Unsere Daten:
Daten nützen – Daten schützen

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Tätigkeitsbericht
Datenschutz 2020

Herausgegeben vom Landesbeauftragten für den Datenschutz und die Informationsfreiheit Dr. Stefan Brink
Königstraße 10a, 70173 Stuttgart
Telefon 0711/615541-0
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: www.milla-grafikdesign.de

Dezember 2020
Veröffentlicht als Landtags-Drucksache 16/9850

36. Datenschutz-Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg 2020

Inhaltsverzeichnis

Vorwort **5**

1 **Datenschutz in der Corona-Krise** **9**

1.1 Beteiligung an den Regelungen der Landesregierung zur Bewältigung der Corona-Krise 9

1.2 Die Verarbeitung von Besucher-Daten zur Kontaktnachverfolgung durch die Gesundheitsbehörden nach den Corona-Verordnungen 10

1.3 Datenverarbeitung zur Corona-Bekämpfung 12
- „Batman war hier“ 12
- „Hilfssheriffs“ der Behörden? 14
- Dokumentationspflichten im Verein 15
- Zugang zum Rathaus nur gegen Daten 16
- Befreiung von der Maskenpflicht: „Nicht ohne meinen Arzt“ 17

1.4 Die Polizei in der Corona-Krise 20
- Der übereifrige Beamte 20
- Polizei und SARS-CoV-2 oder: Schau mal, der Zeppelin! 21
- Die Corona-Verordnungen „Datenverarbeitung“ und „Datenverarbeitung im Auftrag“ 22

1.5 Datenschutz bei Corona-Testzentren 24

1.6 Die Digitalisierung des (öffentlichen) Gesundheitswesens zur Pandemiebekämpfung 27
- Die Datenplattform der Björn-Steiger-Stiftung – digitale Ablösung der analogen Arbeit der Gesundheitsämter in der Corona-Pandemie? 27
- Die Software SORMAS des Helmholtz-Instituts zur Kontaktnachverfolgung 29
- Die Überarbeitung der Software survnet@rki des Robert-Koch-Instituts zur Verbesserung der Kontaktnachverfolgungsfunktion 30

1.7 Fernunterricht an Schulen während der Corona-Krise 32
- Rechtliche Rahmenbedingungen und Empfehlungen für Videokonferenzen im Unterricht 33

1.8 Fragen an den betrieblichen Datenschutz 36
- Urlaubsrückkehr aus Risikogebieten 36
- Beratung und Unterstützung bei datenschutzkonformem Pandemieschutz 36
- Homeoffice – Datenschutzkonformer Umgang am Heimarbeitsplatz 36
- Fiebermessen am Werkstor? 38
- Sonderfall: Schlachtbetriebe 38

1.9 Datenschutzfreundliche Kommunikationsdienste und Videokonferenzen 38
- Praktische Tipps 40

1.10 Konfliktgebiet „Corona-Warn-App“ 42

2 **Das Schrems II – Urteil: ein Paukenschlag** **47**

3 **Eine Bildungsplattform für Schulen** **51**

4 **Der europäische Blick** **53**
- Gemeinsame Verantwortlichkeit und Auftragsverarbeitung 53
- Europäische Gremienarbeit 54
- Grenzüberschreitende Verwaltungsverfahren 55
- Schulungen 55

5 **Prüfung von Tracking auf Medien-Webseiten** **57**

6 **Aktuelles aus der Bußgeldstelle** **61**
- AOK – heilende Wirkung eines Bußgeldes für eine Krankenkasse 61
- Herausforderung Videoüberwachung 62

7 **Exit – Abschied vom Vereinigten Königreich und Twitter** **65**
- Brexit – Folgen für den Transfer personenbezogener Daten 65
- Twexit – Der Ausstieg aus Twitter 67

8 **Bildungszentrum** **71**

9 **Datenschutz als KULTuraufgabe** **73**
- Datenschutz so ganz anders 73
- Herbstkonferenz Datenschutz 74
- Spotlights 74
- Alice lost in Cyberland 75
- Datenschutz geht zur Schule 76
- Kooperation mit der Dualen Hochschule Baden-Württemberg 76
- Datenschutz kinderleicht 77
- „Ach wie gut, dass niemand weiß …“ 77
- Online-Tagung mit der HdM Stuttgart: „Daten schützen – Kinder schützen.“ 77
- Social Distance Stacks 79

