Bußgeldstelle 14 Bußgeldbescheide erlassen, welche sich sowohl gegen natürliche Personen als auch gegen Unternehmen richteten. Während bei den Verfahren gegen Unternehmen die Verstöße vielfältiger Art waren, stand bei den Verfahren gegen natürliche Personen die zweckwidrige Verwendung von personenbezogenen Daten zu privaten Zwecken, insbesondere durch Polizeibeamt_innen, im Zentrum der Vorwürfe. Insgesamt wurden Bußgelder in einer Höhe von 319.700,00 Euro und Gebühren in Höhe von 8.682,00 Euro festgesetzt. 77 weitere Verfahren wurden in sonstiger Weise erledigt, z. B. dadurch dass nach Ermittlungen durch die Bußgeldstelle ein Datenschutzverstoß nicht festgestellt oder nachgewiesen werden konnte oder dass die Verhängung einer Geldbuße aus Verhältnismäßigkeitsgesichtspunkten nicht geboten erschien.

10.1 VfB Stuttgart

Auch im aktuellen Berichtszeitraum hob sich ein Bußgeldverfahren gleich aus mehreren Gründen von den übrigen Verfahren der Bußgeldstelle ab. Durch einen Bericht in einer Sportzeitschrift wurden wir auf behauptete Vorgänge beim Fußballverein VfB Stuttgart 1893 aufmerksam. Die Untersuchung verschiedener datenschutzrechtlicher Fragestellungen ergab schließlich Hinweise, welche die Durchführung eines Bußgeldverfahrens gegen die VfB Stuttgart 1893 AG geboten erscheinen ließen, wohingegen hinsichtlich des Vereins eine beratende Begleitung ausreichend war.

Der Vorwurf, der schließlich zur Verhängung des Bußgeldverfahrens führte, stand dabei nicht in Verbindung mit etwaigen Datenverarbeitungen rund um die Ausgliederung der Profi-Fußballabteilung im Jahr 2017, sondern lag in Datenschutzmissständen begründet, die dazu führten, dass im Jahr 2018 erhebliche Mengen personenbezogener Daten, darunter vollständige Datensätze von Vereinsmitgliedern, an einen externen Dienstleister übermittelt wurden, ohne dass die VfB Stuttgart 1893 AG den konkreten Zweck oder eine taugliche Rechtsgrundlage hierfür benennen konnte. Die AG verstieß damit in nicht unerheblichem Umfang gegen ihre Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO, die seit Wirksamwerden der DS-GVO von den verantwortlichen Stellen fordert, die Rechtmäßigkeit ihrer Datenverarbeitung nachweisen zu können.

Außergewöhnlich war das Verfahren aber nicht allein deshalb, weil es um Datenverarbeitungen im Kontext eines deutschen Profifußballvereins ging, sondern weil damit eine umfangreiche Medienberichterstattung einherging, die sich zum Teil aus Quellen und Informationen speiste, die uns nicht oder erst zu deutlich späteren Zeitpunkten vorlagen, sodass wir in zum Teil sehr kurzen Intervallen unsere Ermittlungen an neue Informationen anzupassen hatten. Außergewöhnlich war aber auch, dass uns trotz des drohenden Bußgeldes für die VfB Stuttgart 1893 AG mit großer Offenheit hinsichtlich der eigenen Versäumnisse und mit umfangreicher Kooperation begegnet wurde.

Auf diese Weise war es möglich, die Ermittlungen effektiv und zügig zu führen und eine Verfahrensbeendigung im Rahmen einer Verständigung zu erreichen, die nicht nur eine angemessene Reaktion auf die Versäumnisse der Vergangenheit darstellte, sondern auch die deutlichen Verbesserungen in den Blick nahm, die beim Datenschutzmanagement der VfB Stuttgart 1893 AG erreicht werden konnten.

Im Rahmen dieser Verständigung verpflichtete sich die VfB Stuttgart 1893 AG zu weitreichenden Maß-

>> Mehr Informationen:

Pressemitteilung „Bußgeldverfahren gegen VfB Stuttgart 1893 AG endet mit der Verhängung eines Bußgeldes“ vom 10.3.21: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/03/20210310_PM_VfB-Stuttgart_Abschluss_Bussgeldverfahren.pdf

Datenschutz geht zur Schule - Der VfB geht mit: https://www.vfb.de/de/1893/club/vfb-e-v-/datenschutz/ <<

nahmen, um das technische und organisatorische Datenschutzniveau zu verbessern und um junge Menschen für Datenschutzanliegen zu sensibilisieren. Dazu gehört in Abstimmung mit uns eine aktive Mitwirkung am Projekt „Datenschutz geht zur Schule“. Der VfB engagiert sich dabei als Botschafter für Datenschutz bei Kindern und Jugendlichen. Das Projekt „Datenschutz geht zur Schule“ ist eine Initiative des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e.V., die die Schülerinnen und Schülern zu den Themen Datenschutz und IT-Sicherheit sensibilisiert. Ein bewusster Umgang mit eigenen und fremden Daten und Informationen steht im Mittelpunkt. Wir unterstützen dieses Projekt seit inzwischen mehr als 10 Jahren, bei dem Datenschutzexpert_innen bundesweit Schulen mit Unterrichtskonzepten besuchen.

In diesem Zusammenhang wurden im Berichtszeitraum von uns und dem VfB verschiedene Maßnahmen angestoßen oder bereits umgesetzt: So gab es einen Online-Elternabend für die Eltern der jüngeren Nachwuchsspieler mit dem Vorstandsvorsitzenden der VfB Stuttgart 1893 AG, Thomas Hitzlsperger, und dem Landesbeauftragten persönlich. Durch Kooperation von VfB und unserem Fachbereich „Datenschutz als Kulturaufgabe“ wurde eine Präsenz für das Projekt auf der Homepage des VfB geschaffen, auf der im Laufe der Saison Videos veröffentlicht werden, die verschiedene Aspekte von Datenschutz erläutern und nützliche Tipps geben, welche an Kinder und Jugendliche, aber auch an Erwachsene gerichtet sind.

Beginnend im Sommer wurden zudem eine Reihe von Datenschutzschulungen für das VfB-Nachwuchsleistungszentrum durchgeführt. Hierfür hat unser Bildungszentrum BIDIB in enger Zusammenarbeit mit der Initiative „Datenschutz geht zur Schule“ Schulungskonzeptionen für die Nachwuchsmannschaften im Fußballbereich ausgearbeitet. Insgesamt wurden in neun Schulungen durch Referent_innen des LfDI alle Jugendmannschaften des VfB (U11 bis U21) für den sicheren und bewussten Umgang mit dem Internet und den sozialen Medien sensibilisiert.

10.2 Herausforderung Corona-Pandemie

Die Corona-Pandemie hat auch vor der Bußgeldstelle nicht Halt gemacht und deren Arbeit in verschiedenster Weise beeinflusst.

Sportler_innen sind Vorbilder und können sich wirksam für Datenschutz einsetzen – so wie der VfB Stuttgart.

Zum einen wurden Datenschutzverstöße in Zusammenhang mit pandemiebedingten Datenverarbeitungen verfolgt und sanktioniert: So gelangen immer wieder Vorgänge zur Anzeige, bei denen Kontaktdaten, die allein zum Zwecke der Kontaktnachverfolgung im Falle einer Corona-Infektion auf Grundlage der Corona-VO Baden-Württemberg angegeben werden, von Inhabern oder Beschäftigten zu privaten Zwecken, etwa zur Kontaktaufnahme, genutzt werden. Auch die unsachgemäße Aufbewahrung und Entsorgung personenbezogener Daten, was einen Verstoß gegen den Grundsatz der Integrität und Vertraulichkeit nach Art. 5 Abs. 1 Buchst. f DS-GVO darstellt, mündete wiederholt in Bußgeldverfahren. So waren z. B. Corona-Kontaktlisten oder Testergebnisse offen einsehbar oder wurden ohne vorheriges Anonymisieren oder „Schreddern" im Wald oder in der normalen Altpapiertonne entsorgt.

In einem solchen Fall, in dem Gesundheitsdaten in einer für eine Vielzahl von Personen zugänglichen Papiertonne entsorgt wurden, erwirkte die Bußgeldstelle, als es die pandemische Lage wieder zuließ, einen Durchsuchungsbeschluss beim zuständigen Amtsgericht und führte eine Durchsuchung auf dieser Grundlage durch. Hierbei konnten eine Vielzahl relevanter Unterlagen sichergestellt werden, die derzeit ausgewertet werden.

Zum anderen hatte die Corona-Pandemie auch Auswirkungen auf die Arbeitsweise der Bußgeldstelle. Wie schon im Vorjahr hat die Bußgeldstelle auch im aktuellen Berichtszeitraum die wirtschaftlichen Belastungen mit zum Teil erheblichen Umsatzeinbußen vor allem bei juristischen Personen besonders berücksichtigt. In Einzelfällen, in denen die verantwortlichen Stellen über längere Zeit keine oder keine nennenswerten Einnahmen generieren konnten, wurde deshalb aus Verhältnismäßigkeitsgründen von der Verhängung einer Geldbuße gänzlich abgesehen, wenn der rechtmäßige Zustand zwischenzeitlich (wieder) hergestellt wurde und der Datenschutzverstoß im konkreten Fall nicht so schwer wog, dass es einer darüberhinausgehenden Ahndung bedurfte.

Ließ die Schwere des Verstoßes oder andere gewichtige Faktoren ein solches Absehen von der Geldbuße nicht zu, so führten die häufig pandemiebedingten finanziellen Belastungen mancher Unternehmen in einigen Fällen dennoch zu erheblichen Reduzierungen der Geldbußen. Dies zeigt einmal mehr, dass es das Selbstverständnis der Bußgeldstelle ist, Geldbußen nur in Einzelfällen zu verhängen, wenn Datenschutzverstöße auch unter Berücksichtigung sonstiger Abhilfemöglichkeiten gem. Art. 58 Abs. 2 DS-GVO sanktionsbedürftig erscheinen.

10.3 „... Kontrolle ist besser?"

Wie im letzten Tätigkeitsbericht ausführlich dargestellt (S. 62 im Tätigkeitsbericht 2020), sind die verschiedensten Formen der Videoüberwachung immer wieder Gegenstand von Bußgeldverfahren. Dieses Jahr sah sich die Bußgeldstelle mit einem speziellen Fall der Videoüberwachung konfrontiert, der bei einer zeit- und personalintensiven Durchsuchung umfangreiches Beweismaterial erbrachte.

Ganz nach dem „Motto Vertrauen ist gut – Kontrolle ist besser" hatte der Eigentümer eines Gebäudekomplexes im Innen- und Außenbereich cirka 50 Videokameras angebracht. Im Innenbereich wurden Wohnungseingänge und die Flure überwacht. Daneben war das Ladengeschäft des Verantwortlichen mit einer Vielzahl von Videokameras ausgestattet. Nahezu jeder Bereich des Geschäfts wurde von Videokameras erfasst, so dass auch das Personal zwangsläufig einer ständigen Überwachung ausgesetzt war. Nachdem die Bußgeldstelle beim zuständigen Amtsgericht einen entsprechenden Beschluss erwirkt hatte, konnten bei der anschließenden Durchsuchung cirka 50 TB Videomaterial gesichert werden, die nunmehr im Detail ausgewertet werden.

11. Datenschutz-Vielfalt, veranschaulicht von Fall zu Fall

11.1 Neues aus dem Amt 1: Innere Sicherheit, Justiz, Kommunalwesen

11.1.1 Pleiten, Pech und Datenpannen

Nicht nur beim Versand von E-Mails an einen Verteiler mit mehreren E-Mail-Adressen, sondern auch beim Versand von Postsendungen müssen die Absendenden Sorgfalt walten lassen, damit die E-Mail-Adressen nicht allen Empfänger_innen offengelegt beziehungsweise die Post nicht an die falschen Empfangenden gesandt wird.

Unter den zahlreichen Datenpannenmeldungen befinden sich auch immer wieder Meldungen von Verantwortlichen und Betroffenen, welche mitteilen, dass eine E-Mail an einen für alle offen einsehbaren Verteiler versandt wurde, obwohl hierfür keine Notwenigkeit bestand. So wurde uns kürzlich eine Datenpanne gemeldet, bei welcher durch einen offenen Verteiler mehr als 400 E-Mail-Adressen offengelegt wurden. Neben der Personenbeziehbarkeit vieler E-Mail-Adressen, z. B. durch Vor- und Nachname als Bestandteil der Adresse, konnte durch den Inhalt der E-Mail nicht ausgeschlossen werden, dass hierdurch auch Gesundheitsdaten der Empfänger_innen für alle offengelegt wurden. Eine abschließende Bewertung steht derzeit noch aus. Begründet wird die Versendung von E-Mails mittels Verteiler häufig damit, dass eine Versendung von einzelnen E-Mails wesentlich mehr Zeit in Anspruch nehmen würde. Grundsätzlich besteht aus datenschutzrechtlicher Sicht die Möglichkeit, E-Mails an einen größeren Kreis von Empfänger_innen zu versenden. Hierbei ist allerdings zu beachten, dass die E-Mail-Adressen eines Verteilers z. B. durch Einfügung ins Cc „carbon copy" („Durchschlag") nur offengelegt werden dürfen, sofern dies erforderlich sein sollte. Ansonsten muss der Verteiler in das Feld Bcc „blind carbon copy" („verdeckter/unsichtbarer Durchschlag") eingefügt werden. Hierdurch wird die Offenlegung der E-Mail-Adressen vermieden.

Vor einiger Zeit erreichte uns auch eine Postsendung auf Abwegen. Beim Posteingang wurden drei Akten mit zahlreichen personenbezogenen Daten festgestellt, welche sich zunächst keinem unserer Vorgänge zuordnen ließen. Bei näherer Betrachtung mussten wir feststellen, dass diese Akten nicht für uns bestimmt waren, sondern für eine andere öffentliche Stelle und es sich wohl um einen Irrläufer handelte. Die Akten wurden sodann unverzüglich wieder an den Absender zurückgegeben mit der Aufforderung zur Überprüfung, ob eine Datenpanne gemeldet werden muss. Bisher hat uns zu diesem Vorgang noch keine Datenpannenmeldung erreicht. Auch bei der Versendung von Post ist es unerlässlich, zu überprüfen, ob dieses tatsächlich an die richtige Empfängerin oder den richtigen Empfänger gerichtet ist.

Datenpannen, die hauptsächlich auf Unachtsamkeit zurückzuführen sind, können z. B. durch klare Anweisungen, der Einführung von strukturierten Arbeitsabläufen und der Einführung eines Vier-Augen-Prinzips bei besonders anspruchsvollen Tätigkeiten entgegengewirkt werden. Die Verantwortlichen sollten die Achtsamkeit auch bei diesen alltäglichen Arbeitsabläufen den Beschäftigten immer wieder in Erinnerung rufen z. B. durch entsprechende Schulungen, Arbeits- oder Dienstanweisungen.

11.1.2 E-Mail-Accounts von Gerichtsvollzieher_innen

In letzter Zeit konnten wir in verschiedensten Fällen feststellen, dass öffentliche Stellen E-Mail-Provider nutzen, die primär für Privatpersonen gedacht sind. Hierbei stellen sich Fragen nach den rechtlichen Grundlagen der Datenverarbeitung durch diese E-Mail-Provider, die nicht-öffentliche Stellen sind, und nach geeigneten technischen und organisatorischen Maßnahmen.

So sind wir u. a. auf Gerichtsvollzieher_innen hingewiesen worden, die dienstliche Schreiben mit personenbezogenen Daten über E-Mail-Accounts, die primär für Privatpersonen gedacht sind (wie z. B. web.de, outlook.de), versenden. Da es sich bei Gerichtsvollzieher_innen nicht um private Stellen handelt – sie gehören vielmehr jeweils zu einem Amtsgericht, also einer öffentlichen Stelle –, ergibt sich hieraus folgende Problemstellung:

Da personenbezogene Daten verarbeitet werden, sind die Anforderungen der DS-GVO umzusetzen. Mehrere nicht-öffentliche E-Mail Provider verweisen in ihren Nutzungsbedingungen beziehungsweise den Datenschutzinformationen auf ihr berechtigtes Interesse, Inhalts- und Metada-

ten der E-Mail-Kommunikation für eigene Zwecke – wie beispielsweise Werbung – zu verarbeiten. Dass öffentliche Stellen personenbezogene Daten nicht-öffentlichen Stellen für derartige Zwecke zur Verfügung stellen, ist jedoch nicht zulässig. Die Erlaubnistatbestände des Artikels 6 DS-GVO sind hier nicht einschlägig. Teilweise lassen sich derartige Verarbeitungen der E-Mail Provider zwar manuell deaktivieren. Hat die verantwortliche Stelle sichergestellt, dass es keine Verarbeitungen außerhalb der Auftragsverarbeitung gibt, sind jedoch noch weitere Maßnahmen umzusetzen. Um etwa einem gezielten Angriff z. B. durch Phishing vorzubeugen, wäre – dem Stand der Technik entsprechend – eine 2-Faktor-Authentifizierung umzusetzen.

Das Ministerium der Justiz und für Migration, das wir wegen der Nutzung von primär für nicht-öffentliche Stellen gedachten E-Mail-Providern durch Gerichtsvollzieher_innen angeschrieben haben, hat uns mitgeteilt, dass es bestrebt sei, für die aufgezeigte Problematik eine praktikable Lösung zu finden. Es werde insbesondere geprüft, ob und ggf. wie eine Anbindung der Gerichtsvollzieher_innen an das Landesverwaltungsnetz erfolgen könne.

Bei der vorgenannten Fallkonstellation sind auch weitere Punkte zu beachten, die allgemein im Zusammenhang mit dem Versand und der Entgegennahme von E-Mail-Nachrichten zu beachten sind: Hierzu verweisen wir auf die Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ der Datenschutzkonferenz, die aufzeigt, welche Anforderungen an die hierbei eingesetzten Verfahren durch Verantwortliche, ihre Auftragsverarbeiter und E-Mail-Provider auf dem Transportweg zu erfüllen sind.

Darüber hinaus ist anzumerken, dass es, je nach E-Mail-Provider, zu einer Datenübermittlung an Drittstaaten kommen kann. So erfolgt bei der Nutzung eines Outlook-Accounts in der Regel eine Übermittlung personenbezogener Daten in Drittstaaten. Das Urteil EuGH vom 16. Juli 2020, Rechtssache C-311/18 („Schrems II“) betrifft alle öffentlichen und nicht-öffentlichen Stellen und legt Bedingungen für eine rechtmäßige Übermittlung personenbezogener Daten in Drittstaaten fest. Details hierzu finden sich in unserer Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?

Mails verschicken kann man auch sicher. Das ist gar nicht so schwer.

11.1.3 Der unzureichende Briefkasten

Der Verantwortliche und ggf. der Auftragsverarbeiter haben geeignete technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten, etwa vor unbefugter oder unrechtmäßiger Verarbeitung oder dem unbeabsichtigten Verlust, zu treffen. Diese Maßnahmen müssen geeignet sein, ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Bei der dabei vorzunehmenden Verhältnismäßigkeitsprüfung sind unter anderem die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Je nach Fallgestaltung kann die Festlegung bestimmter Handlungsabläufe ausreichen, es können aber auch aufwendige technische Maßnahmen angemessen sein. Die nachfolgend geschilderte Problematik kann durch relativ einfache Maßnahmen gelöst werden:

Im Rahmen einer Beschwerde wurden wir darüber informiert, dass der Briefkasten eines Amtsgerichts keinen Schutz vor unberechtigten Zugriffen biete, eingeworfene Sendungen könnten problemlos entnommen werden. Auf unsere Nachfrage hat das Amtsgericht eingeräumt, dass es an manchen Tagen tatsächlich möglich sei, auf in den Briefkasten des Amtsgerichts eingeworfene Briefe zuzugreifen. Dies könne dann passieren, wenn der Briefkasten um Mitternacht die Post über eine Klappe in einen zweiten Behälter leite (Nachtbriefkasten). Insbesondere größere Briefsendungen würden sich am Behälter verfangen und könnten dann aus dem Briefkasten entnommen werden. Das Problem trete jedoch nur in den frühen Morgenstunden in einem kurzen Zeitfenster von höchstens zwei Stunden auf. Auch wenn umfangreiche Sendungen „fast schon gewaltsam in den Briefkasten gestopft" würden, könne eine Entnahme erfolgen. Hier liege – laut Stellungnahme des Amtsgerichts – die Verantwortung beim Einlieferer, dafür Sorge zu tragen, dass sein Schreiben vor Zugriffen Dritter geschützt werde. Wenn der Briefkasten bereits voll sei, müsse der Einlieferer gegebenenfalls die Leistung der Post in Anspruch nehmen.

Diese Ansicht lässt sich weder mit den Rechtsschutzgarantien des Grundgesetzes noch mit dem Datenschutzrecht vereinbaren. So hat das Bundesverfassungsgericht z. B. in einem Beschluss vom 11. Februar 1976, 2 BvR 652/75 ausgeführt, dass sich aus den Rechtsschutzgarantien des Grundgesetzes eine Verpflichtung der Gerichte ergibt, Bürger_innen die volle Ausnutzung der ihm vom Gesetz eingeräumten Fristen zu ermöglichen. Die Gerichte sind somit verpflichtet, einen Briefkasten zur Verfügung zu stellen, der rund um die Uhr den Einwurf von Briefsendungen ermöglicht, wobei das Gericht durch technische Kontrollvorrichtungen sicherstellen muss, dass der rechtzeitige Eingang fristwahrender Schriftstücke nachgewiesen werden kann.

Mit dem Einwurf in den Briefkasten eines Gerichts gelangen die Briefe in den Einflussbereich des Gerichts. Ab diesem Zeitpunkt muss das Gericht als datenschutzrechtlich verantwortliche Stelle die Briefe durch technische und organisatorische Maßnahmen z. B. vor unbefugten Zugriffen und unbeabsichtigtem Verlust schützen. Dies kann etwa durch mehrmalige Leerungen, einen ausreichend dimensionierten Briefkasten und/oder durch Maßnahmen erreicht werden, die verhindern, dass sich größere Umschläge im Behältnis verfangen.

Durch Nutzung eines Briefkastens, der regelmäßig die Entnahme von Postsendungen ermöglichte, hat das Amtsgericht gegen den in Artikel 5 Absatz 1 Buchstabe f der DS-GVO formulierten Grundsatz der Integrität und Vertraulichkeit verstoßen. Auf unseren dahingehenden Hinweis teilte uns das Amtsgericht mit, dass es Maßnahmen getroffen habe, die sowohl den grundgesetzlichen Rechtsschutzgarantien als auch den datenschutzrechtlichen Anforderungen genügen.

>> Mehr Informationen:

DSK-Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail": https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf

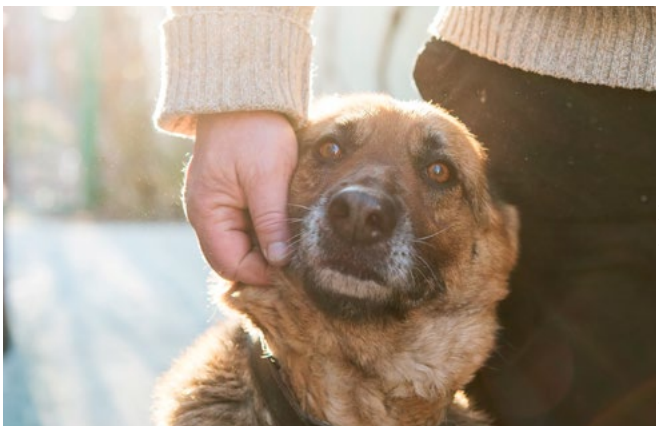
LfDI- Orientierungshilfe „Was jetzt in Sachen internationaler Datentransfer?": https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf <<

11.1.4 Fehlerhafte Adressierung

Von Gerichten werden Tag für Tag unzählige Schriftstücke versandt. Um dies bewältigen zu können, sind die Servicekräfte der Gerichte stark gefordert. Im Eifer des Gefechts kann es passieren, dass einem Anschreiben eine falsche Anlage beigefügt, ein Schreiben falsch adressiert wird oder es zu sonstigen Verwechslungen kommt, die – bleiben diese Versehen unbemerkt – dazu führen, dass Schriftstücke mit sensiblen Daten an die falsche Person verschickt werden.

In einem uns bekannt gewordenen Fall hat ein Amtsgericht in einem strafrechtlichen Ermittlungsverfahren mehrere Beschlüsse erlassen. In diesen wurde jeweils die Sicherstellung von Gegenständen gerichtlich bestätigt, die in Räumlichkeiten zweier Zeugen erfolgt war. Bei der Versendung der Beschlüsse kam es zu einer Verwechslung. Den Zeugen wurde nicht der Beschluss zugeleitet, der sich auf ihre Räumlichkeiten bezog. Vielmehr erhielten die beiden Zeugen jeweils den Beschluss, der sich auf die Räumlichkeiten und die dort sichergestellten Gegenstände des anderen Zeugen bezog.