10 **Datenschutz-Vielfalt, veranschaulicht von Fall zu Fall** **81**

10.1 Neues aus dem Amt I: Innere Sicherheit, Justiz, Kommunalwesen 81
- Auskunft durch den Verfassungsschutz 81
- Was lange währt, wird endlich gut? – Licht und Schatten beim neuen Polizeigesetz 84
- Ist eine private Stelle verpflichtet, der Polizei Auskünfte zu erteilen? 86
- Die Revanche 87
- Das Führungszeugnis 88
- Die „Liste der Auffälligen“ – Fortsetzung folgte 90
- Der Gutachterausschuss 92
- Ja, sind wir denn in China? 93

10.2 Neues aus dem Amt II: Gesundheits-, Sozial-und Bildungswesen 94
- Die Auskunft im Sozialdatenschutz 94
- Masernschutzgesetz in Kindertageseinrichtungen und Schulen 96
- Bewertungsportale im Internet: Wenn mir deine Bewertung nicht passt, gebe ich deine Identität preis! 98
- Rechtsanwälte: Namensnennung auf Biegen und Brechen 98

10.3 Neues aus dem Amt III: Datenschutz in der Privatwirtschaft 100
- Auskunft heißt Auskunft – so konkret wie möglich 100
- Anforderungen an die Benachrichtigung der Betroffenen bei einer Datenpanne 101
- Datenschutz in der Kreditwirtschaft: Fehlüberweisung mit Folgefehler 102
- Ausführung von Überweisungsaufträgen ohne Kontonummer 103
- Nicht ohne den Veranlasser: Werbender und Adresshändler sind regelmäßig gemeinsam Verantwortliche 104
- Weitergabe von Schuldnerdaten an Auskunfteien 105
- Künstliche Intelligenz im Personalwesen 106
- Löschfristen im Betriebs- und Personalratsbüro 107

10.4 Neues aus dem Amt IV: Alles mit V – Videoüberwachung, Verkehr, Vereine 107
- Neue Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ 107
- Videoüberwachung in Gaststätten gibt Anlass für Vor-Ort-Kontrollen 108
- „Mein Auto sieht Dich!“ – Tesla & Co 108
- „Parkraumüberwachung“ 110
- Der Parkausweis für Menschen mit Behinderungen 111
- „Reisefieber“ in pandemischen Zeiten? 112
- Vereine I: Zuschauer-Datenerhebung 114
- Vereine II: Selbsterhebungs-Fragebögen bei der Tieradoption 115
- Vereine III: Veröffentlichungen von Fotos eines Vereinsmitglieds 115
- Vereine IV: Der Gewinner als Verlierer – die Veröffentlichung von Spenden-Daten 116

11 Einblick in die Dienststelle 119
- Auswirkungen der Corona-Pandemie auf den Behördenbetrieb 119
- Besetzung der Neustellen 120
- Vorbereitung Umzug 120
- Mobiles Arbeiten 121
- Zahlenüberblick 121

Vorwort

© Kristina Schäfer

Dr. Stefan Brink

Die Pandemie, ausgelöst durch das Coronavirus SARS-CoV-2, hat das Jahr 2020 maßgeblich bestimmt. Für den notwendigen Schutz der Gesundheit wurden nicht selten persönliche Freiheiten der Bürger_innen eingeschränkt. Zu Recht diskutierten wir alle im Zuge dessen sehr intensiv darüber, ob und wie jeder Eingriff in die persönlichen Rechte zu rechtfertigen ist. Im Zweifel mussten Gerichte für Klarheit sorgen. Viele Grundrechte haben unter der Pandemie gelitten: Die Berufsfreiheit, die Reisefreiheit, die Versammlungsfreiheit und auch unser Grundrecht auf informationelle Selbstbestimmung, der Datenschutz. Alle Grundrechtseinschränkungen verfolgten ein hohes Schutzziel unserer Verfassung, das Recht auf Leben und körperliche Unversehrtheit.

Der Datenschutz als Grundrecht nimmt in der Pandemie eine herausgehobene Rolle ein. Durch den Druck zur digitalen Umstellung in vielen Lebensbereichen sind immer wieder Fragen aufgetaucht, die zwar drängend, doch aber bereits vor der Pandemie virulent waren. Mit der Pandemie musste die digitale Umstellung unter verschärften Bedingungen erfolgen. Behörden und Unternehmen bedienten sich oftmals Techniken, die nicht datenschutzkonform waren oder wollten Entscheidungen vollziehen, die in die Schutzrechte der Bürgerschaft unverhältnismäßig eingreifen sollten. Wir haben interveniert und beraten, geholfen und wo der Eingriff absolut inakzeptabel war, auch unterbunden.

Digitalisierung und Datenschutz gehören zusammen. Wir unterstützen die digitale Transformation. Wir zeigen auf, wie diese Transformation datenschutzkonform gelingen kann. Dass Bürger_innen, so wie es die Datenschutz-Grundverordnung (DS-GVO) vorsieht, selbst entscheiden, was mit ihren Daten passiert, wird umso bedeutsamer, je mehr wir uns in die digitale Welt hineinbegeben. Datenschutz ist nicht bürokratischer Nachteil, sondern ein echter Standortvorteil im Wettbewerb. Und die DS-GVO gibt uns den passenden Rechtsrahmen dafür.

Jede Krise gilt als „Zeit der Exekutive", so auch die Corona-Krise. Im Zuge immer neuer Verordnungen unserer Landesregierung wurde der Datenschutz nicht (mehr) übergangen oder verleugnet. Das ist sehr erfreulich. Aber er ist Anfeindungen ausgesetzt. Es wurde behauptet, dass der Datenschutz Schuld sei an der fehlenden Effektivität der Corona Warn-App. Auch hieß es, der Datenschutz sei bei Videokonferenzsystemen nicht so wichtig – Hauptsache, die Technik läuft. Es wurde gar angekündigt, den Datenschutz zurückschneiden zu wollen. Grundsätzlich ist klar: Wir müssen möglichst bald an den Punkt gelangen, wo alle Grundrechteeinschränkungen wieder aufgehoben werden können. Nach den temporären Einschränkungen dann den vermeintlich sperrigen, unliebsamen Datenschutz zu kappen, wäre fatal. Die informationelle Selbstbestimmung der Bürger_innen sollte nicht beschnitten, sie sollte weiter gestärkt werden.

Gerade der Einsatz von audio-visuellen Techniken, insbesondere die vermehrte Nutzung von Videokameras in Zusammenhang mit der Corona-Pandemie zum Beispiel bei Videokonferenzen stellt hohe Anforderungen an alle Verantwortlichen. Wir erkennen seit Jahren insgesamt eine intensivere Nutzung von Videotechniken auch in anderen Zusammenhängen – auf öffentlichen Plätzen, im Wald, in Restaurants, in Autos. Wir werden weiterhin darauf hinwirken, dass der Technikeinsatz datenschutzkonform erfolgt.

Wir haben in diesem Jahr mehr Beschwerden aus dem öffentlichen Bereich erhalten. Auch wurden zahlreiche Beratungen aus dem öffentlichen Bereich bei uns angefragt. Zu den Corona-Verordnungen haben wir ausführliche Stellungnahmen verfasst, oftmals unter enormen Zeitdruck, ähnlich wie ihn sicherlich auch andere Dienststellen verspürt haben.

Die Corona-Verordnungen hatten zur Folge, dass eine Vielzahl von personenbezogenen Daten gesammelt wurde. Behörden wollten wissen, welche Daten sie wie verarbeiten können, Gastronomen wollten wissen, wie sie Daten richtig verwahren und wem sie diese Daten übermitteln dürfen und müssen. Manchmal mussten wir für Klarheit sorgen, zum Beispiel, als die Polizei auf solche Daten zugreifen wollte – und dies auch unter bestimmten Voraussetzungen durchaus durfte.

Die Beratung des Kultusministeriums im Zuge der möglichen Einführung einer Bildungsplattform hat enorme Kapazitäten bei uns im Haus gebunden. Daten von Schüler_innen sind hoch sensibel. Schulen, Lehrende, Eltern und Schülerschaft haben einen Anspruch auf eine qualitativ hochwertige Bildungsplattform, die den Datenschutz ernst nimmt und umsetzt. Wir sind aktuell inmitten des Pilotprojektes und überprüfen in der Praxis, ob die gemachten Zusagen des Anbieters Microsoft eingehalten werden.