Das von uns angeschriebene Amtsgericht hat die Datenschutzverletzung sofort eingeräumt, veranlasst, dass die Beschlüsse den richtigen Adressaten zugeleitet werden und die Zeugen aufgefordert, die fälschlicherweise zugeschickten Beschlüsse an das Amtsgericht zurückzusenden. Außerdem wurden die Mitarbeiter_innen der betroffenen Abteilung nochmals für die Belange des Datenschutzes sensibilisiert. Auch wenn es eilt – oder sogar besonders wenn es eilt – sollte vor Versendung eines Schreibens oder auch einer E-Mail überprüft werden, ob die Adressierung korrekt ist und – soweit Anlagen zu übersenden sind – ob die richtigen Anlagen beigefügt sind.



© lenaivanova231 – stock.adobe.com

Manchmal führt einen die Spürnase auf die falsche Fährte.

11.1.5 Übers Ziel hinaus

Die öffentliche Nennung des Namens und der Adresse von Fragestellenden einer Gemeinderatsitzung und/oder die Niederschrift dieser Angaben im Protokoll sind nicht notwendig.

Immer wieder erreichen uns Anfragen von Bürger_innen, welche sich darüber beschweren, dass sie insbesondere im Rahmen der Bürgerfragestunden einer Gemeinderatssitzung, um eine Frage überhaupt stellen zu dürfen, dazu aufgefordert werden, Name und Adresse öffentlich zu nennen. Nicht selten werden Name und Anschrift auch ins Protokoll aufgenommen und in einigen Fällen werden die Protokolle ohne Unkenntlichmachung der personenbezogenen Daten der Fragestellenden veröffentlicht. Begründet wird dies damit, dass hierdurch die Frageberechtigung der Fragestellenden überprüft werde.

Eine öffentliche Nennung des Namens ist allerdings nicht notwendig, um die Frageberechtigung zu überprüfen. Vielmehr kann die Frageberechtigung auch durch das nicht öffentliche Vorzeigen des Personalausweises nachgeprüft werden, sodass es im Anschluss nicht mehr erforderlich sein wird, Name und Adresse öffentlich zu nennen und zu protokollieren. Der notwendige Inhalt eines Protokolls ist in § 38 Abs. 1 GemO geregelt. So sind der wesentliche Inhalt der Verhandlung, der Name der Vorsitzenden oder des Vorsitzenden, die Zahl der anwesenden und Namen der abwesenden Gemeinderätinnen und Gemeinderäte, der Gegenstand der Verhandlung, die Anträge und die Wahlergebnisse sowie der Wortlaut der Beschlüsse zu protokollieren. Eine Protokollierungspflicht der Fragestellenden ergibt sich daraus gerade nicht. Die Fragestunde schafft die Möglichkeit, Bürger_innen in den Willensbildungsprozess des Gemeinderats einzubeziehen. Werden Name und Adresse in der Niederschrift protokolliert beziehungsweise gibt es nur dann ein Fragerecht, wenn der Name öffentliche genannt wird, dann könnte dies abschreckend wirken und eine Einschränkung der politischen Teilhabe in den Kommunen bedeuten. Eine datenschutzrechtliche Rechtsgrundlage für die öffentliche Nennung und/oder Erfassung von Namen und Adressen von Bürger_innen in der Bürgerfragestunde ist nicht vorhanden.

11.1.6 Auf den Hund gekommen

Streitereien über Erbschaften haben schon so manchem Familienglück einen Knacks beschert. Dabei kann es auch mal darum gehen, wessen Hundesteuer Mama vor ein paar Jahren bezahlt hat. Eine bei der Faktenschaffung um Hilfe gebetene Gemeinde darf jedoch den Datenschutz nicht vergessen.

In diesem Fall hatte sich eine Person an uns gewandt, weil eine Gemeinde ihrer Schwester Kopien ihrer Hundesteuerbescheide zur Verfügung gestellt hatte. Was war passiert? Die Geschwister befanden sich im Streit über das Erbe der gemeinsamen Mutter. Um nachvollziehen zu können, ob die Mutter in den vergangenen Jahren teilweise die Hundesteuer der beschwerdeführenden Person bezahlt hatte, hatte sich die Schwester kurzerhand an die für diese Steuer zuständige Gemeinde gewandt und um Auskunft gebeten. Bei der Hundesteuer handelt es sich nämlich um eine kommunale Abgabe, die die jeweiligen Gemeinden durch Satzung erheben dürfen. In der Annahme, die Schwester habe als Erbin ein berechtigtes Interesse an dieser Information, wurde ihr tatsächlich jeweils die erste Seite mehrerer Hundesteuerbescheide übermittelt. Diese Hilfsbereitschaft ist jedoch unzulässig! Nicht nur, dass es für die Herausgabe dieser Information keine Rechtsgrundlage gab, die Hundesteuer genießt auch noch besonders hohen Schutz: gem. § 3a Nr. 1 Buchst. c Kommunalabgabengesetz (KAG) gilt für sie nämlich auch das Steuergeheimnis aus § 30 Abgabenordnung (AO). Zwar regelt § 3a Nr. 1 Buchst. c KAG auch Ausnahmen vom Steuergeheimnis im Falle der Hundesteuer, hier war jedoch keine dieser Ausnahmen erfüllt.

Also: Für die Hundesteuer gilt das Steuergeheimnis und auch sonst der allgemeine datenschutzrechtliche Grundsatz, dass es für jede Datenverarbeitung eine Rechtsgrundlage braucht. Alleinig ein „berechtigtes Interesse" ist dies im Übrigen nie: Art. 6 Abs. 1 UA. 1 Buchst. f. DS-GVO benennt zwei weitere zu prüfende Voraussetzungen – und für öffentliche Stellen steht diese Rechtsgrundlage ohnehin grundsätzlich nicht zur Verfügung, siehe Art. 6 Abs. 1 UA. 2 DS-GVO.

11.1.7 Weihnachtsmärkte, Corona und nicht der Datenschutz

Um den Gewerbetreibenden das Geschäft auf dem Weihnachtsmarkt unter Einhaltung von Corona-Maßnahmen dennoch zu ermöglichen, suchte man nach einer praktischen Lösung – hat aber manchmal den Datenschutz vergessen.

Ein zweites Jahr ohne Weihnachtsmarkt ist nicht nur für seine potentiellen Gäste sehr schade, auch für die Standbetreiber_innen war diese Aussicht schlimm, konnte es schließlich sogar das Ende einer wirtschaftlichen Existenz bedeuten. So ist es mehr als nachvollziehbar, dass man nach Möglichkeiten suchte, Weihnachtsmärkte trotz Pandemie stattfinden zu lassen. Die CoronaVO sah einen eigenen Paragrafen für sie vor und gab z. B. die Verantwortung für Hygienekonzept usw. nicht den einzelnen Standbetreiber_innen, sondern den Veranstalter_innen des jeweiligen Marktes. Durch sie begegnete uns dann teilweise die Idee, man könne die Gäste doch am Eingang auf ihren G-Status kontrollieren und ihnen dann ein farbiges Bändchen umbinden, damit klar ist: „Diese Person ist kontrolliert und darf sich hier aufhalten, essen und trinken." So weit, so gut, schließlich gibt es solche Bändchen auch bei anderen Events – so manchen Arm hat viele Sommer lang gleich eine ganze Sammlung an Festivals in dieser Form geziert.

Nicht so gut war allerdings die Idee, diese Bändchen für Geimpfte und Genesene dauerhaft in einer Farbe auszugeben, für Getestete hingegen täglich zu wechseln. Denn dies hätte zwangsweise dazu geführt, dass Getestete nicht nur für diejenige Person als solche erkenntlich wären, die sie kontrolliert, sondern auch für alle anderen Personen im Umfeld. Und warum ist das nun so schlimm? Weil es beim Datenschutz auch um Erforderlichkeit geht und nicht unnötig mehr Informationen als nötig erfasst und preisgegeben werden dürfen. Hier ist es selbstverständlich richtig, dass für eine Situation, in der Menschen dicht gedrängt beisammenstehen, das Risiko der Übertragung eines potentiell tödlichen Virus möglichst niedrig zu halten ist. Eben dem dienten die unterschiedlichen Zugangsbeschränkungen durch die Corona-VO, deren Voraussetzung eben die Kontrolle des G-Status und damit eine Verarbeitung eines Gesundheitsdatums ist. Allerdings ist für diesen Zweck nicht erforderlich, dass alle Umstehenden auch wissen, welchen G-Status man nun hat.

Was also tun? Zugangsberechtigung am Eingang prüfen und täglich neue Bändchen für alle ausge-

ben. So müssen die Standbetreiber_innen trotzdem keine Impfnachweise kontrollieren und Gäste müssen kein Gesundheitsdatum für alle offenlegen, wenn sie einen Glühwein trinken gehen wollen.

Es kann so einfach sein. Auch wir sind Fans von praxisnahen Lösungen und helfen gerne beim Finden solcher.

11.1.8 Gemeinderatssitzungen online

Die Verbreitung von Gemeinderatssitzungen über das Internet bietet niedrigschwellig die Möglichkeit, an einer solchen teilzunehmen – ob aus dem Zug, beim Spazierengehen oder auch aus der Badewanne. Datenschutzrechtlich ist das möglich, die verantwortlichen Stellen sollten sich jedoch mit einigen Fragen auseinandersetzen.

Insbesondere in der Pandemie, aber auch sonst, stellen sich Gemeinderäte die Frage, ob sie ihre Sitzungen nicht über das Internet einem größeren Publikum zugänglich machen können. Diese Überlegung schätzen wir grundsätzlich sehr, denn Transparenz und demokratische Teilhabe sind auch uns wichtige Anliegen. Gleichfalls sind jedoch die Rechte und Freiheiten der gefilmten Personen zu berücksichtigen. Aus datenschutzrechtlicher Sicht sollte deswegen vor allem an das Folgende gedacht werden:

>> Mehr Informationen:

Zum Thema Einwilligung: „Datenschutz bei Gemeinden" (ab S. 96): https://www.baden-wuerttemberg.datenschutz.de/datenschutz-bei-gemeinden

Zum Thema Plattform: LfDI-Orientierungshilfe „Was jetzt in Sachen internationaler Datentransfer?": https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf

Zum Thema Soziale Netzwerke: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/02/DE_Richtlinie-zur-Nutzung-sozialer-Netzwerke-durch-%C3%B6ff.-Stellen-20200205.pdf

Zu Videokonferenztools: https://www.baden-wuerttemberg.datenschutz.de/OG-Videokonferenzsysteme <<

Die richtige Rechtsgrundlage

Da es (noch) kein Gesetz zu diesem Thema gibt, kommt als einzige Rechtsgrundlage die Einwilligung der betroffenen Personen nach Art. 6 Abs. 1 UA. 1 Buchst. a DS-GVO in Betracht.

Hinweis: § 37 a GemO regelt nicht die Veröffentlichung einer Gemeinderatssitzung im Internet, sondern die Durchführung einer solchen, wenn nicht alle Mitglieder im Sitzungsraum anwesend sein können. Damit eine Einwilligung wirksam ist, muss insbesondere klar beschrieben werden, welche Verarbeitungen in welchem Umfang erfolgen sollen (z. B. Erheben von Bild und Ton, Verbreiten in Form von Live-Streaming, Speichern bis zum Zeitpunkt X) und zu welchem Zweck. Und: die Entscheidung muss freiwillig sein. Die betroffenen Personen dürfen also z. B. keine Nachteile befürchten, wenn sie nicht mitmachen möchten. Problematisch sind deswegen ganz grundsätzlich Einwilligungen, die in einem Über-Unterordnungsverhältnis gegeben werden sollen, wie z. B. einem Arbeitsverhältnis. Es darf sich aber auch niemand gegenüber dem Staat darüber sorgen müssen, dass man ein Recht nicht ausüben können wird, weil man nicht im Internet ausgestrahlt werden möchte. In diesen beiden Konstellationen wird eine Einwilligung deswegen regelmäßig nicht wirksam – weil nicht freiwillig – sein. Anders ist die Situation aber bei Gemeinderatsmitgliedern. Vor dem Hintergrund des freien Mandats ist davon auszugehen, dass sie grundsätzlich freien Willens entscheiden können. Allerdings muss auch ihnen eine echte Alternative angeboten werden, wenn sie nicht gefilmt werden wollen. Denkbar ist hier z. B. ein leicht zeitverzögertes Streaming, sodass die jeweilige Person vor Ausstrahlung herausgeschnitten werden kann. Auch können mildere Varianten besprochen werden, wie z. B. eine reine Audioaufnahme (anstatt Ton und Bild).

Der Grundsatz der Datenminimierung

Eine Datenverarbeitung soll ihrem Zweck angemessen und auf ein für diesen Zweck notwendiges Maß beschränkt sein, Art. 5 Abs. 1 Buchst. c DS-GVO. Das heißt: So viel wie nötig, so wenig wie möglich! Die verantwortliche Stelle muss sich also mit der Frage beschäftigen, was genau der Zweck ihres Vorhabens ist und welchen Umfang die Aufzeichnung und Verbreitung zur Erfüllung dieses Zweckes haben muss.

Hier sollte bedacht werden, dass es in Gemeinderatssitzungen in aller Regel um Angelegenheiten der örtlichen Gemeinschaft geht. Der lokale Bezug ist nicht ohne weiteres mit einer globalen Verbreitung in Einklang zu bringen. Soll die Übertragung ins Internet also dem Zweck dienen, interessierten Menschen die Teilnahme an der Gemeinderatssitzung digital zu ermöglichen, dann ist jedenfalls ein Live-Streaming der Veranstaltung ausreichend. Ein dauerhaftes Zurverfügungstellen im World Wide Web ist für diesen Zweck nicht erforderlich. Im Übrigen folgt aus der Zweckerfüllung auch, dass die Aufnahmen insgesamt zu löschen sind. Sie dürfen also auch intern nicht aufbewahrt werden.

Angemessene technische und organisatorische Maßnahmen

Die verantwortliche Stelle muss angemessene Tools verwenden. Für ein Live-Streaming stellt sich da insbesondere die Frage der „richtigen" Plattform. Möchte eine Gemeinde auf einen externen Anbieter zugreifen, sollte sie eingängig prüfen, ob und wenn ja welche personenbezogenen Daten der externe Anbieter auf welche Art verarbeitet. Zusätzliche Funktionen, wie z. B. eine automatische Transkription, sollten kritisch hinterfragt werden, da sie gegebenenfalls weitere Datenübermittlungen erfordern. Konkret ist insbesondere Folgendes zu bedenken: Verarbeitet die Plattform die Aufnahmen oder auch personenbezogene Informationen der Zuschauer_innen zu eigenen Zwecken, kommt eine gemeinsame Verantwortlichkeit in Betracht („Facebook-Fanpage"). Folge einer solchen ist u. a. die Pflicht, in einer Vereinbarung festzulegen, wer welche Verpflichtung der DS-GVO erfüllt, insbesondere im Hinblick auf die Rechte betroffener Personen. Handelt es sich dagegen um einen Auftragsverarbeiter, so muss eine Auftragsverarbeitungsvereinbarung getroffen werden. Bei einem externen Anbieter ist auch zu untersuchen, ob Datenverarbeitungen im außereuropäischen Ausland stattfinden und wie Daten dort geschützt sind („Schrems-II"). Geprüft werden kann jedoch auch, ob nicht eine hinreichende eigene Infrastruktur besteht oder aufgebaut werden kann, um ein Streamen z. B. über die gemeindliche Homepage laufen zu lassen.

Ein digitales Zurverfügungstellen von Gemeinderatssitzungen ist datenschutzrechtlich also umsetzbar. Wesentliche Voraussetzung ist die Auseinandersetzung mit dem Zweck und dem dafür

Live-Streams von Gemeinderatssitzungen sind mit guter Technik und Organisation möglich.

notwendigen Umfang von Datenverarbeitungen, sowie den Merkmalen einer wirksamen Einwilligung und den geeigneten technischen und organisatorischen Maßnahmen.

Bei der Entscheidung für ein Videokonferenztool für Sitzungen, die von vorne herein nicht analog stattfinden (können), haben wir außerdem nützliche Hinweise in unserer Handreichung „Videokonferenzsysteme – Hinweise zur praktischen Nutzung" formuliert.

11.1.10 Kooperierende Rechtsanwaltskanzleien: Datenübermittlung erfordert Einwilligung der Mandantschaft

Durch eine Kooperation mit anderen Rechtsanwaltskanzleien können Synergieeffekte beispielsweise bei der Mandatsakquise genutzt werden. Allerdings darf dies nicht zu Lasten der Betroffenenrechte von potentiellen Mandantinnen und Mandanten gehen.

Rechtsanwaltskanzleien sind häufig in der Form von Partnerschaftsgesellschaften organisiert. Die Briefbögen solcher Partnerschaftsgesellschaften weisen üblicherweise eine Aufzählung sämtlicher Partnerinnen und Partner auf. Je länger die Liste, desto schlagkräftiger die Kanzlei – so wird es der Mandantschaft und Gegner_innen vermittelt. Kein Wunder also, wenn kleine Partnerschaftsgesellschaften mit nur zwei oder drei Rechtsanwältinnen und Rechtsanwälten versuchen, es den großen nachzutun, und sich nach außen präsentieren, als handele es sich um eine viel größere Einheit. Aus datenschutzrechtlicher Sicht ist dies jedoch dann problematisch, wenn für betroffene Personen nicht deutlich ist, wer Verantwortlicher gem. Art. 4 Nr. 7 DS-GVO ist beziehungsweise wann eine Übermittlung an eine andere Partnerschaftsgesellschaft stattfindet.

Besonders raffiniert gestalteten mehrere kooperierende Partnerschaftsgesellschaften ihr Auftreten in einem Fall, in dem ein Mandant eine Beschwerde bei uns einreichte. Drei selbständige Partnerschaftsgesellschaften verwenden eine nicht eingetragene Wort-/Bildmarke, die prominent in großer Schrift und zentral auf dem Briefkopf sämtlicher Schreiben sowie auf dem gemeinsamen Internetauftritt der Kanzleien abgebildet ist. Im rechten Randbereich der Briefbögen waren zunächst die Partnerinnen und Partner sämtlicher Partnerschaftsgesellschaften aufgelistet, wobei eine Sortierung danach erfolgte, in welcher Stadt die jeweilige Person tätig ist. Dies entspricht grundsätzlich dem Sitz der jeweiligen Partnerschaftsgesellschaft, wobei jedoch eine Partnerschaftsgesellschaft in zwei verschiedenen Städten vertreten ist. Aus der Auflistung wurde somit nicht deutlich, dass die genannten Personen tatsächlich teilweise unterschiedlichen Partnerschaftsgesellschaften angehören. In der Fußzeile wurde wiederum nur der Name derjenigen Partnerschaftsgesellschaft genannt, die den Briefbogen im konkreten Fall verwendete. Neben der eigenen Anschrift wurden darüber hinaus die Anschriften der anderen Partnerschaftsgesellschaften angegeben, ohne dass daraus hervorging, dass es sich um andere Partnerschaftsgesellschaften handelt. Den Empfänger_innen der Schreiben wurde somit suggeriert, es handele sich um eine Partnerschaftsgesellschaft mit bundesweiten Standorten und über vierzig Partnerinnen und Partnern, obwohl eine der Partnerschaftsgesellschaften tatsächlich nur aus einem Partner und einer Partnerin besteht.

In dem Fall, der zu einer Beschwerde bei uns führte, hatte ein Mandant zunächst eine der drei Partnerschaftsgesellschaften beauftragt. Im Laufe des Mandats stellte sich heraus, dass möglicherweise zusätzlich eine Fachanwältin für Strafrecht beauftragt werden musste. Die Fachanwältin für Strafrecht gehört einer der kooperierenden Partnerschaftsgesellschaften an. Daraufhin wurden personenbezogene Daten des Mandanten an die Fachanwältin für Strafrecht übermittelt, wozu auch eine Patient_innenakte des Mandanten zählte. Diese sollte prüfen, ob den Unterlagen strafrechtlich relevante Vorwürfe entnommen werden könnten. Nach Prüfung der Unterlagen durch die Fachanwältin für Strafrecht wurde deren Partnerschaftsgesellschaft gesondert beauftragt. Der Mandant teilte uns mit, dass er erst dadurch erfahren habe, dass die Fachanwältin für Strafrecht tatsächlich Partnerin einer anderen Partnerschaftsgesellschaft ist. Zum Zeitpunkt der Übermittlung seiner personenbezogenen Daten sei ihm dies nicht bekannt gewesen.

Bei den beiden Partnerschafsgesellschaften handelt es sich um zwei selbständige Verantwortliche gem. Art. 4 Nr. 7 DS-GVO. Für die Übermittlung der

personenbezogenen Daten bedurfte es somit gem. Art. 6 Abs. 1 DS-GVO einer Rechtsgrundlage. In der Regel verarbeiten Rechtsanwältinnen und Rechtsanwälte die personenbezogenen Daten ihrer Mandantinnen und Mandanten auf der Grundlage von Art. 6 Abs. 1 Unterabs. 1 Buchst. b Alt. 1 DS-GVO, da sie mit ihrer Mandantschaft einen Geschäftsbesorgungsvertrag abgeschlossen haben und die Verarbeitung zu dessen Erfüllung erforderlich ist. Die Mandatierung der Partnerschaftsgesellschaft der Fachanwältin für Strafrecht erfolgte jedoch erst zu einem späteren Zeitpunkt, sodass Art. 6 Abs. 1 Unterabs. 1 Buchst. b Alt. 1 DS-GVO nicht als Rechtsgrundlage herangezogen werden kann. Bei der Prüfung von Unterlagen im Vorfeld einer Mandatierung könnte es sich zwar um eine vorvertragliche Maßnahme im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. b Alt. 2 DS-GVO handeln.

Dies würde jedoch voraussetzen, dass die Maßnahme auf Anfrage der betroffenen Person erfolgte. Anhaltspunkte für eine solche Anfrage lagen nicht vor. Somit bedurfte es einer Einwilligung gem. Art. 6 Abs. 1 Unterabs. 1 Buchst. a DS-GVO i. V. m. Art. 7 DS-GVO. Das Bedürfnis einer Einwilligung ergibt sich zudem aus Art. 9 Abs. 1, Abs. 2 Buchst. a DS-GVO, da mit der Patient_innenakte Gesundheitsdaten übermittelt wurden. Eine Einwilligung konnte weder von der übermittelnden noch von der empfangenden Partnerschaftsgesellschaft nachgewiesen werden.

Aufgrund der Gestaltung des Briefpapiers der Partnerschaftsgesellschaften besteht zudem die Gefahr, dass Briefpost, die für eine andere Partnerschaftsgesellschaft bestimmt ist, an die Adresse einer kooperierenden Kanzlei versendet wird und dort die personenbezogenen Daten verarbeitet werden, ohne dass eine Rechtsgrundlage hierfür besteht.

Wir haben beide Partnerschaftsgesellschaften zur Stellungnahme aufgefordert und auf die datenschutzrechtlichen Probleme hingewiesen. Daraufhin wurden die Briefbögen überarbeitet und neue Musterformulare zur Einwilligung in die Übermittlung personenbezogener Daten erstellt. Darüber hinaus haben die kooperierenden Partnerschaftsgesellschaften Auftragsverarbeitungsverträge abgeschlossen, um Fälle abzudecken, in denen beispielsweise Briefpost zwischen den Kanzleien weitergeleitet wird.

Eine Übermittlung von personenbezogenen Daten eines potentiellen Mandanten an eine andere Partnerschaftsgesellschaft ist zulässig, wenn die Voraussetzungen einer Einwilligung gem. Art. 6 Abs. 1 Buchst. a DS-GVO i. V. m. Art. 7 DS-GVO vorliegen. Sind besondere Kategorien personenbezogener Daten betroffen, ist zusätzlich Art. 9 DS-GVO zu beachten.

11.2 Neues aus dem Amt 2: Gesundheits-, Sozial-und Bildungswesen

11.2.1. Umgang mit Patient_innendaten im Krankenhaus: Die nicht therapierelevante HIV-Erkrankung

Täglich werden in Krankenhäusern Patient_innen wegen verschiedenster Erkrankungen behandelt. Um die Behandlung nach dem medizinischen Standard durchführen zu können, müssen dabei eine ganze Reihe von personenbezogenen Daten erhoben und weiter verarbeitet werden. Hierzu gehören vor allem auch die von der Datenschutz-Grundverordnung (in Artikel 9 DS-GVO) als besonders schutzwürdig eingestuften besonderen Kategorien personenbezogener Daten in Form von Gesundheitsdaten. Deren Offenbaren gegenüber Dritten ist für die Betroffenen vielfach äußerst unangenehm und kann weitereichende nachteilige Folgen haben. Umso wichtiger ist es daher, dass der Datenschutz in diesem Bereich nicht vernachlässigt wird.

Dabei ist es angesichts der allgemeinen Umstände der Arbeit im Krankenhaus nicht immer leicht, die Anforderungen des Datenschutzes einzuhalten. Gerade im Krankenhauswesen steht das Personal bei der Behandlung der Patient_innen vielfach wegen des hohen Arbeitsanfalls unter enormen zeitlichen Druck. Hinzu kommen Situationen, in denen ein rasches Handeln des Personals gefordert ist, um dadurch das Leben und die Gesundheit der Patient_innen schützen zu können (z. B. bei medizinischen Notfällen). Auch die räumlichen Verhältnisse z. B. in Mehrbettzimmern können die erforderliche Diskretion erschweren. Gleichwohl ist es eine wesentliche Aufgabe der Verantwortlichen in Krankenhäusern sicherzustellen, dass der Datenschutz ausreichend gewahrt wird und angemessene technische und organisatorische Maßnahmen umgesetzt werden.

In dem Fall eines an HIV erkrankten Patienten, der aus Anlass einer ganz anderen Erkrankung ein Krankenhaus in Baden-Württemberg aufsuchte, ist dies in mehrfacher Hinsicht nicht gelungen: In seiner an uns gerichteten Beschwerde schilderte er, dass das ärztlichen Personal des Krankenhauses ihn im Rahmen einer Visite vor anderen Mitpatient_innen und bei offener Zimmertür auf seine HIV-Infektion angesprochen habe. Die Ärzt_innen hätten ihn ermahnt, dass er zum Schutz des Personals verpflichtet sei, stets aktiv auf seine HIV-Erkrankung hinzuweisen, so etwa vor der Blutabnahme oder einer Wundversorgung. Andernfalls könne ein HIV-Patient der Klinik verwiesen werden. Selbst der zuständige Oberarzt, an den sich der Betroffene daraufhin gewandt habe, habe dem zugestimmt und sei auch der Beschwerde des Betroffenen über den Umstand, dass das Gespräch über die HIV-Infektion von Dritten habe mitgehört werden können, entgegengetreten: Diagnosen könnten in Anwesenheit von Mitpatient_innen besprochen werden.

Im Rahmen des Beschwerdeverfahrens hat sich unsere Behörde zunächst mit der juristischen Frage auseinandergesetzt, ob und inwieweit überhaupt die Erhebung der Information über die HIV-Infektion datenschutzrechtlich gerechtfertigt und gar die von dem Klinikpersonal postulierte Auskunfts- und Hinweispflicht des Patient_innen gegenüber diesem besteht, ob also der Patient im Falle einer Infektionserkrankung (z. B. HIV-Erkrankung) tatsächlich das Personal aktiv informieren muss.

Für die Verarbeitung dieses Gesundheitsdatums müsste der Klinik nicht nur eine Ausnahme vom Verbot der Verarbeitung aus Artikel 9 Absatz 1 DS-GVO, sondern auch eine Rechtsgrundlage nach Artikel 6 Absatz 1 DS-GVO zugestanden haben. Üblicherweise werden im Rahmen einer ärztlichen Behandlung die erforderlichen Gesundheitsdaten zur Anamnese der Patient_innen auf der Grundlage von Artikel 6 Absatz 1 Buchstabe b, Artikel 9 Absatz 2 Buchstabe h DS-GVO erhoben und weiterverarbeitet, wenn und soweit die Verarbeitung im Rahmen des Behandlungsvertrages mit Patient_innen für die medizinische Diagnostik, die Versorgung und Behandlung (einschließlich Dokumentation und Abrechnung) erforderlich ist.

Hier allerdings spielte die HIV-Infektion des Betroffenen für die ihn betreffende Diagnostik oder die Entscheidung über seine Therapie keine Rolle; die behandelnden Ärzt_innen machten vielmehr geltend, die Kenntnis der Infektion sei zum Schutz des Klinikpersonals erforderlich. Nun kann grundsätzlich auch die Verarbeitung von Gesundheitsdaten, deren Kenntnis zum Schutz der behandelnden Personen oder von Mitpatientinnen und Mitpatient_innen erforderlich ist, insbesondere um Übertragungen von Krankheitserregern im Krankenhaus zu vermeiden, auf die genannten Rechtsgrundlagen gestützt werden.

Allerdings gehört der Umstand, dass eine Patientin oder ein Patient mit HIV infiziert ist, nicht zu den Informationen, deren Kenntnis zur Vermeidung von Ansteckungen erforderlich ist. Eine Erhebung dieses Gesundheitsdatums ist vielmehr weder zum Schutz des Personals noch zum Schutz der Mitpatientinnen oder Mitpatient_innen erforderlich. Nach den derzeit geltenden Empfehlungen der Kommission für Krankenhaushygiene und Infektionsprävention (KRINKO) des Robert Koch-Instituts (RKI) ist bei der Behandlung von Patient_innen mit blutübertragbaren Erregern (wie HIV) vielmehr die Einhaltung von Basishygienemaßnahmen (Standard Precautions) ausreichend.

So müsse beispielsweise bei Tätigkeiten, bei denen ein Kontakt mit virushaltigen Körperflüssigkeiten möglich sei, Schutzhandschuhe getragen oder bei Tätigkeiten, bei welchen blutkontaminierte Aerosole entstehen können, ein mehrlagiger Mund-Nasen-Schutz sowie eine Schutzbrille benutzt werden. Diese Basishygiene gelte bei jeder Form der Patient_innenversorgung. In Bezug auf Zahnärzte weisen beispielsweise auch die Bundeszahnärztekammer und die Deutsche Aidshilfe übereinstimmend darauf hin: Für die Behandlung von HIV-Patient_innen müssen (unabhängig von der Viruslast) in der Zahnarztpraxis keine zusätzlichen Maßnahmen zur Hygiene und zum Arbeitsschutz getroffen werden. Und das Sozialministerium Baden-Württemberg führt in seiner Informationsbroschüre „Das Zahnärzte-HIV-Projekt Baden-Württemberg“ (2017, S. 16) zu Recht aus, dass jede Offenlegung der bekannten HIV-Infektion eines Patienten zu vermeiden ist:

„Viele Menschen mit HIV erleben, dass in ärztlichen Einrichtungen ihr HIV-Status ohne ihre Zustimmung an weitere Personen weitergegeben wird. Ein ‚Warnhinweis‘ zum Beispiel auf der Krankenakte oder ei-

*nem Dokumentationsbogen ist unnötig, weil für alle Patient*innen die gleichen Hygiene- und Schutzmaßnahmen gelten. Außerdem könnte ein solcher Vermerk auch von anderen gesehen werden und stellt einen Verstoß gegen den Datenschutz dar. Aus diesem Grund sollten Akten auch nicht offen am Tresen herumliegen. Auf Überweisungen sollte eine HIV-Diagnose – auch in verschlüsselter Form – nur nach Absprache mit Patient*innen eingetragen werden. In den meisten Fällen besteht keine medizinische Notwendigkeit dafür, den HIV-Status auf der Überweisung festzuhalten. Kommen Patient*innen in Begleitung ihres Partners oder eines Verwandten, berücksichtigen Sie [Anm. LfDI: gemeint ist die angesprochen Zahnärztin/der angesprochen Zahnarzt], dass diese Personen nicht ohne Einwilligung von medizinischen Diagnosen erfahren dürfen."*

Diese Hinweise leiten zur einer weiteren Thematik über, die von den behandelnden Ärzten im Fall unseres Beschwerdeführers nicht ausreichend beachtet wurde: Die Datenschutz-Grundverordnung sieht vor, dass der für eine Datenverarbeitung Verantwortliche unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten insbesondere vor unberechtigter Offenlegung umzusetzen hat (vgl. Art. 24, 25 und 32 DS-GVO; siehe in diesem Zusammenhang auch die „Orientierungshilfe Krankenhausinformationssysteme" der Datenschutzkonferenz, welche als Richtschnur für alle beteiligten Aufsichtsbehörden, Krankenhausbetreiber und Softwareanbieter dienen soll). In Arztpraxen sind daher die räumlichen Verhältnisse tunlichst so anzupassen und Gespräche so zu führen, dass vertrauliche Inhalte wie insbesondere Diagnosen nicht durch Dritte mitverfolgt werden können (s. hierzu schon unseren Artikel „Diskretion in der Arztpraxis", S. 107 im 34. Tätigkeitsbericht 2018).

In Krankenhäusern können freilich diese Bedingungen aufgrund der räumlichen Verhältnisse und der eilbedürftigen Abläufe nicht immer uneingeschränkt hergestellt und eingehalten werden, man denke etwa an voll belegte (Intensiv-)Stationen oder Notfallaufnahmen. Aber auch in Krankenhäusern ist es keinesfalls so, dass Diagnosen stets ohne Weiteres in Anwesenheit von Mitpatient_innen besprochen werden dürften, wie sich das ärztliche Personal im Falle unseres Beschwerdeführers eingelassen haben soll. Soweit die Diskretion aus zeitlichen und räumlichen Gründen nicht bereits vor Beginn des Gesprächs hergestellt werden kann, sind Patient_innen wenigstens zu Beginn des Gesprächs (z. B. im Rahmen der Visite) diskret zu befragen, ob die nachfolgende Besprechung vor den anwesenden Mitpatient_innen stattfinden darf. Für den Fall, dass die/der Patient_in hiermit nicht einverstanden ist, sollte nach Möglichkeit, also nach Mobilität der Patient_innen oder Mitpatient_innen, ein separater Gesprächsraum aufgesucht werden. Bei besonders sensiblen Gesprächen sollte von vornherein versucht werden, den Patient_innen temporär in eine andere Räumlichkeit zu verlegen oder notfalls einen mobilen Raumteiler einzusetzen. Ausreichend kann hierzu beispielsweise sein, wenn die Station über zwei Raumteiler verfügt, auf welche im Bedarfsfall zurückgegriffen werden kann und mit denen auch in einem Mehrbettzimmer mit drei Personen eine Schutzmöglichkeit hergestellt werden kann. Überdies sollte darauf geachtet werden, dass bei der Visite die Besucher_innen der Mitpatient_innen und Patient_innen, sofern keine ausdrückliche Einwilligung seitens der Patient_innen vorliegt, das Zimmer für den Zeitraum der Visite verlassen. Auch gegenüber solchen Besucher_innen kann notfalls ein mobiler Raumteiler die Diskretion wahren. In medizinischen Notfällen lassen sich die Rahmenbedingungen hingegen nicht bestimmen, sodass es dann auf den individuellen Einzelfall ankommt.

Die Relevanz dieser Thematik bleibt, nicht zuletzt wegen zunehmenden Belastungen der Krankenhäuser, welche aus der hohen Anzahl von Patientinnen und Patient_innen und der zu verarbeitenden Patient_innendaten resultiert. Um dem Recht auf informationelle Selbstbestimmung angemessen Rechnung zu tragen, kann allerdings von den Verantwortlichen grundsätzlich verlangt werden, dass diese nach den vorhandenen Gegebenheiten zumutbare und umsetzbare Maßnahmen treffen. Nicht Sinn und Zweck des Datenschutzes ist es hingegen, durch zu hohe Anforderungen den Regelbetrieb einzuschränken oder eine effektive Versorgung von Patient_innen zu gefährden. Ziel sollte es demnach sein, stets einen gerechten Interessenausgleich herzustellen.

Wir sind daher auch weiterhin Ansprechpartner von Verantwortlichen und Betroffenen und unterstützen sie, um praktikable Lösungswege aufzuzeigen.

11.2.2 Verpflichtende Corona-Testungen für Kindergartenkinder

Viele Kindergärten bieten freiwillige Corona-Tests für die Kindergartenkinder an. Bei der Beschaffung der Tests werden die Träger der Kindergärten finanziell vom Land unterstützt. Dieses (freiwillige) Testangebot ist vernünftig und zu begrüßen. Wie sieht es aber mit verpflichtenden Testungen für Kindergartenkinder aus, d. h. Tests, deren Durchführung die Kindertagesstätte zur zwingenden Voraussetzung für den Zugang zum Kindergarten erhebt? Sind diese zulässig? Mit dieser Frage haben wir uns aufgrund der Beschwerde von Eltern eines Kindergartenkinds im Berichtszeitraum (vor Einführung der verbindlichen Tests für Kitas mit der Änderung der CoronaVO Kita vom 7. Januar 2022) befasst.

Der (private) Träger der betroffenen Kindertagesstätte hatte vorgetragen, er führe die (Schnell-) Tests ab einem 7-Tage-Inzidenzwert über 100 verpflichtend durch. Dies geschehe aus gesellschaftlicher Verantwortung und Verantwortung gegenüber den Kindern, die die Einrichtung besuchen, deren Eltern und den Mitarbeitenden. Ziel sei es, für die Eltern die Kinderbetreuung sicherzustellen und dafür zu sorgen, dass sich Kinder, Eltern und Mitarbeitende in der Kindertagesstätte nicht mit Covid-19 infizieren. Die Testungen der Kinder erfolgten vor Ort beim Kindergarten (oder alternativ an einer öffentlichen Teststelle); eine Durchführung der Tests zu Hause hat der Träger der Kindertagesstätte nicht akzeptiert.

Bei den Testungen werden personenbezogene Daten der Kinder verarbeitet. Hierbei handelt es sich um Gesundheitsdaten und damit um besondere Kategorien personenbezogener Daten, die von der Datenschutz-Grundverordnung (DS-GVO) besonders geschützt sind und deren Verarbeitung nur bei Vorliegen eines Ausnahmetatbestands nach Artikel 9 Absatz 2 DS-GVO rechtmäßig ist. Ein solcher Ausnahmefall wurde vom betroffenen Träger nicht vorgetragen und war auch sonst nicht ersichtlich.

Insbesondere war es nicht möglich, die Testpflicht auf eine Einwilligung der Eltern zu stützen (Artikel 9 Absatz 2 Buchstabe a DS-GVO). Dies käme nur dann in Betracht, wenn die Einwilligung auch wirklich freiwillig ist. Für die konkrete Fallkonstellation bedeutet Freiwilligkeit, dass die Kinder auch für den Fall, dass ihre Eltern die Teilnahme am Test ablehnen, die Kindertagesstätte besuchen dürfen. Dies war ab einem 7-Tage-Inzidenzwert über 100 nicht der Fall.

Auch eine andere Ausnahme (im Sinne von Artikel 9 Absatz 2 DS-GVO) war nicht ersichtlich. Insbesondere konnten wir nicht feststellen, dass die Verarbeitung der Testergebnisse auf der Grundlage des Rechts der Bundesrepublik Deutschland oder des Landes Baden-Württemberg aus Gründen eines erheblichen öffentlichen Interesses (gemäß Artikel 9 Absatz 2 Buchstabe g DS-GVO) oder aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit (Artikel 9 Absatz 2 Buchstabe i DS-GVO) erforderlich wäre:

- Das Land Baden-Württemberg hat bei Schulen nach dem Sommerferien 2021 verpflichtende Testungen der (nicht immunisierten) Schülerinnen und Schüler (als Zugangsvoraussetzung zur

>> Mehr Informationen:

Zur Krankenhaushygiene: https://www.rki.de/DE/Content/Infekt/Krankenhaushygiene/ThemenAZ/H/Hyg_blutuebertr_Erreger.html

Zum Umgang mit HIV-Infektionen in der Zahnärztlichen Praxis: https://www.bzaek.de/service/positionen-statements/einzelansicht/zahnaerztliche-behandlung-von-hiv-positiven-patienten.html

https://www.aidshilfe.de/meldung/keine-angst-hiv-zahnarztpraxis

https://www.gesundheitsdialog-bw.de/fileadmin/media/Das_Zahnaerzte-HIV-Projekt_Baden-Wuerttemberg.pdf

Zur Orientierungshilfe für Krankenhausinformationssysteme: Krankenhausinformationssysteme (OH KIS): https://www.baden-wuerttemberg.datenschutz.de/krankenhausinformationssysteme-oh-kis/

Unser 34. Tätigkeitsbericht: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/LfDI-34.-Datenschutz-T%C3%A4tigkeitsbericht-Internet.pdf <<

Schule) vorgesehen; dies ist in der Verordnung des Kultusministeriums über den Schulbetrieb unter Pandemiebedingungen vom 26. September 2021 geregelt. Anders ist es bei Kindergärten. Hier hat sich das Land dagegen entschieden, (verpflichtende) Tests der zu betreuenden Kinder als Zugangsvoraussetzung zum Kindergarten zu regeln; insbesondere enthielt die „Verordnung des Kultusministeriums über den Betrieb der Kindertageseinrichtungen und Kindertagespflegestellen unter Pandemiebedingungen" (zuletzt vom 3. Oktober 2021) bis zum 7. Januar 2022 keine Testpflicht für die zu betreuenden Kinder.

- Eine weitere Möglichkeit staatlichen Handelns ist, dass das Gesundheitsamt des jeweiligen Stadt- oder Landkreises aufgrund der örtlichen Verhältnisse ein Zutritts- und Teilnahmeverbot für Kinder ohne Testnachweis in Kindertageseinrichtungen auf der Grundlage des Infektionsschutzgesetzes (z. B. durch Allgemeinverfügung) regelt. Auch dies war am Ort der Kindertagesstätte nicht erfolgt.

- Der Träger einer Kindertagesstätte kann unserer Auffassung nach auch nicht aufgrund seines Hausrechts einen entsprechenden (negativen) Schnelltest als Zugangsvoraussetzung verlangen: Dies ergibt sich schon daraus, dass es einen Vertrag zwischen den Eltern der Kinder und dem Träger der Kindertagesstätte bezüglich der Betreuung der Kinder (und daher eine vertragliche Verpflichtung des Trägers zur Kinderbetreuung) gibt; eine solche Testpflicht war (unserer Kenntnis) nach vertraglich nicht vorgesehen. Des Weiteren steht einer solchen Ausübung des Hausrechts ggf. auch entgegen, dass es sich bei der Kinderbetreuung möglicherweise um eine lebensnotwendige Dienstleistung der Daseinsvorsorge handelt, die nur bei bestimmten Stellen zur Verfügung steht, so dass die Kinder und deren Eltern nicht ohne Weiteres auf andere Anbieter ausweichen können.

Auch wenn die Gründe des Trägers der Kindertagesstätte für die Entscheidung zu verpflichtenden Testungen ab einem bestimmten Inzidenzwert nachvollziehbar waren, erfolgten diese ohne Rechtsgrundlage für die Verarbeitung der Testergebnisse; eine „Wahlfreiheit" jedes Trägers, verpflichtende Testungen aufgrund seines Hausrechts durchzuführen, besteht nicht.

11.2.3 Datenübermittlung des Jugendamts an den Petitionsausschuss

Das Petitionsrecht ist ein hohes Gut, das im Grundgesetz verankert ist. So hat nach Artikel 17 des Grundgesetzes (GG) jedermann das Recht, sich einzeln oder in Gemeinschaft mit anderen schriftlich mit Bitten oder Beschwerden an die Volksvertretung zu wenden. Daran anknüpfend regeln Artikel 2 und 35a der Verfassung des Landes Baden-Württemberg (LV), dass sich jede und jeder an den Petitionsausschuss des Landtags (von Baden-Württemberg) wenden kann, wenn er mit dem Handeln von Behörden des Landes nicht einverstanden ist. Eine eigene Betroffenheit ist für das Einlegen einer Petition nicht erforderlich. So ist es z. B. auch möglich, sich über die Untätigkeit eines Jugendamts in einer Angelegenheit zu beschweren, die gar nicht die eigenen Kinder betrifft.

Das Petitionsverfahren läuft in aller Regel so ab, dass der Petitionsausschuss das sachlich zuständige Ministerium um Stellungnahme zur Sach- und Rechtslage bittet. Wenn die Petition den sog. „nachgeordneten Bereich" betrifft, benötigt das Ministerium zur Erstellung dieser Stellungnahme einen Bericht der nachgeordneten Behörde. Mit diesem Bericht an das Ministerium und der Stellungnahme des Ministeriums gegenüber dem Petitionsausschuss werden in aller Regel personenbezogene Daten weitergegeben. Hierbei handelt es sich auch nicht unbedingt (nur) um personenbezogene Daten der Person, die die Petition eingelegt hat, sondern häufig auch um Daten Dritter. Gerade in besonders sensiblen Bereichen, wie z. B. im Aufgabenbereich eines Jugendamts, kommt es hier zu einem Spannungsfeld zwischen dem verfassungsrechtlich gewährleisteten Petitionsrecht und dem Recht auf informationelle Selbstbestimmung der betroffenen Person, deren Daten an den Petitionsausschuss weitergegeben werden sollen – insbesondere wenn die Datenweitergabe sehr persönliche Lebensbereiche betrifft. Zu diesem Spannungsfeld hat uns das Ministerium für Soziales, Gesundheit und Integration Baden-Württemberg im Berichtszeitraum um Mitteilung unserer Rechtsauffassung in Zusammenhang mit Petitionen, die das Jugendamt betreffen, gebeten.

Die Frage, ob ein Jugendamt berechtigt ist, dem Ministerium bzw. dem Petitionsausschuss im Rahmen eines Berichts zu einer Petition Sozialdaten (dies

sind personenbezogene Daten im Bereich des Jugendamts) zu übermitteln, haben wir grundsätzlich bejaht. Rechtsgrundlage hierfür ist § 69 Absatz 5 des Zehnten Buchs des Sozialgesetzbuchs (SGB X) i. V. mit § 67c Absatz 3 Satz 1 SGB X. Nach diesen Vorschriften ist eine Übermittlung von Sozialdaten zulässig, wenn sie für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen erforderlich ist. Mit dem Petitionsrecht ist eine parlamentarische Kontrollfunktion verbunden. Daher ist es zumindest vertretbar, eine Übermittlung auf diese Vorschriften zu stützen. Allerdings gilt dies nicht für alle Sozialdaten. Im Bereich des Jugendamts gibt es Folgendes zu beachten:

1. Sozialdaten, die einer/m Mitarbeitenden eines Jugendamts zum Zwecke persönlicher und erzieherischer Hilfe anvertraut worden sind, dürfen nur in eng begrenzten, gesetzlich geregelten Ausnahmefällen weitergegeben werden (§ 65 des Achten Buchs des Sozialgesetzbuchs – SGB VIII). Eine Übermittlung dieser Sozialdaten an den Petitionsausschuss kommt – soweit keine Einwilligung der Person, die die Daten anvertraut hat, vorliegt – nicht in Betracht.

2. Eine Übermittlung von Sozialdaten an den Petitionsausschuss ist nur zulässig, soweit dadurch der Erfolg einer zu gewährenden Leistung nicht in Frage gestellt wird (vgl. § 64 Absatz 2 SGB VIII). Zweck dieser gesetzlichen Regelung ist es, die Effektivität von Leistungen des Jugendamts, z. B. der Hilfe zur Erziehung, nicht durch den Vollzug anderer Aufgaben zu gefährden (vgl. Mörsberger in Wiesner, Kommentar zum SGB VIII, 5. Auflage, § 64 Rn. 10). Wenn der Erfolg einer vom Jugendamt zu gewährenden Leistung in einer konkreten Angelegenheit durch die Übermittlung der Sozialdaten an das Ministerium bzw. den Petitionsausschuss gefährdet wird, ist eine Übermittlung unzulässig.

3. Generell ist davon auszugehen, dass die Kontrollfunktion des Parlaments eine Grenze in den nach Artikel 1 Absatz 3 GG (i. V. mit Artikel 2 LV) zu beachtenden Grundrechten Dritter findet. So hat der Verfassungsgerichtshof für das Land Nordrhein-Westfalen in einer aktuellen Entscheidung (Urteil vom 20. April 2021, Az.: VerfGH 177/20) zum Recht des parlamentarischen Untersuchungsausschusses auf Aktenvorlage entschieden, dass insoweit dem Schutz personenbezogener Daten eine besondere Bedeutung zuzumessen sei. Umfang, Reichweite und Grenzen des Aktenvorlagerechts bedürften daher einer verfahrensrechtlichen Konkretisierung, die die widerstreitenden verfassungsrechtlichen Positionen von parlamentarischem Untersuchungsrecht einerseits und Grundrechtsschutz andererseits in schonenden und zugleich wirksamen Ausgleich (sog. praktische Konkordanz) bringe.

Diese vom Verfassungsgerichtshof im Zusammenhang mit der Aktenvorlage an einen parlamentarischen Untersuchungsausschuss angesprochenen Punkte haben unserer Auffassung nach auch Bedeutung bei der Übermittlung personenbezogener Daten an einen Petitionsausschuss. Dies führt nach unserer Einschätzung insbesondere zu Folgendem:

- Es ist zu prüfen, ob von der (beabsichtigen) Datenübermittlung Informationen betroffen sind, die den Kernbereich privater Lebensgestaltung betreffen. Welche Informationen wegen ihres streng persönlichen Charakters unter diese Kategorie fallen, bedarf der einzelfallbezogenen Bewertung anhand des Kriteriums der Unzumutbarkeit einer etwaigen Kenntnisnahme durch außerhalb der zuständigen aktenführenden Stelle stehende Dritte. Enthalten Akten streng persönliche Informationen, deren Preisgabe für die Betroffenen unzumutbar sei, kommt eine Aktenvorlage grundsätzlich nur unter besonderen datenschutzrechtlichen Vorkehrungen in Betracht, die eine Identifizierbarkeit der Betroffenen wirksam ausschließen. Die bloße Ergreifung von Geheimnisschutzmaßnahmen durch den parlamentarischen Ausschuss sind insoweit nicht zum Schutz dieser Daten ausreichend; vielmehr besteht insoweit ein absolutes Verbot der Weitergabe in personenbezogener Weise.

- Weiter bedarf es einer verfahrensrechtlichen Konkretisierung, die die widerstreitenden verfassungsrechtlichen Positionen von parlamentarischen Rechten einerseits und dem Grundrechtsschutz andererseits in schonenden und zugleich wirksamen Ausgleich (sog. praktische Konkordanz) bringt. Die Verfassungsorgane trifft insoweit eine Abwägungs- und Koordinationsobliegenheit. Sie haben über die Art und Weise der Gewährleistung des Schutzes der

betroffenen höchstpersönlichen Informationen verfahrensrechtlich verbindliche Absprachen zu treffen. Dies kann z. B. den Ausschluss der Öffentlichkeit (bei der „Behandlung" der Petition durch den Petitionsausschuss) und sonstige Vorkehrungen zur Geheimhaltung betreffen. In diesem Zusammenhang ist ggf. auch zu prüfen, ob die Übermittlung anonymisierter (bzw. ausnahmsweise pseudonymisierter) schutzbedürftiger Daten für das parlamentarische Kontrollrecht ausreichend ist.

Soweit eine Übermittlung von Sozialdaten zulässig ist, darf das Jugendamt auf Verlangen des Petitionsausschusses vor dem Ausschuss auch mündlich Auskunft über den Gegenstand der Petition geben und dem Ausschuss (auf Anforderung) Akten vorlegen. Hier ist allerdings Folgendes zu beachten: Im Sozialrecht gilt – wenn die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, erfolgt – nicht der im Landesdatenschutzgesetz geltende Grundsatz, dass die ersuchende Stelle die Verantwortung für die Übermittlung trägt. Vorrangig und abschließend ist hier die Regelung des § 67d Absatz 1 SGB X.

Nach dieser Vorschrift trägt das Jugendamt als übermittelnde Stelle weitgehend (mit Ausnahme derjenigen für die Richtigkeit der im Ersuchen mitgeteilten Tatsachen) die Verantwortung für die Zulässigkeit der Übermittlung und hat in diesem Rahmen wohl auch zu prüfen, ob die Übermittlung zur Aufgabenerfüllung (Kontrolle durch den Petitionsausschuss) erforderlich ist. Damit das Jugendamt dies prüfen kann, muss der Petitionsausschuss daher ggf. begründen, weswegen er eine mündliche Auskunft bzw. die Vorlage der Akten (ggf. vollständig) benötigt.

Wir hoffen, dass unsere Ausführungen eine Hilfestellung für die Praxis sind und dazu beitragen, dass der Petitionsausschuss seine Aufgaben vernünftig wahrnehmen kann und zugleich die von der Weitergabe sensibler Sozialdaten betroffenen Personen so gut wie möglich geschützt werden.

11.2.4 Forschungsprojekt STARKIDS im Universitätsklinikum

Im Berichtszeitraum haben wir bei verschiedenen Forschungsprojekten, insbesondere solchen mit der Verarbeitung von Gesundheitsdaten, datenschutzrechtlich beraten. So hat sich u. a. das Universitätsklinikum Tübingen vor der Umsetzung des Forschungsprojektes STARKIDS mit der Bitte um datenschutzrechtliche Prüfung und Beratung an uns gewandt. Gegenstand des Forschungsprojektes STARKIDS ist die wissenschaftliche Untersuchung von Kindern und Jugendlichen mit Übergewicht oder Adipositas (Fettleibigkeit) und der damit verbundenen Begleiterscheinungen. Diese wissenschaftlichen Untersuchungen setzen die Verarbeitung personenbezogener (Gesundheits-)Daten bei den betroffenen Kindern und Jugendlichen voraus.

Für die datenschutzrechtliche Prüfung und Beratung hat uns das Universitätsklinikum Tübingen die relevanten Unterlagen zugesandt. Dazu gehörten insbesondere die Beschreibung des Forschungsprojektes und der Verarbeitungsvorgänge, die Vereinbarungen über eine gemeinsame Verantwortlichkeit zwischen den Projektpartnern, Verträge über Auftragsverarbeitungen, eine Datenschutz-Folgenabschätzung, das Verarbeitungsverzeichnis und die Informationen über die Verarbeitung personenbezogener Daten für die betroffenen Studienteilnehmer_innen.

Unsere datenschutzrechtliche Bewertung bezog sich auf zwei Ebenen: Die erste Ebene betrifft die Vorbereitung des Forschungsprojektes mit der Bestandsaufnahme der datenschutzrechtlichen Anforderungen und deren Umsetzung. Auf dieser Ebene hat uns das Universitätsklinikum Tübingen als Konsortialführer (folgend: UKT) für das Forschungsprojekt STARKIDS die Dokumentation zur Vorbereitung des Projektes zukommen lassen. Diese haben wir datenschutzrechtlich bewertet und hierzu im Berichtszeitraum per Videokonferenz und mit mehreren ausführlichen Schreiben Stellung genommen sowie Ergänzungen bzw. Änderungen angeraten. Die zweite Ebene betrifft die datenschutzkonforme Umsetzung des Forschungsprojektes STARKDIS, wenn die wissenschaftlichen Untersuchungen an den Studienteilnehmenden begonnen haben. Auf dieser Ebene bedarf es der regelmäßigen Prüfung des Forschungsprojektes während der Laufzeit. Dazu gehört es, dass die verantwortliche Projektleitung bei Bedarf die einmal getroffenen datenschutzrechtlichen Maßnahmen zu einem späteren Zeitpunkt des Forschungsprojektes überprüft und anpasst.

In unseren Beratungen haben wir uns mit unseren Schreiben insbesondere mit folgenden Fragestellungen zum Forschungsprojekt STARKIDS an das Universitätsklinikum Tübingen gewandt:

- Welche der teilnehmenden Projektpartner_innen entscheidet allein oder gemeinsam über die Zwecke und Mittel der Verarbeitung personenbezogener Daten und ist damit Verantwortlicher im Sinne des Artikels 4 Nummer 7 der DS-GVO? Und wer ist Auftragsverarbeiter im Sinne des Artikels 28 DS-GVO?

- Wie informieren die Forschungspartner_innen die (auch minderjährigen) Studienteilnehmenden über die Verarbeitung personenbezogener Gesundheitsdaten nach Artikel 12-14 DS-GVO?

- Auf welchen Rechtsgrundlagen beruhen die jeweiligen Verarbeitungen personenbezogener Daten?

Auf der ersten Ebene der Vorbereitung des Forschungsprojektes hat uns das UKT mitgeteilt, dass es sich bei den Partner_innen des Forschungsprojektes um gemeinsam Verantwortliche im Sinne des Artikels 26 DS-GVO handele. Das UKT hat infolge unserer Hinweise eine neue Vereinbarung über die gemeinsame Verantwortlichkeit zwischen den Konsortialpartnern vorgesehen. Die Verwendung des – auf unserer Homepage abrufbaren – Musters unserer Behörde über die Vereinbarung gemäß Artikel 26 Absatz 1 Satz 1 Datenschutz-Grundverordnung (DS-GVO) erleichterte es dabei, die relevanten und klärungsbedürften Regelungsbereiche festzustellen.

Weiter haben wir außerdem aufgezeigt, dass das UKT für eine datenschutzkonforme Umsetzung des Forschungsprojektes STARKIDS die Informationen über die Verarbeitung personenbezogener Daten weiter differenzieren sollte. Dabei hat das UKT erkennbare Anstrengungen vorgenommen, die Informationen über die Verarbeitung personenbezogener Daten auf die Kinder, Jugendlichen und Erwachsenen Studienteilnehmenden anzupassen und diese in einer verständlichen, klaren und einfachen Sprache einzusetzen. Dies ist die notwendige Voraussetzung für eine informierte freiwillige Einwilligung der Studienteilnehmenden, was wir dem UKT aufgezeigt haben. Denn die Einwilligung hat freiwillig zu erfolgen und aufgrund des Koppelungsverbotes nach Artikel 7 Absatz 4 DS-GVO darf das UKT diese nicht zur Voraussetzung für die Behandlung machen. Daher haben wir in unseren Beratungen verstärkt darauf hingewirkt, dass das UKT auch die Informationen über die Verarbeitungen personenbezogener Daten in den teilnehmenden Arztpraxen und über die Projektwebseite entsprechend anpasst.

In Anbetracht der im Rahmen des Forschungsprojektes verarbeiteten besonders sensiblen Gesundheitsdaten nach Artikel 4 Nummer 15 DS-GVO haben wir auf eine Differenzierung hinsichtlich der relevanten Rechtsgrundlagen hingewiesen. Dabei sind über die pauschale Anwendung der Einwilligung nach Artikel 9 Absatz 2 Buchstabe a DS-GVO in die Verarbeitung der besonders sensiblen Gesundheitsdaten im Forschungsprojekt STARKIDS hinaus weitere Rechtsgrundlagen anwendbar, so etwa für die Datenverarbeitung zur therapeutischen Behandlung die Rechtsgrundlage aus dem Behandlungsvertrag nach Artikel 6 Absatz 1 Buchstabe b (und Artikel 9 Absatz 2 Buchstabe h DS-GVO) in Verbindung mit § 630a des Bürgerlichen Gesetzbuches und für die Leistungsabrechnung Artikel 6 Absatz 1 Buchstabe b, Artikel 9 Absatz 2 Buchstabe h DS-GVO in Verbindung mit § 284 Absatz 1 Nummer 8 Sozialgesetzbuch Fünftes Buch.

Dies hat das UKT nach unseren Hinweisen anerkannt und einbezogen. Schließlich haben wir darauf hingewirkt, dass das UKT über das Widerrufsrecht dahingehend aufklärt, gegenüber wem dieses auszuüben ist und welche Rechtswirkungen damit einhergehen. Wir haben insbesondere darauf hingewiesen, dass die Weiterleitung z. B. der Widerrufserklärung und Umsetzung der Betroffenenrechte über die behandelnden Ärzt_innen sicherzustellen sind. Weiter haben wir in der ersten Ebene deutlich gemacht, dass bereits die Information über die Teilnahme an dem Forschungsprojekt ein besonders sensibles Gesundheitsdatum darstellt, zumal die Teilnahme zumindest die Diagnose des Übergewichts oder der Adipositas voraussetzt. Eine Verarbeitung personenbezogener Gesundheitsdaten verlangt aber gesteigerte Schutzanforderungen an die technischen und organisatorischen Maßnahmen nach Artikel 32 DS-GVO und § 22 Absatz 2 BDSG. Das Versenden einer E-Mail, die die Information über die Teilnahme an der Stu-

die enthält, ist daher nicht ohne weiteres zulässig; vielmehr hat ein solcher Versand Ende-zu-Ende verschlüsselt erfolgen. Dabei darf dieses aufgrund der gesetzlichen Verpflichtung der gemeinsam Verantwortlichen aus Artikel 32 DS-GVO und § 22 Absatz 2 BDSG durch technische und organisatorische Maßnahmen einzuhaltende Datenschutzniveau auch nicht mittels einer Einwilligung der Betroffenen abbedungen werden. Der ursprünglichen Rechtsauffassung des UKT, dass Benachrichtigungen per E-Mail an die Studienteilnehmenden keinerlei personenbezogene Inhalte enthalten würden, sind wir daher entschieden entgegengetreten. Das UKT hat sich insoweit überzeugen lassen und sieht nunmehr Kontaktaufnahmen und Benachrichtigungen ausschließlich per SMS vor, was wir begrüßen.

In Anbetracht der datenschutzrechtlichen Wertung aus der DS-GVO, dass die Verarbeitung besonderer Kategorien personenbezogener Daten ein hohes Risiko indiziert, haben wir in der Datenschutz-Folgenabschätzung auf den deutlichen Differenzierungsbedarf hingewiesen. Denn erst mit der Feststellung des jeweiligen Risikos der Verarbeitung personenbezogener Daten, lassen sich die technischen und organisatorischen Maßnahmen kalibrieren. Dies setzt voraus, dass das UKT die potentiellen Schäden für die Rechte und Freiheiten natürlicher Personen feststellt. Im Forschungsprojekt STAR-KIDS kann dies z. B. die Stigmatisierung einer Person mit Fettleibigkeit sein, wenn die Teilnahme an diesem Forschungsprojekt bekannt wird. Abhängig vom Einzelfall kann dies im schlimmsten Fall z. B. zu einem (immateriellen) Schaden infolge von „Mobbing“ führen. Folglich sind die gesteigerten Schutzanforderungen bei der Verarbeitung von Gesundheitsdaten in den technischen und organisatorischen Maßnahmen anzupassen.

Die Umsetzung des Forschungsprojektes in der zweiten Ebene verlangt, dass das UKT die Maßnahmen nach der DS-GVO regelmäßig überprüft. Wir haben insbesondere darauf hingewiesen, dass aufgrund der Dynamik innerhalb des Forschungsprojektes mindestens halbjährliche Bewertungen anzusetzen sind und iterative Prüfungen der technischen und organisatorischen Maßnahmen und ggf. Kalibrierungen erforderlich sind. In diesem Zusammenhang haben wir auch nach einem differenzierten Löschkonzept gefragt, nachdem uns das UKT bislang nur sehr allgemein die Löschroutinen und Aufbewahrungsfristen dargelegt hat. Die Beratungen hinsichtlich der Maßnahmen auf dieser zweiten Ebene dauern noch an.

Der LfDI unterstützt die Gesundheitsforschung in Baden-Württemberg.

Es hat sich insgesamt gezeigt, dass bereits vor Beginn eines Forschungsprojektes die Bestandsaufnahme der bevorstehenden Verarbeitungen personenbezogener Daten mit den jeweiligen Rechtsgrundlagen zu komplexen datenschutzrechtlichen Fragen führen kann. Daher empfiehlt sich eine frühzeitige datenschutzrechtliche Bestandsaufnahme und Bewertung. Diese bedarf im Einzelfall aufgrund möglicherweise komplexer datenschutzrechtlicher Fragestellungen und damit verbundenen Aufklärungsbedarf angemessene zeitliche und personelle Ressourcen. Denn nur eine gründliche Vorbereitung vor Projektbeginn und eine regelmäßige wiederholende Prüfung im laufenden Projekt stellen die datenschutzrechtliche Zulässigkeit der Verarbeitungen im Rahmen des Forschungsprojekts sicher. Forschenden des Landes Baden-Württemberg stehen wir insoweit im Rahmen unserer Kapazitäten gerne beratend zur Seite.

11.2.6 Lost Places

Wer ist für vergessene Patient_innendaten bei „lost places" verantwortlich?

Patient_innendaten sind als Gesundheitsdaten im Sinne von Artikel 4 Nummer 15 der DS-GVO (DS-GVO) eine besondere Kategorie von personenbezogenen Daten nach Artikel 9 DS-GVO, welche aufgrund ihrer Sensibilität eines besonderen Schutzes bedürfen. Umso wichtiger ist es, dass der Verantwortliche seine Kernpflicht erfüllt und durch geeignete technische und organisatorische Maßnahmen die Rechtmäßigkeit der Verarbeitung sicherstellt (Artikel 24 Absatz 1 Satz 1 DS-GVO). Dazu gehört u. a. eine datenschutzkonforme Speicherung der personenbezogenen Daten und ihre anschließende datenschutzkonforme Löschung. Wer als Verantwortlicher im Sinne der DS-GVO für die Rechtmäßigkeit der Verarbeitung Sorge zu tragen hat, kann unter Umständen – insbesondere wenn die der Datenverarbeitung zugrundeliegenden Aktivitäten schon länger zurückliegen – schwierig zu beantworten sein.

So wurden wir durch eine Presseanfrage auf einen gravierenden Datenschutzvorfall aufmerksam gemacht, bei welchem eine Person in einem seit langer Zeit verlassenen Gebäude diverse Akten mit Patient_innendaten eines Krankenhauses aufgefunden habe. Diese lagen dort in einem Treppenhaus verstreut herum, sodass Dritte diese problemlos einsehen konnten. Erlangt eine Aufsichtsbehörde für den Datenschutz auf solch einem Wege Kenntnis von einem Datenschutzvorfall, kann sie nach pflichtgemäßem Ermessen von Amts wegen tätig werden, da nach Artikel 57 Absatz 1 Buchstabe a und h DS-GVO die Überwachung und Durchsetzung der DS-GVO zu ihren Aufgaben zählt. Der Umgang mit sensiblen Akten in aufgegebenen Räumen beschäftigt daher immer wieder die Aufsichtsbehörden (so z. B. auch die Hamburger Kollegen im Fall des Hamburgischen Oberverwaltungsgerichts, Beschluss vom 15.10.2020 – 5 Bs 152/20). Charakteristisch und zugleich problematisch ist, dass von solchen verlassenen und geheimnisvoll erscheinenden Bauwerken aus der jüngeren Geschichte (sog. lost places) regelmäßig abenteuerlustige Personen angezogen werden, die diese Orte erkunden wollen. Oftmals erstellen sie auch Fotografien oder Filme und veröffentlichen diese. Insbesondere dann, wenn der Ort mediale Aufmerksamkeit erfährt, kann bei der Sicherung der Daten der Faktor Zeit eine entscheidende Rolle spielen.

Dann wird als erster Schritt zu prüfen sein, ob sich rasch aufklären lässt, wer Verantwortlicher im Sinne der DS-GVO und damit Ansprechpartner_in der Aufsichtsbehörde ist, die/der für die Beseitigung des rechtswidrigen Zustandes in die Pflicht genommen werden kann. In unserem Fall konnten wir im Rahmen erster Recherchen herausfinden, dass das Gebäude in der Vergangenheit mehrfach Gegenstand von Zwangsversteigerungen war und in den letzten Jahrzehnten verschiedene Mieter_innen hatte; über das Vermögen einer der Gesellschaften war zudem ein Insolvenzverfahren geführt worden. All dies erschwerte die Ermittlung des datenschutzrechtlichen Verantwortlichen. Es zeichnete sich also ab, dass dessen Bestimmung nicht umgehend möglich sein würde. Daher galt es, zunächst ohne diese Klärung die Akten mit den sensiblen Daten schnellstmöglich und damit noch vor dem bevorstehenden Wochenende zu sichern, mithin potentielle Zugriffe durch Dritte zu unterbinden. Dies gelang uns vor allem durch die effektive Zusammenarbeit unserer Behörde mit den Behörden und Beteiligten vor Ort, insbesondere mit dem örtlich zuständigen Polizeivollzugsdienst.

Mit der vorläufigen Sicherung der Akten ist der Fall aber noch nicht abgeschlossen. Vielmehr muss

immer noch u. a. über den weiteren Verbleib oder die Löschung der Daten entschieden werden. Einer umgehenden Vernichtung der Akten können dabei insbesondere gesetzliche Aufbewahrungsfristen entgegenstehen, die möglicherweise gebieten, die Akten weiter aufzubewahren. So sind etwa Patient_innendaten nach § 630 f Absatz 3 des Bürgerlichen Gesetzbuchs (BGB) und § 10 Absatz 3 der Berufsordnung der Landesärztekammer Baden-Württemberg vom 21. September 2016 (ÄBW 2016, S. 506), zuletzt geändert durch Satzung vom 22. April 2020 (ÄBW 2020, S. 259) für mindestens zehn Jahre aufzubewahren. Auch diese Prüfung hat in erster Linie der datenschutzrechtlich Verantwortliche vorzunehmen, so dass es weiter gilt, diesen aufzufinden.

Die DS-GVO definiert den Verantwortlichen in Artikel 4 Nummer 7 DS-GVO als die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Nach den Leitlinien des Europäischen Datenschutzbeauftragten zu den Begriffen „Verantwortlicher", „Auftragsverarbeiter" und „gemeinsam Verantwortliche" der Verordnung (EU) 2018/1725 bestimmt sich die Verantwortlichkeit insbesondere nach dem faktischen Einfluss, den der Verantwortliche auf den Verarbeitungsvorgang nimmt. Der Europäische Gerichtshof geht insoweit grundsätzlich davon aus, dass der Begriff des „Verantwortlichen" weit auszulegen sei, um einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten (vgl. EuGH Urt. v. 10.07.2018, Az. C-25/17, Rn. 66).

In einem Krankenhaus ist grundsätzlich der Träger als juristische Person der datenschutzrechtlich Verantwortliche, da dieser die Einrichtung betreibt und damit über die Zwecke und Mittel der Datenverarbeitung entscheidet. Er bestimmt insbesondere, welche Patient_innendaten zu welchem Zweck erhoben werden und wie diese aufbewahrt werden. Probleme ergeben sich dann, wenn der Betrieb bereits seit mehreren Jahren oder Jahrzehnten eingestellt wurde und sich die juristische Person entweder in der Insolvenz befindet oder bereits rechtlich nicht mehr existent ist.

Wurde über die juristische Person ein Insolvenzverfahren eröffnet, ist zu fragen, ob sich durch diese Eröffnung die Verantwortlichkeit geändert hat. In der Rechtsprechung ist diese Frage umstritten. Weder die DS-GVO noch das deutsche Recht enthält eine spezielle Regelung der datenschutzrechtlichen Verantwortlichkeit in der Insolvenz. Das bedeutet, dass sich auch insoweit die Verantwortlichkeit nach Artikel 4 Nummer 7 DS-GVO bestimmt, also danach, wer die Entscheidungsgewalt über die Zwecke und Mittel der Verarbeitung hat. Mit der Eröff-

Lost-Places: Manchmal bewohnnen diese aufregenden Pläze nicht mehr nur Pflazen, sondern es liegen dort auch sensible Akten herum, die dort nicht hingehören.

nung des Insolvenzverfahrens geht aber das Recht des Schuldners, das zur Insolvenzmasse gehörende Vermögen zu verwalten und über es zu verfügen, nach § 80 der Insolvenzverordnung (InsO) auf die/den Insolvenzverwalter_in über. Nach der Eröffnung des Insolvenzverfahrens hat die/der Insolvenzverwalter_in gemäß § 148 InsO das gesamte zur Insolvenzmasse gehörende Vermögen sofort in Besitz und Verwaltung zu nehmen. Solange und soweit die Akten zur Insolvenzmasse gehören, wird daher in der Regel die/der Insolvenzverwalter_in, der über die Zwecke und Mittel der Verarbeitung bestimmen kann, als datenschutzrechtlich Verantwortlicher anzusehen sein (anderer Auffassung allerdings das Amtsgericht Hamburg in seinem Urteil vom 15.11.2021 – 11 C 75/21). Auch schon bei einem vorläufigen Insolvenzverwalter (vgl. § 22 InsO) kann unter bestimmten Bedingungen ein solcher Übergang in Betracht kommen.

Erst recht kann die Ermittlung des Verantwortlichen Schwierigkeiten bereiten, wenn das Insolvenzverfahren mangels Masse nicht eröffnet oder eingestellt wurde oder wenn die das Krankenhaus tragende juristische Person sonst aufgelöst oder beendet wurde. Hier kommt insbesondere in Betracht, die letzten Gesellschafter oder ggf. den nach § 74 Absatz 2 des Gesetzes betreffend die Gesellschaften mit beschränkter Haftung bzw. § 273 Absatz 2 des Aktiengesetzes (vgl. für Personengesellschaften auch § 157 Absatz 2 des Handelsgesetzbuchs) zu bestimmenden Verwahrer der Bücher und Schriften der Gesellschaft als datenschutzrechtlich Verantwortlichen anzusehen.

Möglich ist nach Aufgabe des Krankenhausbetriebes ferner eine Verantwortlichkeit der Eingentümerin/des Eigentümers der des Grundstücks, auf dem sich die Akten befinden. Nach der eingangs zitierten Entscheidung des Hamburgischen Oberverwaltungsgerichts wird dieser allerdings nicht automatisch durch seinen Eigentumserwerb Verantwortlicher im Sinne der DS-GVO hinsichtlich der auf dem Grundstück lagernden Akten, sondern erst dann, wenn er über die Zwecke und Mittel der Datenverarbeitung bestimmt und damit einen faktischen Einfluss hierauf ausübt. All dies verdeutlicht, wie schwierig sich insbesondere nach Einstellung des Betriebs die Suche nach einem Verantwortlichen im Einzelfall gestalten kann. Was die datenschutzrechtliche Verantwortlichkeit während und nach Abschluss eines Insolvenzverfahrens betrifft, wären zur Vermeidung solcher Schwierigkeiten gesetzliche Klarstellungen geboten und sinnvoll. Dasselbe gilt für gesetzliche Regelungen, die für eine bessere Transparenz hinsichtlich des datenschutzrechtlich Verantwortlichen nach Beendigung einer juristischen Person (z. B. auch durch Sicherstellung einer Eintragung des datenschutzrechtlich Verantwortlichen und von dessen Anschrift im Handelsregister) sorgen, zumal immer noch mit einer relevanten Zahl von Krankenhausinsolvenzen zu rechnen ist (vgl. hierzu schon Vallender, „Wohin mit den Patientenakten?“, NZI 2013, 1001-1007).

Ist – wie es in unserem Fall gelang – der Verantwortliche gefunden, wird er die Akten in Obhut nehmen müssen und dabei für angemessene technische und organisatorische Maßnahmen zum Schutz der Daten zu sorgen haben. Ferner hat er – wie ausgeführt – zu prüfen, welche Akten noch weiter aufzubewahren sind und welche datenschutzkonform vernichtet werden müssen. Wenn nicht auszuschließen ist, dass Dritte die Möglichkeit hatten, Einblick in die (im „lost Place“ lagernden) personenbezogenen Daten zu nehmen, wird regelmäßig auch eine „Verletzung des Schutzes personenbezogener Daten“ im Sinne von Artikel 4 Nummer 12 DS-GVO vorliegen. Diese ist nach Maßgabe von Artikel 33 DS-GVO meldepflichtig. Von maßgeblichem Interesse für die Aufsichtsbehörde sind dabei die nach Artikel 33 Absatz 3 DS-GVO mitzuteilenden Informationen.

Der Verantwortliche wird ferner zu prüfen haben, ob die Betroffenen nach Artikel 34 DS-GVO zu benachrichtigen sind oder eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen hat, durch die die betroffenen Personen vergleichbar wirksam informiert werden (vgl. hierzu und zu den dabei mitzuteilenden Informationen schon unseren TB 2020, S. 101 f.). Ferner wird der Verantwortlich etwaige Ansprüche Betroffener z. B. auf Auskunft zu erfüllen haben, wenn diese sich aufgrund der Benachrichtigung oder aufgrund von Presseberichten an den Verantwortlichen wenden.

Namentlich bei Beendigung eines Krankenhausbetriebs ist darauf zu achten, dass die Patient_innenakten, soweit sie noch aufbewahrungspflichtig sind, weiter unter Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz verwahrt werden. Bei Beendi-

gung der das Krankenhaus betreibenden juristischen Person sollte zudem transparent gemacht werden, wer insoweit datenschutzrechtlich verantwortlich ist. Hier besteht offensichtlich gesetzgeberischer Handlungsbedarf.

11.3 Neues aus dem Amt 3: Privatwirtschaft

11.3.1 Da hab' ich keinen Vertrag mit! – Datenverarbeitung durch Energieverteilnetzbetreibende

Auch Unternehmen, die selbst keinen Strom liefern, aber das Verteilnetz betreiben, dürfen personenbezogene Daten von Stromverbraucher_innen verarbeiten. Immer wieder erreichen meine Behörde ungehaltene Anfragen von Stromverbraucher_innen, die sich darüber verwundern, dass nicht nur das von ihnen ausgewählte Stromlieferungsunternehmen, sondern auch das Unternehmen, welches das Stromverteilnetz betreibt, Daten von Stromkund_innen erheben. Höchst misslich sei es, so wird versichert, dass aller Vertragsfreiheit zum Trotz ein nicht beauftragtes Unternehmen sich anmaße, den Namen und die Anschrift der betroffenen Kundschaft samt den Zählerstandsdaten des Stromzählers zu erheben und zu speichern.

Den Stromverbrauchenden kann nicht anders als mit Nachdruck zugestimmt werden, dass ihr Recht darauf, selbst zu entscheiden, welches Unternehmen sie mit Strom beliefert, keinen Zweifeln unterliegen darf. Dennoch bleibt zu bedenken, dass neben dem Vertrag mit dem Stromlieferungsunternehmen stets auch ein Anschlussnutzungsverhältnis zwischen die/der Stromkund_in und dem Verteilnetzbetriebsunternehmen besteht, das die Verarbeitung personenbezogener Daten durch letzteres erforderlich macht.

Die Verarbeitung personenbezogener Daten ist nach Artikel 6 Absatz 1 Unterabsatz 1 lit. b DS-GVO zulässig, wenn sie für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, erforderlich ist. Zwar schließt die/der Stromkund_in in der Regel keinen schriftlichen Vertrag mit dem Verteilnetzbetriebsunternehmen. Mit der erstmaligen Entnahme von Elektrizität aus dem Verteilnetz über den Netzanschluss der von dem/der Stromkund_in genutzten Wohnung kommt nach § 3 Absatz 2 Satz 1 der Niederspannungsanschlussverordnung (NAV) zwischen dem Verteilnetzbetriebsunternehmen der die Wohnung nutzenden Person das Anschlussnutzungsverhältnis zustande. Nach § 3 Absatz 3 Satz 1 NAV ist die anschlussnutzende Person verpflichtet, dem Netzbetriebsunternehmen die Entnahme der Elektrizität unverzüglich mitzuteilen. Diese Mitteilung hat neben dem Namen zur näheren örtlichen Bestimmung der anschlussnutzenden Person auch deren Anschrift zu enthalten. Angesichts dieser Mitteilungspflicht begegnet auch die Erhebung und Speicherung dieser Angaben durch das Netzbetriebsunternehmen während der Dauer des Anschlussnutzungsverhältnisses keinen datenschutzrechtlichen Bedenken. Hierfür spricht auch, dass das Netzbetriebsunternehmen der anschlussnutzenden Person die Mitteilung der Elektrizitätsentnahme gemäß § 3 Absatz 3 Satz 2 NAV unverzüglich in Textform zu bestätigen hat. Die Bestätigung muss nach § 4 Absatz 1 Satz 1 Nr. 1 NAV den Familiennamen, den Vornamen, den Geburtstag, die Adresse und die Kund_innennummer der anschlussnutzenden Person enthalten.

Neben diesen Stammdaten ergibt sich die Befugnis des Netzbetriebsunternehmens zur Speicherung der Zählerstandsdaten aus Folgendem: Die stromliefernden Unternehmen schulden für die Durchleitung des gelieferten Stroms durch das Verteilnetz dem Netzbetriebsunternehmen ein Netzentgelt. Die Datenverarbeitung durch zum Zweck der Abrechnung des Netzentgelts ist im Messstellenbetriebsgesetz (MsbG) geregelt.

Das Netzbetriebsunternehmen ist gemäß § 2 Satz 1 Nr. 4 MsbG grundzuständiger Messstellenbetreiber und somit für den Zählerbetrieb zuständig, soweit es nicht die Grundzuständigkeit auf ein anderes Unternehmen übertragen hat. Nach § 50 Absatz 2 Nr. 5 in Verbindung mit § 49 Absatz 2 Nr. 2 MsbG darf das Netzbetriebsunternehmen personenbezogene Daten aus einer Messeinrichtung erheben und verwenden, soweit dies für die Abrechnung des Netzentgelts gegenüber dem Stromlieferungsunternehmen erforderlich ist. Da die Höhe des vom Stromlieferanten zu zahlenden Netzentgelts von der durch das Verteilnetz geleiteten Strommenge abhängt, darf auch der Stromzählerstand für die Abrechnung des Netzentgelts erhoben und genutzt werden. Zudem benötigt das Netzbetriebsunternehmen hierfür die Firma des Stromlieferungsunternehmens.

Das Netzbetriebsunternehmen hat die Messwerte jedoch nach § 66 Absatz 3 MsbG zu löschen, wenn sie nicht mehr für seine Aufgabenwahrnehmung als Netzbetreiber erforderlich sind. Zudem hat es die Vertraulichkeit der Daten durch ausreichende technische und organisatorische Maßnahmen zu gewährleisten. Solange Stromversorgung leitungsgebunden ist, darf auch das zuständige Netzbetriebsunternehmen im hierfür erforderlichen Umfang personenbezogene Daten der Stromverbraucher_innen verarbeiten.

11.3.2 Datenschutz in der Kreditwirtschaft: Keine Geschäftsbeziehung ohne Werbeeinwilligung?

Es ist zu begrüßen, wenn Kreditinstitute Datenverarbeitungen zu Werbezwecken nur mit Einwilligung der Kund_innen durchführen und hierfür entsprechende Einwilligungsformulare formulieren. Wenn die Unterzeichnung des Formulars aber zur Bedingung für jegliche Kommunikation mit der/dem Kund_in gemacht wird, so ist dies aus datenschutzrechtlicher Sicht kontraproduktiv.

Eine Kundin eines Kreditinstituts im Land wollte sich einen aktuellen Überblick über ihre dort geführten Vermögenswerte verschaffen. Sie bat die Bank daher telefonisch um Übersendung einer Darstellung ihres sogenannten Kundenfinanzstatus an ihre Wohnanschrift. Die zuständige Bankbedienstete antwortete, dies sei nur möglich, wenn die Kundin sich mit der Verarbeitung ihrer personenbezogenen Daten zum Zweck ihrer Beratung, Betreuung und Information einverstanden erkläre. Die Bank werde ihr das hierfür notwendige Einwilligungsformular postalisch übersenden. Sie solle die gelb markierten Ankreuzfelder ankreuzen und das Formular unterschrieben zurücksenden. Dann stünde der Mitteilung ihrer Kontostände durch die Bank nichts mehr entgegen.

Die Kundin erhielt das Einwilligungsformular und war bass erstaunt über dessen Umfang und Inhalt. Detailliert und gut verständlich wurde ihr darin vorgeschlagen, in die Verknüpfung, Auswertung und Verwendung einer Vielzahl von Datenkategorien einzuwilligen. Dabei handelte es sich neben ihrem Namen, Geburtsdatum und Familienstand unter anderem auch um Angaben zu ihrer Bonität und Risikobereitschaft. Des Weiteren sollten die Auftraggebenden an sie ergangener Überweisungen, die Überweisungsempfangenden und die dazugehörigen Verwendungszwecke verarbeitet werden. Zudem sollte die Kundin in den Datenaustausch zwischen dem Kreditinstitut und dessen Verbundpartnern einwilligen. Auch die Freiwilligkeit und Widerrufbarkeit der Einwilligung blieben nicht unerwähnt. Als Zweck der Datenverarbeitungen wurde in erster Linie die Information über für die Kundin geeignete Produkte und Aktionen genannt. Die Datenverarbeitung sollte also Werbezwecken dienen.

Das Formular sah in lobenswerter Differenziertheit mehrere Ankreuzfelder für verschiedene Arten der Datenverarbeitung vor. Im Fall der Kundin waren allerdings sämtliche Ankreuzfelder gelb markiert worden, um wie telefonisch vereinbart klarzustellen, dass die entsprechenden Kreuze für die Mitteilung des Kundenfinanzstatus nun einmal unentbehrlich seien.

Diese der Kundin mitgeteilte Auffassung war irreführend, denn für die Mitteilung einer aktuellen Vermögensübersicht bedurfte es der genannten Einwilligungen nicht. Auf Anfrage der Kundin ist eine solche Mitteilung bereits nach Artikel 6 Absatz 1 Unterabsatz 1 lit. b DS-GVO für die Erfüllung des zwischen der Bank und der Kundin geschlossenen Vertrags erforderlich und daher ohne Einwilligung zulässig. Auch im Fall eines rechtskonform formulierten Einwilligungsformulars, wäre die Einwilligung der Kundin aufgrund der Begleitumstände unwirksam gewesen und darauf gestützte Datenverarbeitungen somit rechtswidrig gewesen. Nachdem sich die Kundin bei uns über die Rechtslage informiert hatte, genügte ein Hinweis auf unsere Beratung, um die Bank zu veranlassen, ihr die gewünschte Vermögensaufstellung auch ohne Abgabe der Werbeeinwilligung zu überlassen.

Damit eine Einwilligung freiwillig und wirksam ist, genügt es nicht, dass die Freiwilligkeit sich eindeutig aus dem Text des verwendeten Einwilligungsformulars ergibt. Es darf gegenüber Kund_innen auch im Beratungsgespräch nicht der Eindruck erweckt werden, dass die Geschäftsbeziehung ohne die Einwilligung nicht fortgesetzt werden kann.

11.3.3 Umgang mit der Kenntnis von Corona-Positiv-Fällen

Wer kennt es nicht: Das Verhältnis zwischen Mieter_innen und Vermieter_innen gestaltet sich oft komplizierter als gewünscht. Neben den üblichen persönlichen Diskrepanzen, stellte Corona Mietverhältnisse jedoch nochmal vor gänzlich neue datenschutzrechtliche Herausforderungen. So wandte sich ein Mitglied einer Wohngemeinschaft (WG) an uns, um uns folgenden Sachverhalt mitzuteilen: In der WG war ein Mitglied Corona-positiv getestet worden und erhielt daher am darauffolgenden Tag eine Quarantäne-Anordnung. Just an demselben Tag plante die Vermieterin der Wohngemeinschaft, dieser einen Besuch abzustatten, um nach dem Rechten zu sehen. Um mögliche Infektionsgefahren auszuschließen, informierte die WG die Vermieterin rechtzeitig vor dem Besuch über den unerfreulichen Sachverhalt.

Der geplante Besuchstermin wurde daraufhin beidseitig abgesagt. Was nun jedoch passierte, war sehr außergewöhnlich: Die Vermieterin sah sich durch die Mitteilung des positiven Corona-Ergebnisses veranlasst, sämtliche Bewohner_innen des Mehrparteienhauses über die Corona-Infektion des betroffenen WG-Mitglieds zu informieren.

Wir können hier einen Irrtum aufklären. Das Bedürfnis, sich und andere zu schützen, ist in Pandemiezeiten vernünftig und richtig. Aber auch in diesen besonderen Zeiten gilt es, die Vorgaben des Datenschutzrechts zu beachten. Dabei ist insbesondere zu berücksichtigen, dass es sich bei der Angabe, dass jemand mit dem Coronavirus infiziert ist, um ein besonders schützenswertes Gesundheitsdatum im Sinne von Artikel 9 Absatz 1 DS-GVO handelt.

Die Verarbeitung solcher sensiblen Daten ist nur dann zulässig, wenn einer der Artikel 9 Absatz 2 DS-GVO genannten Fälle vorliegt. Eine Rechtsgrundlage zur Offenlegung der Covid-Infektion durch die Vermieterin war hier jedoch nicht gegeben. Insbesondere war die Bekanntgabe der Infektion unter namentlicher Nennung der infizierten Person nicht gemäß Artikel 9 Absatz 2 lit. i DS-GVO aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich. Vielmehr ist davon auszugehen, dass den anderen Hausbewohner_innen bekannt war, dass sie ohnehin rechtlich verpflichtet waren, das Infektionsrisiko durch die Einhaltung der Abstands- und Hygieneregeln sowie das Tragen von Masken außerhalb der eigenen Wohnung zu minimieren.

Der Französische Schriftsteller Georges Perec hat mit „Das Leben. Gebrauchsanweisung" ein wundervollles Buch über das Leben und Zusammenleben in einem Wohnhaus geschrieben. Heute machen Geschichten über Corona-Erkrankungen in der Nachbarschaft schnell die Runde. Vermieter_innen dürfen aber nicht einfach herumerzählen, wenn Mieter_innen corona-positiv sind.

Von der Offenlegung einer Covid-Infektion kann für die betroffene Person – hier den WG-Bewohner – eine hohe Stigmatisierungswirkung ausgehen. Die Weitergabe dieses Datums ohne die Einverständniserklärung/Einwilligung des Bewohners stellt einen erheblichen Eingriff in dessen Persönlichkeitsrechte dar und ist mangels Rechtsgrundlage nicht mit den Vorgaben des Datenschutzrechts vereinbar. Die Zuständigkeit für Maßnahmen nach dem Auftreten übertragbarer Krankheiten liegt nach § 25 Absatz 1 IfSG beim Gesundheitsamt. Einzelnen Bürger_innen hingegen sind insoweit keine Zuständigkeiten zugewiesen. Dies bedeutet, dass es Privatpersonen, wie z. B. Vermieter_innen, zu keinem Zeitpunkt zusteht, ohne Einwilligung der betroffenen Person Dritte über mögliche Infektionen zu informieren.

11.4 Alles mit V: Verkehr, Vereine, Videoüberwachung

11.4.1 Sind smarte Poller auch smarte Datenschützer?

Smarte Poller erkennen automatisch, welche Fahrzeuge berechtigt sind, einen bestimmten Straßenabschnitt zu befahren. So kann beispielsweise geregelt werden, dass zu einem bestimmten Bereich und innerhalb eines bestimmten Zeitraumes nur Fahrzeugen von Anwohner_innen sowie Einsatzfahrzeugen die Zufahrt gewährt wird. Lässt sich der Einsatz dieser Technik auch datenschutzkonform gestalten?

Eine Kommune wandte sich mit der Bitte um Beratung bezüglich einer Polleranlage an uns. Bis dato würde die Zufahrt durch den Einsatz von Transpondern geregelt. Dabei sei jedoch problematisch, dass bei Verlust eine Ersatzbeschaffung sehr aufwändig und mit hohen Kosten verbunden sei. Das viel größere Problem bestünde jedoch darin, dass die Transponder an Unberechtigte weitergegeben würden. Es komme häufig zu verbotswidrigen Einfahrten und damit einhergehender Lärmbelästigung in den Abend- und Nachtstunden, auch verbunden mit der sogenannten Poserszene. Zudem würden Fremdfahrzeuge auf Bewohnerparkplätzen und in Brandschutzzonen abgestellt. Daher prüfe man nun den Einsatz sogenannter smarter Poller.

Die smarten Poller sind mit einer Kamera ausgestattet. Ist der Poller im Straßenboden versenkt, ist die Kamera ebenfalls deaktiviert. Nur wenn der

Wie smart sind smarte Poller? Wenn das einer Kommune unklar ist, lohnt eine Beratung beim LfDI.

Poller oben ist, werden Fahrzeuge von der Kamera erfasst. Die Objekterkennung mittels eines neuronalen Netzes (künstliche Intelligenz) ist dann aktiv. Wird beispielsweise ein KfZ-Kennzeichen erkannt, erfolgt ein Abgleich mit einer Positiv-Liste, in der berechtigte Fahrzeuge hinterlegt sind. Liegt ein Treffer vor, wird der Poller versenkt und damit die Zufahrt ermöglicht. Darüber hinaus werden auch Rettungs-, Polizei- und Feuerwehrfahrzeuge erkannt. Auf die Datenverarbeitung solle mit Schildern hingewiesen werden. Die bisherigen Inhaber_innen von Transpondern sollen die Wahl haben, ob sie weiterhin die Transponder nutzen oder auf die automatische Erkennung umsteigen.

Aus datenschutzrechtlicher Sicht ist einerseits problematisch, aufgrund welcher Rechtsgrundlage die Datenverarbeitung erfolgen kann. § 18 LDSG regelt die Videoüberwachung öffentlich zugänglicher Räume. Dies setzt voraus, dass die Videoüberwachung zum Schutz von Sachen oder Personen, die sich in unmittelbarer Nähe einer der in § 18 Abs. 1 Nr. 1 und Nr. 2 LDSG genannten baulichen Anlagen öffentlicher Stellen befinden, erforderlich ist. Eine Gefährdungslage für Sachen oder Personen wurde jedoch nicht dargelegt. Selbst bei Vorliegen dieser Voraussetzung wäre die Erforderlichkeit fraglich, zumal das Transpondersystem weiterhin parallel zum Einsatz kommen soll. Darüber hinaus ist an eine Datenverarbeitung aufgrund einer Einwilligung gem. Art. 6 Abs. 1 Unterabs. 1 Buchst. a DS-GVO i. V. m. Art. 7 DS-GVO zu denken. Im Hinblick auf die zur Durchfahrt berechtigten Personen wäre die Einholung von Einwilligungserklärungen grundsätzlich denkbar.

Allerdings werden auch die Kfz-Kennzeichen und damit personenbezogene Daten von Personen erfasst, die über keine Durchfahrtsberechtigung verfügen. Wird auf einem Schild auf die Verarbeitung hingewiesen, kann in dem bloßen Betreten oder Befahren des Erfassungsbereichs der Kamera keine Einwilligung in eine Datenverarbeitung gesehen werden. Darüber hinaus ist es auch möglich, dass Personen über eine Durchfahrtsberechtigung verfügen, aber nicht in die Verarbeitung einwilligen. Durchfahrtsberechtige Personen, etwa mit eigenem Stellplatz, könnten nicht ohne Videoerfassung ihren Stellplatz nutzen – die Freiwilligkeit der Einwilligung wäre daher zweifelhaft.

Mit der Kommune wurden die datenschutzrechtlichen Probleme erörtert. Die Kommune hat sich in der Folge für eine andere, kosten- und datensparsamere Lösung entschieden. Vor dem Einsatz neuer Technologien, bei denen personenbezogene Daten verarbeitet werden, lohnt es sich, den LfDI im Rahmen einer Beratung einzubeziehen. So können Investitionen in Technologien, die nicht datenschutzkonform sind, vermieden werden.

11.4.2 Intelligente Verkehrszählung mit intelligentem Datenschutz?

Durch den Einsatz von Infrarottechnik, Künstlicher Intelligenz und Daten über Bewegungen im Mobilfunknetz kann festgestellt werden, wie viele Fahrzeuge in einem bestimmten Zeitraum einen Streckenabschnitt befahren und mit wie vielen Personen die Fahrzeuge besetzt sind. Wir prüften die datenschutzrechtliche Zulässigkeit.

Verkehrszählungen stellen eine wichtige Datengrundlage dar, wenn es darum geht, für Fahrgemeinschaften zu werben oder Fördermaßnahmen zur Bildung von Fahrgemeinschaften zu evaluieren. Darüber hinaus können auf dieser Datengrundlage Maßnahmen zur Verkehrssteuerung wie z. B. bezüglich Parkraum oder Fahrspuren erfolgen. Grundsätzlich können Verkehrszählungen auf unterschiedliche Art und Weise durchgeführt werden. Traditionell werden dazu Personen am Straßenrand eingesetzt, die mit Klemmbrett und Klickzähler ausgestattet händisch festhalten, wie viele Fahrzeuge in einem bestimmten Zeitraum einen Streckenabschnitt passieren. Dies erscheint zum einen nicht mehr ganz zeitgemäß. Zum anderen bestehen inzwischen leistungsfähigere technische Alternativen.

Wir befassten uns mit dem Einsatz eines Systems, bei dem zunächst Tiefenbilder auf Infrarotbasis erstellt werden. Der Tiefenbild-Sensor liefert dabei Aufnahmen bei denen Personen, die in einem Pkw sitzen, nur schemenhaft zu sehen sind. Im Anschluss kommt eine künstliche Intelligenz in Form von Bilderkennung zum Einsatz, die ermittelt, mit wie vielen Personen ein Pkw besetzt ist. Die DS-GVO gilt gemäß Art. 2 Abs. 1 DS-GVO nur für die Verarbeitung personenbezogener Daten. Darunter sind gem. Art. 4 Abs. 1 HS 1 DS-GVO alle Informationen zu verstehen, die sich auf eine identifi-

zierte oder identifizierbare Person beziehen. Die bloßen Umrisse einer Person ermöglichen jedoch noch keine Identifizierung. Die Beschriftung von Kfz-Kennzeichen, bei der es sich um ein personenbezogenes Datum handelt, wird von den Kameras des eingesetzten Systems nicht erfasst, da die starke Reflexion der Kfz-Kennzeichen zu einer starken Überbelichtung in diesem Bereich führt. Daher liegt insoweit keine Verarbeitung personenbezogener Daten vor und die DS-GVO ist nicht anwendbar. Etwas anderes ergibt sich auch nicht daraus, dass zusätzlich Daten von Mobilfunkbetreibern über Bewegungen im Mobilfunknetz eingesetzt werden. Diese Daten wurden bereits zuvor durch die Mobilfunkbetreiber anonymisiert. Es handelt sich um die abstrakte Angabe, wie viele Mobilfunkteilnehmende sich in einem bestimmten Zeitfenster in dem Bereich einer Mobilfunkzelle aufgehalten haben. Die Ermittlung ist möglich, da sich die Mobilfunkgeräte automatisch mit der nächstgelegenen/signalstärksten Mobilfunkbasisstation verbinden. Eine Mobilfunkbasisstation versorgt immer nur einen begrenzten räumlichen Bereich (Mobilfunkzelle). Durch den Vergleich der Verbindungszahlen bei verschiedenen Mobilfunkbasisstationen kann festgestellt werden, wie sich die Mobilfunkteilnehmer bewegen. Die Daten werden dabei erst ab einer bestimmten Anzahl an Mobilfunkteilnehmern in einer Mobilfunkzelle erhoben, so dass ein Bezug zu einzelnen Personen ausgeschlossen werden kann. Auch durch Hinzuziehen dieser anonymisierten Daten wird keine Identifizierung der betroffenen Personen ermöglicht.

Im Ergebnis haben wir den Einsatz der Technik als zulässig bewertet, da keine personenbezogenen Daten verarbeitet werden. Die Datengrundlage kann zu Maßnahmen für besseren Klimaschutz und eine Verringerung des Stauaufkommens eingesetzt werden. Es zeigt sich: Die intelligentesten Datenverarbeitungen kommen ganz ohne Personenbezug aus.

11.4.3. Urteil des OLG Stuttgart zur Videoüberwachung in einem Lebensmittelgeschäft

Neben der Möglichkeit, sich als betroffene Person an die Aufsichtsbehörde zu wenden, können auch zivilrechtliche Ansprüche gegen Verantwortliche einer unzulässigen Videoüberwachung geltend gemacht werden. Diese können ebenfalls gerichtlich durchgesetzt werden. Das Urteil des OLG Stuttgart vom 18.05.2021 (Az. 12 U 296/20) hatte eine Videoüberwachung in einem Lebensmittelgeschäft zum

Tiefenbilder-Sensoren können bei Verkehrszählungen sehr intelligent funktionieren – und helfen, künftig Staus zu vermeiden.

Gegenstand. Das OLG hat den Beklagten dazu verurteilt, es zu unterlassen, in den öffentlich zugänglichen Verkaufsräumen des Lebensmittelgeschäfts eine Videoüberwachung entgegen der Bestimmung der den Kläger individuell schätzenden Normen des § 4 BDSG sowie des Art. 6 DS-GVO zu betreiben.

Der Beklagte habe dargelegt, dass er zur Abschreckung von Dieben nur bestimmte Bereiche filme und er aus wirtschaftlichen Gründen nicht weiteres Personal zur Überwachung einstellen könne. Der Beklagte habe jedoch nicht vorgetragen, dass er den Zweck der Videoüberwachung vor Beginn der Maßnahme festgelegt habe. Ob der Beklagte den Umstand der Beobachtung sowie den Namen und Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar gemacht hat, wie dies § 4 Abs. 2 BDSG vorschreibe, sei offen. Der Beklagte habe zuletzt lediglich behaupten lassen, Schilder aufgestellt zu haben. Die Beweislast dafür, dass die Videoüberwachung auf rechtmäßige Weise erfolge, liege sowohl nach den allgemeinen Beweislastregeln im Zivilprozess als auch gem. Art. 5 Abs. 2 DS-GVO beim Beklagten. Der Beweis eines rechtmäßigen Betriebs der Videoüberwachung sei dem Beklagten nicht gelungen. Unterstellt, es läge ein berechtigtes Interesse etc. an der Videoüberwachung vor, würde der Beklagte seine Kund_innen gleichwohl unter Verstoß gegen das Datenschutzrecht beobachten, da es jedenfalls an der vorherigen Festlegung eines Zwecks der Maßnahme fehle, wobei das OLG auf §§ 4 Abs. 1 Nr. 3 BDSG und § 6b Abs. 1 Nr. 3 BDSG a.F. verwies. Ob aktuell eine ordnungsgemäße Kenntlichmachung der Beobachtung und Nennung der verantwortlichen Stelle gem. § 4 Abs. 2 BDSG und § 6 b Abs. 2 BDSG erfolge, falle daneben nicht mehr ins Gewicht.

Personen, die sich tagtäglich mit Videoüberwachung befassen, fällt bei der Entscheidung sofort auf, dass das OLG neben Art. 6 DS-GVO auch § 4 BDSG sowie dessen Vorgängervorschrift als Schutzgesetze gem. § 823 Abs. 2 BGB im Rahmen des Unterlassungsanspruchs prüft. Dies überrascht, zumal das Bundesverwaltungsgericht in seinem Urteil vom 27.3.2019 (Az. 6 C 2/18) im Rahmen eines obiter dictums § 4 BDSG für nicht anwendbar erklärt hat. Eine solche Regelung würde eine Öffnungsklausel in der DS-GVO voraussetzen. Für die Videoüberwachung durch private Stellen fehlt es jedoch an einer Öffnungsklausel. Richtigerweise wäre also lediglich Art. 6 Abs. 1 DS-GVO als Schutzgesetz zu prüfen gewesen.

© titikul_b – stock.adobe.com

Wie die Videoüberwachung im Lebensmittelgeschäft funktioniert, beschäftigt auch Gerichte.

Die Entscheidung des OLG Stuttgart ist im Ergebnis zu begrüßen. Soweit das OLG den Anspruch des Klägers auch mit § 4 BDSG begründet, kann jedoch der Argumentation nicht zugestimmt werden, da die Vorschrift wegen des Vorrangs der DS-GVO nicht anwendbar ist.

11.4.4 Videoüberwachung in Gaststätten – Verwaltungsgericht Stuttgart bestätigt unsere Anordnung

Videoüberwachung in Gaststätten ist immer wieder der Gegenstand von Beschwerden und Kontrollen des LfDI. Hierüber haben wir bereits im 33. Tätigkeitsbericht (2016/2017) und im 36. Tätigkeitsbericht (2020) informiert. Sind Verantwortliche nicht bereit, freiwillig datenschutzkonforme Zustände herzustellen, kann die Aufsichtsbehörde gem. Art. 58 Abs. 2 DS-GVO Maßnahmen per Verwaltungsakt anordnen. Im vorliegenden Fall wurde die Videoüberwachung des Gastraumes einer Gaststätte während der Öffnungszeiten untersagt. Die Anfechtungsklage des Verantwortlichen hatte keinen Erfolg.

Gegenstand der Entscheidung vom 12. März 2021, Az. 18 K 8202/19, war ein sogenanntes Live-Monitoring des Gastraums. Echtzeitbilder von zwei Kameras im Gastraum wurden in das dahinter liegende Büro des Inhabers der Gaststätte übertragen. Darüber hinaus konnte der Inhaber die Livebilder jederzeit über sein Mobiltelefon einsehen. Eine Speicherung der Aufnahmen fand nicht statt. Die beiden Kameras waren über der Theke angebracht und erfassten den Eingangsbereich der Gaststätte, Stühle und Tische im Gastraum, Gästesitze an der Theke und einen kleinen Bereich hinter der Theke. Betroffen waren sowohl Gäste als auch das Personal, das im Servicebereich tätig ist. Im Eingangsbereich wurde auf die Videoüberwachung mittels eines Schildes hingewiesen.

Der Inhaber der Gaststätte war der Auffassung, dass die Videoüberwachung zur Wahrung berechtigter Interessen gem. Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO erforderlich sei. Zierliche, weibliche Mitarbeiterinnen seien bereits von Gästen angegangen worden. Da die Übertragung der Videodaten in sein Büro stattfinde, habe er umgehend die Situation deeskalieren können. Die Mitarbeiterinnen hätten sich aktiv an ihn gewandt und gebeten, eine entsprechende Anlage zu installieren. Vorfälle hätten gezeigt, dass sich das Verfahren bewährt habe. Bei den geschilderten Situationen seien die Gäste der Gaststätte verwiesen worden. Eine Mitarbeiterin sei mindestens zu einer Gelegenheit sexuell belästigt beziehungsweise unangemessen angefasst worden. Darüber hinaus sei bereits in die benachbarte Bäckerei eingebrochen und der Tresor gestohlen worden. Restaurants seien bekanntlich auch bargeldintensive Betrieb, bei denen es in den Abendstunden zu Überfällen kommen könne. In seiner Gaststätte sei dies jedoch noch nicht vorgekommen. Mildere Maßnahmen, wie etwa die Einstellung von Sicherheitspersonal in den Abendstunden, seien verworfen worden. Zum einen handele es sich dabei nicht um weniger einschneidende Maßnahmen, da sich die Gäste insoweit in noch stärkerem Maße beobachtet fühlen würden. Zum anderen sei dies Maßnahme wirtschaftlich untragbar.

Dem Verwaltungsgericht zufolge stützte der LfDI die Untersagung zu recht auf Art. 58 Abs. 2 Buchst. f DS-GVO. Danach ist es der Aufsichtsbehörde gestattet, eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen. Das Verwaltungsgericht führt weiter aus, dass die Videoüberwachung rechtswidrig sei, da keine der in Art. 6 Abs. 1 DS-GVO genannten Rechtsgrundlagen erfüllt ist. Die von der Videoüberwachung betroffenen Personen hätten nicht in die Datenverarbeitung eingewilligt. Eine (konkludente) Willenserklärung sei nicht im Lesen des Schildes am Eingang zu erkennen. Dass die Mitarbeiterinnen des Klägers selbst um eine Überwachung gebeten und damit gegebenenfalls in eine solche eingewilligt haben, spiele keine Rolle, da nicht nur Mitarbeiterinnen des Klägers, sondern auch viele Gäste von den Kameras erfasst werden würden. Die Videoüberwachung sei auch nicht nach Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO gerechtfertigt.

Danach ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei den betroffenen Personen um ein Kind handelt.

Nach Auffassung des Verwaltungsgerichts ist die Videoüberwachung bereits nicht erforderlich. In Anlehnung an die Rechtsprechung des Bundesverwaltungsgerichts sei Erforderlichkeit dann anzunehmen, wenn ein Grund, etwa eine Gefährdungslage, hinreichend durch Tatsachen oder die allgemeinen Lebenserfahrung belegt sei und ihm nicht ebenso gut durch eine andere gleich wirksame, aber schonendere Maßnahme Rechnung getragen werden könne (vgl. BVerwG, Urteil vom 27. 03.2019 – Az. 6 C 2/18). Die Gesichtspunkte der Verhinderung von Straftaten sowie des Schutzes von Mitarbeiterinnen stellten zwar grundsätzlich berechtigte Interessen im Sinne von Art. 6 Abs. 1 Unterabs. 1 Buchst. f DS-GVO dar. Vorliegend könnten aber keine Tatsachen festgestellt werden, die die Annahme stützten, in der Gaststätte des Klägers bestehe eine erhöhte, über das allgemeine Lebensrisiko hinausgehende Gefährdungslage. Der Vortrag bezüglich der Einbrüche in die benachbarte Bäckerei vermöge keine erhöhte Gefährdungslage bezüglich der Gaststätte selbst zu begründen. So habe der Inhaber bereits nicht vorgetragen, dass der Einbruch während der Öffnungszeiten der Gaststätte erfolgt sei. Vorliegend gehe es aber nur um die Untersagung der Videoüberwachung während der Öffnungszeiten, eine Videoüberwachung außerhalb der Öffnungszeiten sei vom LfDI nicht untersagt worden. Sofern der Inhaber vorträgt, dass es Vorfälle gegeben habe, bei denen seine zierlichen Mitarbeiterinnen sexuell belästigt beziehungsweise unangemessen angefasst worden seien, fehle es bereits an einem substantiierten Vortrag sowie entsprechender Nachweise.

Darüber hinaus handele es sich um vereinzelte Vorfälle, die keine besondere Gefährdungslage begründen würden. Nach Auffassung des Gerichts habe die körperliche Anwesenheit des Inhabers im Lokal eine stärkere Wirkung auf die Gäste und stelle eine effektivere und schonendere Maßnahme zum Schutz der Mitarbeiterinnen dar. Der Kläger habe auch nicht ansatzweise dargelegt, dass die Einstellung von Sicherheitspersonal unverhältnismäßig teuer wäre. Bis zur gerichtlichen Entscheidung habe er keine nachprüfbaren Angaben gemacht. Im Übrigen würden auch die Interessen der von der Videoüberwachung betroffenen Personen überwiegen. Das Verwaltungsgericht Stuttgart folgt in weiten Teilen der Rechtsprechung des Bundesverwaltungsgerichts (BVerwG, Urteil vom 27. 03.2019 – Az. 6 C 2/18) und bestätigt unsere datenschutzrechtliche Einschätzung. Zum Nachweis einer Gefährdungslage beziehungsweise der

© titikul_b – stock.adobe.com

Auch in Gaststätten kommen Videokameras zum Einsatz – dafür gelten klare Regeln für den Betreiber.

Erforderlichkeit einer Videoüberwachung bedarf es einer substantiierten Argumentation sowie geeigneter Nachweise.

11.4.5 Videoüberwachung in der „Milchstraße"

Aufgrund einer Bürgerbeschwerde wurden wir darauf hingewiesen, dass sich auf der Website einer Sternwarte mit Planetarium via Webcam live die Bewegungen von Personen auf der „Milchstraße" zu sehen wären.

Nicht nur aufgrund dieser astrologischen Sensation sahen wir uns veranlasst, diesem Umstand nachzugehen und besuchten die Webseite des betreibenden Vereins. Zu unserer Enttäuschung wurde über die betriebene Webcam der genannten Sternwarte aber nicht die „Weite des Weltalls" abgebildet, sondern „nur" ein weitläufig asphaltierter öffentlicher Weg umgeben von einer grünen Landschaft. Auch die Betrachtung des eingereichten Screenshots, auf welchem tatsächlich diverse Personen abgebildet waren, brachte uns nicht weiter.

Fündig wurden wir bei einer genaueren Recherche der Homepage des „Sternenforscher"-Vereins. Neben Übertragungen einer Webcam befand sich ein Hinweis, dass ‚die WebCam minütlich ein aktuelles Bild aus der „Musterstadt' Milchstraße liefert." Nicht aufgrund dieser unzureichenden Informationen für Betroffene, sondern aufgrund des offensichtlich unbekümmerten „Abfilmens" einer irdischen öffentlichen Straße richteten wir eine Anfrage an den Vorstand des Vereins.

Statt von unseren umfangreichen Abhilfemaßnahmen Gebrauch zu machen, beschränkten wir uns auf einen „Wink mit dem Fernrohr", indem wir dem Betreiber mitteilten, dass die vereinseigene Webcam vermutlich versehentlich die irdische „Milchstraße" im Internet zeigen würde. Zudem wiesen wir auf den Vereinszweck hin, wonach die Kamera wohl eher auf das Himmelsgewölbe und das Sternenfirmament auszurichten wäre.

Freilich kamen wir nicht ohne ein paar wenige rechtliche Ausführungen aus. So teilten wird mit, dass die vorliegende Webcam unter die strengen rechtlichen Voraussetzungen einer privaten Videoüberwachung im öffentlichen Bereich i.S. Art. 6 Abs. 1 Buchst. f DS-GVO fallen würde und in dieser Form nicht zulässig wäre. Dies begründeten wir damit, dass eine Webcam in der Regel nur dann datenschutzkonform betrieben werde, wenn deren Bildaufnahmen keinen Personenbezug aufzeigen oder die gefilmten Betroffenen vorher wirksam eingewilligt hätten. Datenschutzrechtlich nicht zu beanstanden sind dagegen weitläufige Übersichtsaufnahmen ohne Zoomfunktion, bei verminderter Bildqualität und einer Frequenz, welche nur wenige Bilder täglich anfertigt.

Zu unserer Verwunderung teilte uns die bestellte Datenschutzbeauftragte des Vereins selbstsicher mit, dass die Webcam nicht nur korrekt ausgerichtet wäre, sondern auch datenschutzkonform betrieben werde. Verwiesen wurde hier auf die Vereinssatzung und den unter § 2 Nr. 2 festgehaltenen Vereinszweck mit dem Betrieb einer öffentlich zugänglichen Sternwarte, Sternwartenführungen und die Betreuung beobachtender Amateur-Astronom_innen. Mit der Videoüberwachung des öffentlichen Raumes werde nach Auffassung der Datenschutzbeauftragten ein legitimer und nachvollziehbarer Zweck verfolgt, da eine Sonnen- und Sternbeobachtungen nur bei klarem Himmel möglich wäre. So wurden wir auf die außerordentliche Bedeutung der aktuellen Wetterlage für den potentiellen Besucher der Sternwarte hingewiesen. Gerade der oberschwäbische Hochnebel wäre nicht förderlich zur Sternenforschung, weshalb es von essenzieller Wichtigkeit sei, auch die Witterungsverhältnisse und Straßenbeschaffenheit der gerade verlaufenden 250 Meter langen „Milchstraße" ins Blickfeld der Kamera zu nehmen. Die webbasierte Einsicht auf die „Milchstraße" ermögliche der/dem Betrachter_in anhand der dargestellten Wetterlage vor Ort zumindest eine Prognose, ob ein Besuch des Planetariums lohnenswert erscheine oder nicht.

Der Verein war deshalb der Ansicht, dass er für den Betrieb seiner Webcam ein berechtigtes Interesse und damit eine datenschutzkonforme Rechtsgrundlage gem. Art. 6 Abs. 1 lit. f DS-GVO habe. Erfreulicherweise war sich der Verein seiner Informations- und Rechenschaftspflichten bewusst und verfügt sowohl über ein Verfahrensverzeichnis im Sinne des Art. 30 DS-GVO als auch über entsprechende Hinweisschilder in der „Milchstraße". Obwohl wir die Bemühungen des Vereins zur Erfüllung seiner Rechenschafts- und Informati-

onspflichten ausdrücklich begrüßen, konnten wir doch seine Auffassung zur Frage, ob eine wirksame Rechtsgrundlage vorliegt, nicht teilen. Denn bei der Berufung auf Art. 6 Abs. 1 lit. f DS-GVO hat der Verein sein „berechtigtes Interesse" zu einseitig gewichtet und dabei dem Interesse der von der Videographierung Betroffenen zu wenig Bedeutung beigemessen.

Durch eine Videoüberwachung wird in das allgemeine Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG in seiner Ausprägung als Grundrecht auf informationelle Selbstbestimmung eingegriffen. Dieses Recht umfasst die Befugnis der/des Einzelnen, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und selbst über die Preisgabe und Verwendung öffentlicher Daten zu bestimmen (BVerfGE 65, 1; BGH NJW 2010, 1533).

Hat eine Videoüberwachung – wie hier – allein den Zweck, die Wetterlage zu dokumentieren, muss dieses legitime Ziel gegenüber den Grundrechten betroffener Personen bereits deshalb zurücktreten, weil der Zweck auch ohne die Verarbeitung personenbezogener Daten erreicht werden kann. So könnte die WebCam leicht so ausgerichtet werden, dass nur Natur (beispielsweise die Baumkronen) oder ausschließlich private Flächen von der WebCam erfasst würden. Dass es sich bei der zum Planetarium führenden „Milchstraße" um keine Durchgangsstraße handelt, sondern um eine Sackgasse, ändert an der Schutzwürdigkeit der sie nutzenden Personen nichts, denn die so ausgerichtete Videoübertragung betrifft all jene in ihrem Recht auf informationelle Selbstbestimmung, die sich in der „Hemisphäre" des Planetariums befinden, selbst wenn sie ausschließlich irdische Absichten wie einen Wochenendspaziergang verfolgen.

Zwar wurden wir zuletzt unterrichtet, dass die Kamera vorläufig vom Netz genommen wurde. Allerdings soll sie alsbald neu ausgerichtet werden. Wir werden die Sternengucker auch künftig dabei unterstützen, ihr Interesse statt auf den schwäbischen, lieber auf den Orionnebel zu richten.

11.4.6 Türklingelkamera – „Augen auf!"

Hinsichtlich dieser Thematik hatten wir im vergangenen Jahr eine Vielzahl von Eingaben sowohl von Personen, die sich eine solche Technik „ins Haus holen" wollten, als auch von Personen, die sich durch diese Videotechnik in unzulässiger Weise überwacht fühlten.

Oft handelte es sich bei der eingesetzten Technik um Kamerasysteme, die auch eine Datenspeicherung umfasste. Wir mussten in diesen Fällen stets darauf hinweisen, dass diese Art der Klingelkamera in rechtlicher Hinsicht mit einer privaten Videoüberwachung gleichzusetzen ist, die sich an den gesetzlichen Grundsätzen des Art. 6 DS-GVO zu messen hat und nach diesem Maßstab in vielen Fällen unzulässig betrieben wurde.

Häufig konnten wir für weitergehende Informationen zum datenschutzkonformen Betrieb einer Klingelkamera oder Videogegensprechanlage auf die Orientierungshilfe der Datenschutzkonferenz verweisen, die praktische Hinweise für die Installation und den Betrieb entsprechender Kameras gibt. Immer wieder mussten wir darauf hinweisen, dass nicht dem Hersteller, sondern den Betreiber_innen die datenschutzrechtliche Verantwortlichkeit obliegt. Verbraucher_innen haben oftmals nicht im Blick, dass einige der erhältlichen Kamerasysteme für den „Weltmarkt" produziert werden, sodass die Kamerasysteme zum Teil nicht mit datenschutzfreundlichen Voreinstellungen versehen sind, weil die DS-GVO als europäisches Recht für diese Hersteller nicht den (alleinigen) Maßstab darstellt.

Wiederholt wurde durch uns festgestellt, dass installierte Türklingelkameras sich nicht nur anlassbezogen durch das betätigen der Türklingel aktivieren lassen, sondern durch das bloße Betätigen einer am Gerät angebrachten Vorrichtung. Auf diese Weise können und werden Hausmitbewohner_innen oder Mieter_innen überwacht, wenn sie sich im Erfassungsbereich der Türklingelkamera aufhalten, beispielsweise um den Müll zu entsorgen oder den Fahrradstellplatz aufsuchen. Eine derartige Überwachung ermöglicht eine Verhaltenskontrolle und greift damit erheblich in das Recht auf informationelle Selbstbestimmung der Betroffenen ein. Eine solche Nutzung von Türklingelkameras ist deshalb unzulässig.

Dass eine Türklingelkamera in der Praxis in manchen Fällen nicht nur den Nahbereich der Haustüre, sondern den vollständigen Gehweg über die gesamte Gebäudefront erfasste – und damit den öffentlichen Raum – zeigte uns ein Fall der als Beschwerde bei uns einging. Dabei wurde die Kamera an der Hausecke eines Mehrfamilienhauses so installiert, dass aufgrund des weiten Erfassungsbereichs der gesamte Gehweg und Teile der Straße überwacht wurden. Erfreulicherweise zeigte sich der Verantwortliche einsichtig und erklärte sich nach einem beratenden Telefonat bereit, die Kamera an einer geeigneteren Position zu platzieren.

Sorgen bereiten uns solche Videotürklingelsysteme, die ihre Aufnahmen in „Clouds" speichern. Zwischenzeitlich verfügen viele, häufig auch sehr preisgünstige Produkte, über eine solche Speicherfunktion, wobei damit in vielen Fällen eine Datenübertragung ins EU-Ausland einhergeht. Zwar hat die EU-Kommission infolge des sogenannte „Schrems-II- Urteils" vom 16. Juli 2020 (Rechtssache C-311/18) am 4. Juni 2021 neue Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer erlassen. Dennoch haben Verantwortliche auch nach diesen neuen Klauseln umfangreiche rechtliche und tatsächliche Sorgfaltspflichten, die Privatpersonen kaum erfüllen können. Aus datenschutzrechtlicher Sicht sind daher vor allem solche Systeme vorzugswürdig, die gerade keine dauerhafte Speicherung der Bildaufnahmen vornehmen. Deshalb: Augen auf beim Türklingelkamerakauf!

11.4.7 Wenn die Polizei sich selbst beobachtet

Im Frühsommer wurden wir sowohl durch einen Pressebericht als auch durch anonyme Hinweisgeber aus den Reihen der Polizei darauf hingewiesen, dass in einigen Schießanlagen der Polizei Videokameras installiert seien, die datenschutzrechtliche Fragen aufwerfen würden. Auch Landtagsabgeordnete wurden hierauf aufmerksam und richteten daraufhin eine parlamentarische Anfrage (Drs. 17/275) an die Landesregierung / das Innenministerium.

Das Einsatz- und Schießtraining gehört zu einem der wichtigsten Elemente im Rahmen der polizeilichen Ausbildung. Aber auch nach bestandener Laufbahnprüfung wird das Gelernte nicht nur in regelmäßigen Abständen wiederholt, sondern das bestehende Leistungsniveau verbessert. Konkrete Anweisungen hierzu enthält die bundesweit geltende Polizeidienstvorschrift 211 (PDV 211) zur theoretischen und praktischen Ausbildung mit Dienstwaffen. Geregelt ist aber nicht nur der Ablauf der Ausbildung, sondern es werden auch Vorgaben zu den Trainingseinheiten und den jährlich zu erfüllenden Kontrollübungen gemacht.

Wie auch im Leistungssport erschien es den Verantwortlichen beim Landespolizeipräsidium, der Hochschule der Polizei und dem Technik-Präsidium nützlich, im Bereich der polizeilichen Schießaus- und Weiterbildung modernste Technik einzusetzen. Hierzu soll der Einsatz von Videotechnik dienen. Denn mittels Videoanalyse können sich Treffsicherheit und der Umgang mit der Waffe besser vermitteln und erlernen lassen. Die Vorteile sind unbestreitbar: Der Verbesserungs- und Lernprozess der Polizeibeamt_innen in taktischen Situationen kann dokumentiert und unmittelbar korrigiert werden. In einer anschließenden Besprechung mit den Einsatztrainer_innen können Gelungenes und Verbesserungsbedarf in aufbereiteter Form gezeigt und besprochen werden.

Eine solche Videoübertragung stellt – ebenso wie eine Speicherung der Aufnahmen – eine Verarbeitung personenbezogener Daten dar, die einer datenschutzrechtlichen Rechtsgrundlage bedarf. Nachdem uns zugetragen wurde, dass die Videotechnik in den Schießanlagen ohne Kenntnis der Polizeibeamt_innen betrieben würde, schied eine Einwilligung als Rechtsgrundlage aus, zumal diese in einem Beschäftigungs- beziehungsweise Beamtenverhältnis aufgrund von erheblichen Zweifeln an der Freiwilligkeit einer solchen Einwilligung ohnehin kaum eine taugliche Grundlage hätte darstellen können.

Eine Herausforderung lag und liegt weiterhin darin, dass weder das Landesdatenschutzgesetz (LDSG) noch das Polizeigesetz BW (PolG) eine ausdrückliche Regelung zum Einsatz von Videotechnik zu Ausbildungszwecken enthält. Stattdessen normiert § 15 Abs. 7 S. 1 LDSG ein ausdrückliches Verbot des Einsatzes von Videotechnik zur Leistungskontrolle. Wir hatten also zu klären, welche Anforderungen an eine ggf. noch zu schaffende Rechtsgrundlage zu stellen wären und in welchen Ausbildungs- oder Prüfungssituationen auf der Schießbahn von einer

Leistungskontrolle im Sinne des § 15 Abs. 7 LDSG auszugehen war, die ein Verbot der Aufzeichnung bedeutete.

Auf Einladung des Innenministeriums – Landespolizeipräsidium (IM-LPP) und des Polizeipräsidiums Stuttgart nutzten wir die Gelegenheit, um uns am 26.08.2021 bei einem Ortstermin in der Schießanlage des Polizeipräsidiums Stuttgart die Funktionsweise und die verschiedenen Einsatzzwecke für die Videotechnik erläutern zu lassen. Hierbei wurde uns u. a. erläutert, dass die Schießausbildung deutlich an Komplexität zugenommen habe. Dies insbesondere deshalb, weil u. a. dynamische Einsatzszenarien, wie das Vorgehen bei einer sogenannte „Amoklage" trainiert würden. In solchen Trainingssituationen sei der Einsatz der Videotechnik eine effektive und notwendige Unterstützung der/des Schießausbilderin/Schießausbilders.

Nach wie vor besteht keine spezifische Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Zusammenhang mit sogenannte Schützenbeobachtungskameras. Wollte man eine solche Datenverarbeitung auf die Generalklausel des § 15 Abs. 1 LDSG stützen, wäre zu fragen, ob diese Regelung hinreichend bestimmt ist, um den damit verbundenen Grundrechtseingriff zu rechtfertigen. Denn je tiefer der Eingriff in das betroffene Grundrecht erfolgt, desto höher sind die Anforderungen an die Bestimmtheit der Rechtsgrundlage. Angesichts der hohen Qualität der durch die Schützenbeobachtungskameras aufgenommenen Videos und des Umfangs der beabsichtigten Aufzeichnungen (nämlich während der gesamten Dauer des Schießtrainings) kann nach hiesiger Auffassung der Einsatz der Schützenbeobachtungskameras durch § 15 LDSG allein nicht gedeckt sein. Die Schaffung einer ergänzenden, konkretisieren-

Auch bei Türklingelkameras sollte man darauf achten, dass sie datenschutzkonform sind.

den Rechtsgrundlage, wie sie von Seiten des IM-LPP beabsichtigt ist, erscheint deshalb geboten.

Zu bedenken ist hierbei auch, dass durch die Schützenbeobachtungskameras nicht nur die Erfassung der Schützen einer Rechtsgrundlage bedarf, sondern auch die Erfassung der Schießausbilder. Im Gegensatz zu den Schützen würden die Schießausbilder bei einer dauerhaften Videoaufzeichnung über einen längeren Zeitraum ununterbrochen erfasst, ohne dass sie sich dieser entziehen können. Der (dauerhafte) Einsatz von Videokameras am Arbeitsplatz, der grundsätzlich zur Leistungskontrolle eingesetzt werden kann – auch wenn dies nicht beabsichtigt ist – und/oder dem sich die/der Beschäftigte nicht entziehen kann, ist unabhängig von einer etwaigen Regelung in einer Dienstvereinbarung unzulässig.

Selbst bei Vorliegen einer hinreichenden Rechtsgrundlage muss der Einsatz der Schützenbeobachtungskamera die Voraussetzung der Erforderlichkeit im Rechtssinne erfüllen, also das relativ mildeste Mittel darstellen. Diesbezüglich wurde uns vermittelt, dass die Schießausbildung an Komplexität zugenommen habe und im Einzelfall für eine_n Schießausbilder_in ohne Zuhilfenahme technischer Unterstützung kaum zu bewältigen sei. Die Unterschiedlichkeit der Trainingsszenarien ist jedoch auch bei der Beurteilung der Erforderlichkeit des Einsatzes der Schützenbeobachtungskameras zu berücksichtigen. Während der Kameraeinsatz bspw. bei Amoktrainingssituationen tatsächlich erforderlich sein kann, erscheint dies bei der Vermittlung von Grundfertigkeiten wie dem richtigen „Ziehen" der Waffe aus dem Holster eher schwer zu rechtfertigen.

Im Rahmen der Verhältnismäßigkeitsprüfung sind zudem die Belange der Polizeipräsidien, der Hochschule der Polizei und des LPP, die den Einsatz der Schützenbeobachtungskameras befürworten, mit denen der Schütz_innen und der Schießausbilder _innen abzuwägen. Dabei ist zu berücksichtigen, dass die Betroffenen durch die vergleichsweise gute Bildqualität der Kameras nicht unerheblich in ihrem Grundrecht auf informationelle Selbstbestimmung betroffen sind. Im Rahmen der Verhältnismäßigkeitsabwägung sind zudem die Einhaltung sonstiger datenschutzrechtlicher Grundprinzipien wie Transparenz, Zweckbindung, Speicherbegrenzung und Integrität und Vertraulichkeit relevant. Wir bleiben im Austausch mit dem IM-LPP und begleiten bei der Schaffung einer datenschutzkonformen Rechtsgrundlage zum Einsatz von Videotechnik auf Schießständen.

11.4.8 Vereine sind bunt und vielseitig – auch unter datenschutzrechtlichen Gesichtspunkten

Seit dem Inkrafttreten der DS-GVO haben unser Haus vielfältigste Fragestellungen aus der Mitte des Vereinslebens erreicht. Das Vereinsleben lebt vom ehrenamtlichen Engagement. Vereine sind vielseitig, sie fördern unser Miteinander, sie sind vor Ort. Sie sind lebendige Tradition und Teil unserer Gemeinschaft. Diese Werte gilt es zu stärken und zu erhalten. Angesichts der fortbestehenden pandemischen Lage und steigender Inzidenzwerte sorgten sich zahlreiche Vereine nicht nur um die Zukunft ihrer Arbeit, sondern sahen sich zudem auch vor völlig neue Herausforderungen gestellt, wenn es darum ging, datenschutzkonform ihr Engagement aufrecht zu erhalten.

Wo Menschen zusammenkommen, menschelt es oftmals mehr, als man zu glauben meint. Entsprechend hoch war in diesem Jahr daher die Zahl von Beschwerden, bei denen die Beschwerdeführer_innen von uns eine anonyme Behandlung ihrer Beschwerden wünschten. Zu groß war oftmals die Sorge, dass es zu einem Ausschluss aus dem innig geliebten eignen Verein kommen könne, sollte der Umstand herauskommen, dass man sich als Vereinsmitglied hilfesuchend an uns als Datenschutzaufsichtsbehörde gewandt habe. Entsprechend hoch war dieses Jahr die Zahl der Beschwerden, in denen sich Vereinsmitglieder entweder vollkommen anonym oder aber mit der Bitte um anonyme Behandlung ihrer Eingabe an uns wandten.

Durchaus ist eine solche anonyme Behandlung durch uns grundsätzlich möglich, hierbei sollten folgende Umstände bedacht und beachtet werden: In vielen Fällen ist eine anonyme Bearbeitung der Beschwerden bedauerlicherweise oft nicht vollumfänglich möglich. Wie mittlerweile bekannt sein sollte, fordern wir im regulären Beschwerdeverfahren in der regel den jeweiligen Verein zur Stellungnahme auf. Um den betroffenen Vereinen rechtliche Gehör zu gewähren und zu erklären, worin wir einen Datenschutzverstoß sehen und – falls nötig – die Vereine

bezüglich einer zukünftigen datenschutzgerechten Verarbeitung beraten können, kann es daher notwendig sein, die Identität der betroffenen Person offenzulegen. Für eine effiziente Bearbeitung ist es daher oftmals zielführend, allen befürchteten Auseinandersetzungen im Verein zum Trotze, sich zunächst selbst direkt an den Verein zu wenden und dort ggf. Betroffenenrechte geltend zu machen. Erst wenn dies erfolglos bleibt, sollten betroffene Personen dann in einem zweiten Schritt auf die Datenschutzaufsichtsbehörden zukommen.

Bei Dachverbänden handelt es sich im Verhältnis zu Vereinsmitgliedern datenschutzrechtlich um Dritte im Sinne des Art. 4 Nr. 10 DS-GVO. Übermitteln Vereine personenbezogene Daten ihrer Mitglieder an einen Dachverband, bei denen der Verein Mitglied ist, wird dies in der Regel bereits aufgrund einer entsprechenden Erlaubnisnorm in der Vereinssatzung zulässig sein. Der Verein ist darüber hinaus verpflichtet, dafür Sorge zu tragen, dass die von ihm weitergegebenen Mitgliederdaten vom Dritten nicht zweckentfremdet genutzt werden (etwa durch Verkauf der Mitgliederadressen für Werbezwecke) oder dies allenfalls mit Einwilligung der betroffenen Vereinsmitglieder geschieht.

Pandemiebedingt bangten viele Vereine um die Zahl ihrer Mitglieder, und insbesondere das Abhalten der Mitgliederversammlungen stellte zahlreiche Vereine vor neue Herausforderungen. So berieten wir viele Vereine rund um die Frage, wie datenschutzkonform eine Mitgliederversammlung abgehalten werden kann. Zahlreiche Vereine entschieden sich aufgrund der geltenden Höchstteilnehmendenzahlen dafür, Versammlungen hybrid, das heißt eine Mischung aus Präsenz- und Distanzveranstaltung, abzuhalten. Grundsätzlich gilt hierbei, dass eine hybride Veranstaltung nur dann möglich ist, wenn die jeweilige Vereinssatzung dies ausdrücklich zulässt. Das Abhalten einer Mitgliederversammlung über Distanz, also über das Internet, ist ohne Satzungsgrundlage und ohne die Zustimmung/Einwilligung aller stimmberechtigten Mitglieder grundsätzlich unzulässig.

Insbesondere das Verbot von Zusammenkünften in Vereinen führte dazu, dass oftmals keine Mitgliederversammlungen als Präsenzveranstaltungen stattfinden durften und damit viele Vereine keine Entscheidungen mehr treffen konnten. Der Bundesgesetzgeber erkannte dieses Problem zum Glück sehr schnell und reagierte bereits im Frühjahr 2020 erstmalig mit einem Gesetz zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht. Hierin waren auch Sonderregelungen für Vereine enthalten. Diese Regelungen umfassten folgende Bereiche: Vorstände bleiben auch ohne Satzungsregelung bis zur Neuwahl im Amt und Online- itgliederversammlungen wurden auch ohne Satzungsgrundlage als zulässig erklärt. Diese Änderungen traten am 28. Februar 2021 in Kraft. Die Regelungen des COVID-19-Abmilderungsgesetzes für Vereine wurden bis zum 31. August 2022 verlängert (Artikel 15 des Aufbauhilfegesetzes 2021, Bundesgesetzblatt Jahrgang 2021, Teil 1 Nr. 63, vom 14.09.2021, Seite 4147 ff.). Aus der gesetzgeberisch vorgesehenen Möglichkeit, Mitgliederversammlungen auch online unter Verwendung von Videokonferenzsystemen abhalten zu können, erwuchs eine Vielzahl von Beratungsanfragen.

Insbesondere berieten wir zahlreiche Vereine zu der Frage, welche Videokonferenz-Software nun am datenschutzfreundlichsten sei und welche datenschutzrechtlichen Fallstricke bei dem Einsatz von Videokonferenzsystemen von den Vereinen zu vermeiden seien. Nicht zuletzt gilt auch bei deren Einsatz im Verein, dass die eingesetzten Tools DS-GVO-konform sein müssen. Vertiefte Hinweise hierzu können Sie unserer Handreichung entnehmen.

>> Mehr Informationen:

Handreichung des LfDI zu Videokonferenzsystemen: https://www.baden-wuerttemberg.datenschutz.de/videokonferenzsysteme/ <<

12. Veranstaltungen

12.1 LfDI 2.0: Freiheit geht voran!

Der Umzug in eine neue größere Dienststelle hatte nicht nur pragmatische Gründe, sondern ist auch sichtbares Resultat davon, dass Digitalisierung und Datenschutz in Baden-Württemberg zusammen gedacht werden, immer orientiert an den Bürger_innen als Zentrum der Arbeit einer obersten Landesbehörde. Die neue Dienstelle soll noch stärker als bisher Ausdruck dafür sein, dass sich der LfDI als Anlaufstelle für Bürger_innen und verantwortliche Stellen versteht und der Gesamtgesellschaft – ob Polizei, ob Schulen, ob Unternehmen oder jeder_m einzelnen Bürger_in – beratend zur Seite steht.

Ein wichtiger Baustein hierfür ist auch das Bildungszentrum BIDIB, das in den neuen Diensträumen nun auch die Möglichkeit hat, Präsenzveranstaltungen in eigens dafür vorgesehenen Schulungsräumen anzubieten. Um diese Botschaft nach außen zu tragen und die neuen Räumlichkeiten auch für die Öffentlichkeit zu öffnen, luden wir unter dem Motto „LfDI 2.0 – Freiheit geht voran!“ am 22. September 2021 zahlreiche Gäste ein aus der Landespolitik, aus den Datenschutzbehörden anderer Länder, Wegbegleiter_innen des Datenschutzes und der Informationsfreiheit sowie langjährige Kooperationspartner_innen, um einen Einblick in die Aktivitäten der Behörde zu geben.

Rund 120 Gäste folgten der Einladung und bekamen auf zwei Etagen in Kurzvorträgen der LfDI-Kolleg_innen, bei Informationsständen oder einer Musikdarbietung der Wiener Liedermacherin Flickentanz einen facettenreichen Eindruck, wie sich die Arbeit für Datenschutz und Informationsfreiheit gestaltet – inmitten der Lichtkunstkunst „Data to Light“ des Künstlers Florian Mehnert. Eröffnet wurde die Veranstaltung durch Grußworte der landespolitischen Fraktionen, des Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. und der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. Einen auch mahnenden Blick auf die Herausforderungen für den Datenschutz warfen hierbei Professor Niko Härting (Herausgeber der Zeitschrift PinG – Privacy in Germany) und die Sprecherin des Chaos Computer Clubs Constanze Kurz.

Wie viele Veranstaltungen im vergangenen Jahr war auch „LfDI 2.0: Freiheit geht voran!“ als öffentliche Veranstaltung geplant und wurde von der pandemischen Lage eingeholt. Daher musste auf den letzten Metern der Teilnehmehmendenkreis doch noch begrenzt werden. Doch ganz nach der Devise „aufgeschoben ist nicht aufgehoben“ wird bereits eine Wiederholung der Veranstaltung geplant: Bei der langen Nacht der Museen 2022 sollen die Türen des LfDI nun auch endlich für alle Interessierten geöffnet werden.

12.2 Speyerer Forum zur Digitalen Lebenswelt

Die Jubiläumsausgabe der jährlich stattfindenden Tagung stand am 21. und 22. April 2021 unter dem Motto „Von der Strategie zur Umsetzung“. In der seit vielen Jahren bestehenden Kooperation von uns mit der Deutschen Universität für Verwaltungswissenschaften Speyer und dem LfDI Rheinland-Pfalz wurde in diesem Jahr ein Blick nach vorne geworfen: Was kann und muss der Staat nun tun, um die Digitalisierung in Deutschland zu einer Erfolgsgeschichte zu machen? Im Besonderen durch den pandemiebedingten Digitalisierungsschub rückte die Frage danach, wie wir in digitalen Zeiten leben wollen und welche Rolle dabei die Verwaltung trägt, in den Fokus des Interesses. Als Ausgangspunkt für die Diskussion diente die Eröffnungsrede von Jan Philipp Albrecht (Minister für Energiewende, Landwirtschaft, Umwelt, Natur und Digitalisierung Schleswig-Holstein) zum Thema „Die DSGVO aus der heutigen Perspektive“.

Im Anschluss diskutierten Akteur_innen aus Wissenschaft, Politik, Datenschutz und Verwaltungspraxis über brandaktuelle Themen wie die Digitalisierung des Gesundheitswesens, Datenschutz und IT-Sicherheit in Zeiten von Home Office und die OZG-Umsetzung oder gingen der Frage nach, ob Proctoring als neuer Standard für eine gelingende Hochschullehre dienen kann oder was Umweltschutz in einer KI-getriebenen Lebenswelt bedeutet. Den Abschluss der Tagung bildete eine strategische Perspektive des

>> Mehr Informationen:

LfDI-Präsentationen der BvD Herbstkonferenz:
https://www.baden-wuerttemberg.datenschutz.de/jetzt-online-verfuegbar-praesentationen-der-bvd-herbstkonferenz-datenschutz-und-behoerdentag-2021/<

LfDI auf das Thema „Datenschutz und Digitalisierung“. Hierbei wurde deutlich, welche kulturpolitische Aufgabe die Digitalisierung darstellt, was das für das Selbstverständnis der Verwaltung bedeutet und dass der Datenschutz hierbei als Werkzeug dienen kann, eine bürger_innenzentrierte digitale Lebenswelt mitzugestalten.

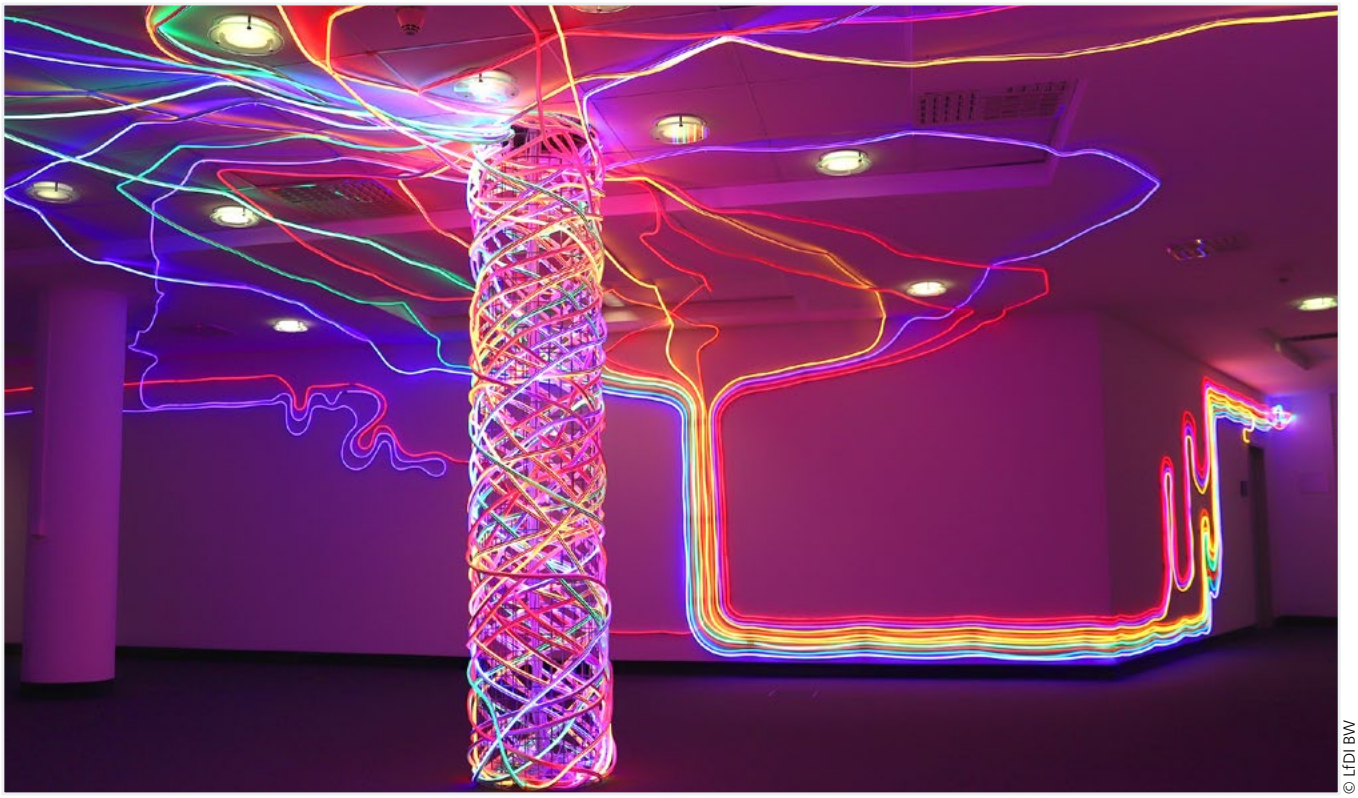
12.3 Herbstkonferenz

Im Oktober 2021 oblag uns ein weiteres Mal die Schirmherrschaft der Herbstkonferenz Datenschutz. Veranstalter dieser von unserer Behörde initiierten Fachtagung ist der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.. Die Schirmherrschaft teilen wir uns mit Michael Will, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht und Prof. Dr. Thomas Petri, bayrischer Landesbeauftragter für Datenschutz. Wie bereits in den vergangenen Jahren steht der Themenblock „Wirtschaft trifft Aufsicht“ an den ersten beiden Konferenztagen im Mittelpunkt. Der dritte Tag der Veranstaltung richtet sich gezielt an Vertreter_innen von Behörden und öffentlichen Verwaltungen. Um den häufig in diesem Bereich sehr speziellen Fragestellungen gerecht zu werden, werden die Fachvorträge und Diskussionen auf die Fragestellungen öffentlicher Verwaltungen spezifisch zugeschnitten.

Die Herbstkonferenz Datenschutz bietet Fachvorträge, Diskussionen, Expertengespräche, Handlungsleitfäden und Beispiele aus der Praxis für alle, die mit dem Thema Datenschutz befasst sind. Die Formate „Wirtschaft trifft Aufsicht“ und auch der Behördentag sind bundesweit einmalig. Wie bereits im vergangenen Jahr veröffentlichen wir die Präsentationen und Vorträge unserer Dienststelle im Nachgang zu der Herbstkonferenz.

13. Einblick in die Dienststelle

Die Dienststelle des Landesbeauftragten für den Datenschutz und die Informationsfreiheit wurde in den vergangenen Jahren vom Landtag mehrmals mit zusätzlichen Personalstellen ausgestattet. Im Jahr 2021 umfasste der Personalbestand 63,5 Stellen (zzgl. dem Landesbeauftragten selbst). Sieht man von der üblichen Personalfluktuation ab, waren alle Stellen besetzt. Das Onboarding, die Einarbeitung neuer Kolleg_innen in die Dienststelle in Zeiten von pandemiebedingter Telearbeit und eingeschränkten persönlichen Kontaktmöglichkeiten, stellt nach wie vor eine große Herausforderung dar und bildet auch einen der Schwerpunkte der Personalarbeit des vergangenen Jahres. Die Einbindung und Integration der Mitarbeitenden in die Abteilungen sowohl in fachlicher, als auch sozialer



Mit dem Umzug in die neuen Diensträume hat der Konzeptkünstler Florian Mehnert mit „Data to Light“ Kunst im Bau geschaffen.

Hinsicht, ist unerlässlich, stärkt den schnellen und niederschwelligen fachlichen Austausch untereinander und führt zu einem besseren Arbeitsklima.

Neuer Einzelplan im Staatshaushalt

Das Jahr 2021 sorgte auch mit Anpassungen im Finanzbereich der Dienststelle für große Herausforderungen.

Ab dem Jahr 2022 werden 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 Landesbeauftragten für den Datenschutz und die Informationsfreiheit von anderen Ressorts und Behörden des Landes Baden-Württemberg nun auch haushaltsrechtlich ab. Zur Vorbereitung dieser Änderung wurde der Haushalt 2022 erstellt, ins Buchungssystem eingegeben und zum Druck des Staatshaushaltplans mit sämtlichen Anlagen fertiggestellt. Diese Aufgaben wurden bisher in weiten Teilen von der Verwaltung des Landtags übernommen. Ich danke dem Landtag für seinen Entschluss, uns einen eigenen Haushaltsplan zuzuordnen, dem Ministerium der Finanzen für die engagierte Unterstützung dabei und der Landtagsverwaltung dafür, dass sie uns über viele Jahre hervorragend betreute. Daneben nimmt die Begleitung des „Restrukturierungsprojekts Baden-Württemberg („RePro BW"), welches eines der größten IT-Projekte des Landes Baden-Württemberg darstellt, mit welchem unter anderem das Haushaltsmanagement modernisiert wird, sehr viel Zeit des Sachgebiets „Finanzen, Reisestelle, Bücherei" in Anspruch.

13.1 Umzug in neue Diensträumlichkeiten

Nachdem das Jahr 2020 mit der Einführung von flächendeckender Telearbeit und den Anpassungen an die Pandemiesituation bereits große Herausforderungen und Veränderungen in der täglichen Arbeit mit sich brachte, konnte im Jahr 2021 zudem endlich ein Großprojekt abgeschlossen werden, welches uns viele Jahre begleitet hatte: Der Umzug in die neuen Diensträume.

Die Problematik wurde bereits in mehreren vergangenen Tätigkeitsberichten ausgeführt. Die Räume in der Königstraße 10a in Stuttgart waren aufgrund des Personalzuwachses der Dienststelle nicht mehr adäquat bemessen. Nach langer Suche konnte Vermögen und Bau Baden-Württemberg uns neue Räume in der Lautenschlagerstraße 20 in Stuttgart anbieten. Die unmittelbare Nähe zum Hauptbahnhof Stuttgart ist sowohl für die Mitarbeitenden, als auch für unsere Besucher_innen, die beispielsweise die Angebote des Bildungszentrums Datenschutz und Informationsfreiheit (BIDIB) des LfDI nutzen möchten, von großem Vorteil. Das BIDIB kann durch die neuen Räumlichkeiten und die beschaffte moderne Veranstaltungstechnik Veranstaltungen per Live-Übertragung, in hybrider Form und auch in Präsenz durchführen.

Der Umzug selbst beschäftigte die zuständige Abteilung 1 „Zentraler Service" und hierbei speziell das Sachgebiet „Organisation, IuK, Innerer Dienst" dieses Jahr in besonderem Maße. Dies begann zunächst bei der Planung und Begleitung der Sanierungsmaßnahmen und Ausstattung der neuen Räume. Weitere Planungen betrafen die Raumverteilung und die Nutzung der verschiedenen Lagerflächen, die Vorbereitung des Einbaus der korrekten IT-Infrastruktur (Serverräume, Datenleitungen für WLAN-Hotspots etc.), die Beschaffung von Mobiliar sowie Seminartechnik und natürlich die Abstimmungen mit der beauftragten Umzugsfirma. Auch die ständige Information der Belegschaft über die anstehenden Maßnahmen war für die Durchführung eines reibungslosen Umzugs notwendig.

Der Umzug selbst fand an drei Tagen im Juli 2021 statt und verlief – insbesondere dank der sehr guten Vorbereitungen und Mithilfe der Mitarbeitenden der Dienststelle und der Umzugsfirma – völlig reibungslos. Bereits am ersten Tag nach dem Umzug war die Dienststelle wieder voll arbeitsfähig. Im Anschluss mussten die alten Räume in der Königstraße 10a geräumt und in einen vertragsgemäßen Zustand versetzt werden, bevor die Übergabe an Vermögen und Bau durchgeführt werden konnte.

Ferner war die Einrichtung der neuen Räume naturgemäß mit dem Einzug noch nicht abgeschlossen. Beispielsweise mussten die Schließanlage korrekt programmiert, Rettungspläne aktualisiert, Lampen, Jalousien und Spülmaschinen repariert oder ersetzt,

Brandmelder installiert und viele weitere kleine Anpassungen umgesetzt werden. All diese „Kleinigkeiten“ wurden eine nach der anderen von den zuständigen Mitarbeitenden, neben den sonstigen laufenden Aufgaben, angegangen und erledigt.

Ausdrücklicher Dank gilt allen Kolleg_innen, die sich hier eingebracht und dieses Projekt, welches für die Arbeitsfähigkeit der Dienststelle und den Erfolg des BIDIB so wichtig war, zu einem vollen Erfolg gemacht haben.

13.2 Data to Light

Datenschutz und Informationsfreiheit sind für viele Menschen recht abstrakte Themen, die ihnen nur als störende Cookie-Banner, als Einwilligungen in seitenlangen Datenschutzerklärungen und als Anträge an gesichtslose Behörden begegnen. Dass es sich hier aber um Bürgerrechte handelt, die jeder_m mehr Selbstbestimmung und Transparenz in vielen Bereichen des Lebens verschaffen sollen, ist vielen fremd. Daher ist ein erklärtes Ziel von uns, Datenschutz und Informationsfreiheit für Bürger_innen erfahrbar, erlebbar und nun auch begehbar zu machen. Mit der Lichtkunstinstallation „Data to Light“ hat der Konzeptkünstler Florian Mehnert ein Kunstwerk in unseren neuen Räumen geschaffen, in dem Datenströme sichtbar gemacht werden und der/die Betrachter_in Teil des Kunstwerks – der Datenströme – wird. So wird auf eine ganz neue Art erlebbar, dass jede_r ein Teil der Digitalität ist, der selbst Datenströme generiert, die mit den Daten anderer Menschen zusammenfließen und einen gemeinsamen Datenstrom bilden, der sich weiter verbreitet. Inmitten dieser Datenströme arbeiten die Mitarbeitenden unserer Dienststelle, um diese zu schützen und Freiheit zu sichern. Über zwei Etagen, nahezu 3 km und über 700 qm erstrecken sich die Lichtstränge durch die Flure und sorgen für eine besondere Stimmung, die den/die Betrachter_in direkt in ihren Bann ziehen und einen Impuls zur Auseinandersetzung und Diskussion setzen.

„Data to Light“ bildet damit eine Weiterführung der schon seit einigen Jahren andauernden Beschäftigung des Künstlers mit dem Thema Datenschutz als gesellschaftliche Herausforderung und individuelle Verantwortung. Das Kunstwerk stellt eine weitere

„Data to Light“ vom Konzeptkünsler Florian Mehnert.

Arbeit zur Visualisierung von Datenströmen dar, die sich direkt aus der App Freiheit 2.0 entwickelt und auf diese rückbezieht. „Data to Light" ist das dritte Großprojekt, nach „Social Distance Stacks 2021" und „Freiheit 2.0", bei dem der LfDI zum Kunstwerk Florian Mehnerts beitragen konnte und mit dieser Vermittlungsform einen neuen Zugang zum gesellschaftlichen Diskurs um Datenschutz anbietet. Sobald es wieder möglich ist, wird der LfDI regelmäßig Gelegenheit geben, dass Interessierte das Kunstwerk vor Ort erleben können.

13.3 Neuorganisation der Dienststelle

Die wachsende Zahl an Mitarbeitenden in unserer Dienststelle führte des Weiteren dazu, dass in den Abteilungen 1 und 2 der Dienststelle mit der Einführung von Sachgebieten eine neue Ebene in die Struktur eingezogen wurde. So können fachliche Bereiche auch organisatorisch zusammengeführt, Ergebnisse kanalisiert und eine schnellere Aufgabenerledigung ermöglicht werden. Außerdem kann die Übernahme einer Sachgebietsleitung einen Anreiz für die Belegschaft darstellen, sodass der Einführung auch Elemente der Personalentwicklung zukommen.

Dienstvereinbarung mobiles Arbeiten

Es zeigt sich, dass die Corona-Pandemie der Auslöser eines tiefgreifenden und nachhaltigen Kulturwandels in der Arbeitswelt ist. Zuvor war Homeoffice auch in unserer der Dienststelle zwar verbreitet, aber nicht die Regel; dass alle Mitarbeitenden pauschal und flächendeckend von zu Hause aus arbeiten, war undenkbar. Nach dem für die allermeisten erzwungenen „Wechsel" ins Homeoffice mit dem Lockdown im Frühjahr 2020 hat die große Mehrheit in der vergangenen Zeit aber überwiegend positive Erfahrungen gemacht. Die Corona-Krise hat gezeigt, dass flexibles Arbeiten die Qualität der Arbeitsergebnisse nicht schmälert – im Gegenteil.

Im Jahr 2021 wurden mit dem Personalrat zunächst Eckpunkte für eine Dienstvereinbarung zum Mobilen Arbeiten festgelegt, im Anschluss die konkrete Vereinbarung verhandelt, welche im November unterzeichnet werden konnte. Diese neue Dienstvereinbarung „Mobiles Arbeiten" löst die bisherige Dienstvereinbarung Telearbeit ab. Mit der Einführung des mobilen Arbeitens soll insbesondere die berufliche Tätigkeit und die persönliche Lebenssituation der Mitarbeitenden besser in Einklang gebracht werden können, die Motivation, die Leistungsbereitschaft und die Bindung aller Mitarbeitenden an die Dienststelle gestärkt, das Arbeitsklima durch eine modernere Gestaltung der Arbeitsbedingungen weiter verbessert werden sowie die Ergebnisorientierung und Selbstverantwortung bei der Gestaltung und Durchführung der Arbeit weiter in den Vordergrund rücken.

Technische Migration zur BITBW

Die Dienststelle wird zukünftig Infrastrukturdienstleistungen von der zentralen IT-Dienstleisterin des Landes Baden-Württemberg, der BITBW, beziehen. Durch die Partizipation an der zentralen IT-Landschaft der Landesverwaltung können technische Vorgänge sowie Ausstattungen standardisiert und Doppelstrukturen vermieden werden. Außerdem werden dadurch die gesetzlichen Vorgaben des Errichtungsgesetz BITBW (BITBWG) erfüllt.

2021 konnten wir mit der Migration beginnen und etwa den Umzug sämtlicher Exchange-Postfächer bereits Anfang des Jahres erfolgreich durchführen. Der Plan, die vollständige Migration der IT-Infrastruktur bis Ende 2021 abzuschließen, konnte insbesondere auch auf Grund von Lieferengpässen bei der Hardware leider nicht vollumfänglich gehalten werden. In laufender, enger Abstimmung mit der BITBW sehen die Planungen nun vor, dass die Migration im Wesentlichen im 1. Quartal 2022 abgeschlossen sein wird. Dies ist Voraussetzung für den Start des Projekts „Einführung der E-Akte", welcher im unmittelbaren Anschluss erfolgen soll.

Die elektronische Personalakte des Landes wurde bereits zum 1. Mai 2021 in der Dienststelle eingeführt. Durch die elektronische Aktenführung wird sowohl das mobile Arbeiten als auch das Arbeiten in der Dienststelle, insbesondere für das Sachgebiet Personal, stark vereinfacht.

Online-Zugangsgesetz

Das Online-Zugangsgesetz verpflichtet Behörden, den Bürger_innen einen elektronischen Zugang zu den jeweiligen Verwaltungsleistungen zu ermöglichen. Wir haben dies für die Datenschutzbeschwerde, die Datenpannen-Meldung und die Meldung der Datenschutzbeauftragten bereits umgesetzt.

Bereits seit längerer Zeit sind die Einreichung einer Beschwerde, einer Meldung über die Verletzung des Schutzes personenbezogener Daten („Datenpannen-Meldung“) und die Meldung eines oder einer Datenschutzbeauftragten einer verantwortlichen Stelle auch über ein elektronisches Meldeformular auf unserer Homepage möglich. Das (bisher durch uns selbst angebotene) Beschwerdeformular wurde nun durch ein moderneres Formular auf www.service-bw.de ersetzt. Dies ermöglicht die konsolidierte Nutzung des landesweiten Systems für Verwaltungsleistungen.

Inhouse-Schulungen

Um weiterhin in die wichtigste Ressource der Dienststelle – die Mitarbeitenden – zu investieren, haben wir neben einer Vielzahl von externen Fortbildungen auch eine ganze Reihe von Inhouse-Schulungen angeboten. Die Stabsstelle Europa organisierte hierzu regelmäßig einstündige Fortbildungen zu üblicherweise datenschutzrechtlichen Themen oder Fragestellungen. Das Sachgebiet Personal organisierte des Weiteren Veranstaltungen mit externen Referenten wie etwa zum Vergaberecht und möchte diese Angebote im nächsten Jahr noch ausweiten.

Gesundheitstag von Beschäftigten für Beschäftigte

Eine besondere Aktion stellten die „Gesundheitstage“ im Oktober dar. Hervorzuheben ist, dass diese „von der Belegschaft für die Belegschaft“ organisiert wurden. Die verschiedenen Angebote, wie etwa das Live-Kochen eines gesunden Mittagessens, Sportkurse und Vorträge zu Resilienz und gesunder Ernährung, stießen in der Belegschaft auf großes Interesse und gaben wichtige Impulse.

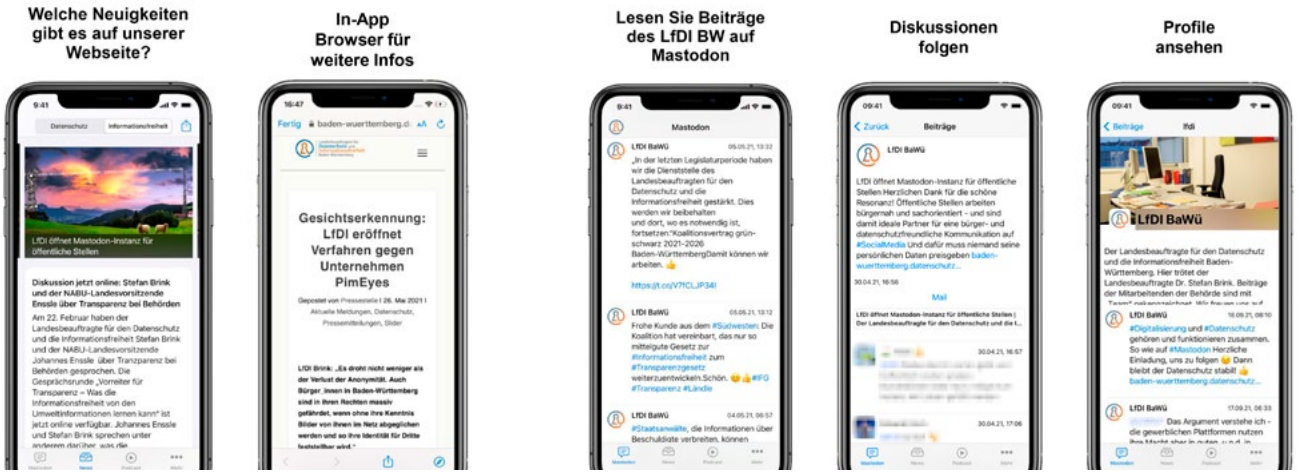
Ausbildung und Hospitationen

Um auch Studierenden die Möglichkeit zu geben, Einblicke in das Datenschutzrecht und das Arbeiten in der Dienststelle zu geben, wurden im vergangenen Jahr insgesamt sechs Referendar_innen im Rahmen ihres juristischen Vorbereitungsdiensts, fünf Praktikant_innen sowie ein Hospitant in der Dienststelle betreut. Von diesen Tätigkeiten profitieren beide Seiten, da nicht nur Wissen vermittelt und die Dienststelle tatkräftig unterstützt werden kann, sondern zugleich Berufsanfänger_innen frühzeitig für datenschutzrechtliche Gesichtspunkte sensibilisiert werden, welche sie wiederum bei späteren beruflichen Stationen einbringen können. Gleichzeitig handelt es sich um eine Maßnahme der Personalgewinnung. Insbesondere im Bereich der Hospitationen sind Personen aus der Landesverwaltung und darüber hinaus gerne eingeladen, mit uns Kontakt aufzunehmen.

13.4 Digitale und direkte Kommunikation

LfDI-App

Im September 2021 wurde die LfDI-App für iPhone veröffentlicht. Eine Veröffentlichung der Android-App ist derzeit in Planung für Anfang 2022. Ziele sind eine direkte Kommunikation trotz „Twit-



© LfDI BW

ter-Abschied", einen leichteren Zugriff auf Informationen der Behörde zu erreichen und im Rahmen der Digitalisierung ein digitales Produkt der Verwaltung für den Kontakt mit Bürger_innen anzubieten. Der Mastodon Bereich in der App ermöglicht, Beiträge der Behörde zu lesen und Inhalte von Diskussionen anzusehen. Im Bereich News werden Neuigkeiten aus Datenschutz und Informationsfreiheit von unserer Webseite angeboten. Unseren Podcast „Datenfreiheit!" kann im Podcast-Bereich heruntergeladen und offline angehört werden, wozu zukünftig auch Kapitelmarken gehören.

Bei der In-House Entwicklung der nativen App haben wir uns im Rahmen von „data protection by design" darüber Gedanken gemacht (z. B. hinsichtlich Rechtmäßigkeit, Transparenz, Datenminimierung, Sicherheit der Verarbeitung), 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 (z. B. Urheberrecht).

Wir möchten die Vorzüge der digitalen Welt unbedingt fördern. Um diese Vorzüge tatsächlich aber nutzen zu können, müssen Bürger_innen darauf vertrauen können, dass sie ihre bürgerliche Freiheit auch in der digitalen Welt nutzen und davon ausgehen können, dass ihre Daten nicht von Anbietern für ihnen unbekannte Zwecke genutzt werden. Digitalisierung und Datenschutz gehörden und funktionieren nur zusammen. Wenn im Netz die Bürgerrechte nicht gewahrt werden, werden die Menschen über kurz oder lang das Vertrauen ins Netz verlieren. Sie werden auch das Vertrauen in rechtsstaatliche Prinzipien verlieren, wenn sie davon ausgehen müssen, dass der Staat nicht in der Lage ist, ihr freiheitliches Recht – nähmlich sich als Bürger_in entfalten zu können ohne sich preisgeben zu müssen – zu wahren. Anders formuliert: Wenn Bürger_innen im Netz nicht mehr Bürger_innen sind, wozu braucht er in einer Welt, die digital ist, einen Rechtsstaat, der ihn nicht respektiert?

Als Datenschützer sind wir Ermöglicher von digitalen Techniken, die nützlich sind für die Bürger_innen. Wir respektieren ihren Willen, mit ihren Daten so umzugehen, wie sie es möchten. Die DS-GVO ist hier sehr klar: Sie untersagt nicht, dass Daten

>> Mehr Informationen:

LfDI-App im Apple-Store: App-Store-Seite https://apps.apple.com/de/app/lfdi-bw/id1566528364 <<

verarbeitet werden, sie regelt, wie sie verarbeitet werden. Die zentralen Akteur_innen bei diesen Regelungen sind die Bürger_innen. Sie stehen im Zentrum. Unternehmen dürfen Daten verarbeiten, aber nach bestimmten Regeln. Diese beinhalten zum Beispiel auch, dass Bürger_innen in der Lage sein sollten, eine informierte Entscheidung zu treffen, wem sie wofür ihre persönlichen Daten geben möchten. Und sie müssen auch in der Lage sein, ihre Meinung zu ändern und zu sagen: „So, jetzt bitte löscht meine Daten!". Und wenn sie erklärt haben möchten, wofür ihre Daten verarbeitet und mit wem die Daten geteilt werden, dann muss das Unternehmen oder die öffentliche Stelle liefern.

Die DS-GVO schafft damit kein Privileg für europäische Bürger_innen. Die Datenschutz-Grundverordnung überführt die bereits bestehenden europäischen Werte und Bürgerrechte ins Digitale und damit in eine neue kulturelle Praxis. Digitalisierung als kulturelle Praxis müssen wir gemeinschaftlich aber weiter einüben. Die ökonomische Verwertung der Digitaliserung ist uns voraus. Diese nun in die europäische Idee einzuhegen und wertebasiert zu bewerten, ist Teil unserer Aufgabe, die wir seit 2018, seit dem die DS-GVO gilt, gewissenhaft wahrnehmen.

Videoreihe „B.sucht Freiheit"

Wir sind die Adresse der Freiheit. Wir suchen von hier aus das Gespräch, den Streit und den interdisziplinären Austausch mit Persönlichkeiten und Organisationen, die sich intensiv mit Datenschutz- und Fragen der Informationsfreiheit beschäftigt haben. Dies tun wir in Veranstaltungen, auf denen wir zu Gast sind. Wir organisieren mit unserem Bildungszentrum selbst zahlreiche Events. Wir gehen Kooperationen ein, produzieren eigene Podcasts und seit dem Herbst auch die eigene Videoreihe „B.sucht Freiheit". Zum Auftakt der neuen Videoreihe sprachen wir mit Bundesinnenminister a.D. und Bürgerrechtler Gerhart Baum. Es ist ein tolles Gespräch über die Freiheit geworden. Wir haben zudem mit dem Soziologen Harald Welzer, dem

Journalisten und Kolumnisten Jan Fleischhauer, den Gründern von Digitalcourage e.V. padeluun und Rena Tangens gesprochen. Alle Videos stehen auf unserer Homepage.

Auch suchen wir das direkte Gespräch mit den Bürger_innen. Dafür nutzen wir auch die datenschutzfreundliche Twitter-Alternative Mastodon. Mittlerweile folgen uns über 1600 Interessierte auf Mastodon, was sehr erfreulich ist. Ebenfalls erfreulich ist, dass zahlreiche öffentliche Stellen auf unserem Server einen eigenen Account eingerichtet haben und jetzt datenschutzfreundlich kommunizieren. Obwohl sich immer mehr Menschen auf Mastodon tummeln, sind es im Verhältnis weniger als bei den großen wirtschaftlich organisierten US-Amerikanischen Unternehmen. 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. Mastodon ist dafür eine gute Option. 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 wir dort bald unsere Videos online. Diese sind dann für Interessierte, die sich in Sozialen Netzwerken bewegen, sehr leicht zugänglich. Wir sind Fans der Digitalisierung. Wir haben hausintern die Apple-Version unserer LfDI-App entwickelt. Wir betreiben eigene Server, um digital und direkt mit Bürger_innen zu kommunizieren. Das alles klappt, weil wir Kolleg_innen haben, die sich technisch sehr gut auskennen, viel von Digitalisierung verstehen und Lust haben, zu zeigen, dass Digitalisierung und Datenschutz wunderbar zusammenpassen. Wenn wir das können – warum sollten Ministerien, Städte und Kommunen sowie Universitäten das nicht können? Das Wissen haben alle. Wo nötig und gewünscht, beraten wir mit unseren Fachleuten öffentliche Stellen natürlich sehr gerne, wie sie Bürger_innen auch in der digitalen Welt niederschwellig und fair ansprechen können.

13.5 Dienst für die Bürgerschaft

Als unabhängige Aufsichtsbehörde gehört es zu unserer Kernaufgabe, uns in öffentliche Debatten um die Freiheit einzubringen. Das ist in der DS-GVO sogar festgeschrieben. Wir leisten hier unseren Beitrag. Zudem haben wir im vergangenen Jahr wieder sehr viele Beschwerden erhalten und so viele Datenpannenmeldungen wie noch nie verzeichnet. Insbesondere die Microsoft-Exchange Lücke im Frühjahr 2021

© LfDI BW

Zum Auftakt der neuen Videoreihe „B.sucht Freiheit“ sprach Stefan Brink mit Gerhart Baum.

und die log4j-Lücke zeigten auf, wie wichtig IT-Sicherheit und Datenschutz sind. Diese Lücken führten zu zahlreichen Datenpannen-Meldungen bei uns.

Wir verzeichneten weniger Beratungsanfragen direkt an unsere Dienststelle. Zugleich sehen wir, dass die Nachfrage nach unseren Handreichungen, die wir online zum download anbieten, sehr groß ist. Unsere Hinweise etwa zum Schrems-II-Urteil, zur Lohnforzahlung im Krankheitsfall, zu 3G am Arbeitsplatz, zu Videokonfrenzsystemen, zu online-Prüfungen an Hochschulen interessierten zehntausende Menschen. Sie greifen wichtige aktuelle Fragenstellungen auf und bieten substanzielle Unterstützung. Besonders erfreulich ist: Unser Bildungszentrum wird hervorragend angenommen. Es zeigt sich, dass wir hier auf dem richtigen Weg sind. Das Parlament hat dankenswerterweise das in dieser Form bundesweit einzigartige Bildungszentrum ermöglicht. Es ist ein voller Erfolg. Wir können mit unserem Angebot des Bildungszentrums nun sehr viel umfassender und präsizier informieren und etwa Schulen sowie andere öffentliche Stellen, Unternehmen, Vereine und Initiativen beraten und ihnen aktiv und konkret helfen.

Das Bildungszentrum gibt es erst seit Mitte 2020. Dass es in dieser kurzen Zeit schon so konsequent genutzt wird, erfreut uns sehr. Allein im Jahr 2021 haben sich über 2000 Interessierte zu 50 Veranstaltungen angemeldet, von denen zahlreiche sehr fachspezifisch – etwa für die Polizei oder Kommunen – waren. Wir achten im Bildungszentrum neben guter Programmplanung auch darauf, dass wir ein sehr gutes digitales Angebot bereitstellen. Hybridveranstaltungen wird es künftig häufiger geben. Auch im Jahr 2022 führen wir konsequent unseren Beratungsansatz fort.

Statistische Übersicht – Zeitraum jeweils vom 01.01. – 31.12.

	2016	2017	2018	2019	2020	2021
Beschwerden	2.048	3.058	3.902	3.757	4.782	4.708
Kontrollen	16	55	13	111	31	10
Beratungen[1]	1.515	1.786	4.440	3.842	3.285	2.206
Anmeldungen Bildungs- und Beratungszentrum BIDIB					785	2.016
Datenpannen	68	121	900	2.030	2.321	3.136
Bußgeldverfahren (eingeleitet)	-	-	138[2]	233	174	136

1 ohne telefonische Beratung
2 Mai – Dez

NOTIZEN

Der Landesbeauftragte für
Datenschutz und
Informationsfreiheit
Baden-Württemberg