Gerade unser Beratungserfolg bei Microsoft ist positiv zu werten. Wir haben in den Verhandlungen mit dem Unternehmen darauf gedrungen, dass es den Nutzer_innen zusätzliche Garantien gibt. Mit Blick auf die europäische Rechtsprechung herrscht große Unsicherheit, ob ein US-Anbieter überhaupt personenbezogene Daten in die USA übertragen darf. Microsoft hat deshalb verbindlich zusätzliche Sicherheitsgarantien ausgesprochen und europäische Standards übernommen. Im privaten Sektor ist dies ein Erfolg für den Datenschutz. Weitere Unternehmen werden dem sicher folgen. Es zeigt sich: Wer in Europa Geschäfte machen möchte, der muss europäische Standards erfüllen. Die DS-GVO ist ein Standortfaktor geworden.

Wir haben in diesem Jahr im privaten Bereich nicht sehr viele Kontrollen durchgeführt. Unsere Kontrolle der AOK Baden-Württemberg hingegen hat große Beachtung gefunden, weil das darauffolgende Bußgeld verhältnismäßig hoch ausgefallen ist. Wir haben festgestellte Verstöße angemessen bewertet und mit der AOK auch eine sehr gute Lösung gefunden. Insgesamt haben wir im vergangenen Jahr 174 Bußgeldverfahren durchgeführt. Es macht wenig Freude, Bußgelder zu verhängen, manchmal ist dies aber notwendig. Die DS-GVO ist kein „nice to have“. Sie ist auch kein Papiertiger. Sie ist elementares Recht, das es einzuhalten und umzusetzen gilt.

Wir nehmen in Baden-Württemberg den Datenschutz ernst. Seit dem Juli 2020 können wir zudem sagen, dass wir bundesweit die erste Landesbehörde sind, die ein eigenes Bildungszentrum für Datenschutz und Informationsfreiheit (BIDIB) betreibt. Es ist dem Parlament zu verdanken, dass wir die Mittel dafür bereitgestellt bekamen, um konsequent und mit breiter Wirkung beraten zu können. Wir mussten zunächst das Personal für das Bildungszentrum gewinnen, dann sind wir in die Programmplanung eingestiegen und schließlich haben wir die ersten Veranstaltungen konzipiert. Hier hat uns dann auch die Corona-Pandemie getroffen, geplante Präsenzveranstaltungen mussten wir leider absagen. Wir haben unser Angebot jedoch anpasst und noch stärker auf digitale Angebote gesetzt. Deswegen lief auch der Startschuss fürs BIDIB – mit breiter Unterstützung der Fraktionen des Landtags in Form von Videobotschaften – prima. Die gute Nachricht: Unser BIDIB kann Online-Schulungen. Und: Alle bisherigen online-Veranstaltungen waren binnen kurzer Zeit ausgebucht. Die weitere Ausgestaltung des Bildungszentrums haben wir zunächst zurückgestellt, weil geplant war, zum Herbst dieses Jahres mit der Behörde umzuziehen. Das heißt, vieles lief noch „handgestrickt“. Mit dem nun anstehenden Umzug im Frühjahr werden wir das Bildungszentrum jetzt auch technisch so ausstatten, dass Fortbildungen, Schulungen, Vorträge, Diskussionen und Fachgespräche analog und digital konsequent und qualitativ gut möglich sind. Wir nehmen 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 ist ein ausgezeichneter Ort für die Beratung, Vermittlung, Schulung und Qualifizierung.

Der Datenschutz und die Informationsfreiheit sind moderne Bürgerrechte. Der Umgang mit den eigenen personenbezogenen Daten ist in der digitalen Zeit ein alltägliches Phänomen, es ist zu einer eigenen Kulturtechnik geworden. Wir sehen diese Kulturtechnik in der digitalen Welt noch als eine sehr junge Form der Alltagspraxis. Nach wie vor. Auch wenn es bereits die ersten Generationen gibt, die von Kindesbeinen an mit dem Smartphone umgehen. Auch der Kulturbetrieb und die Kunst blicken intensiver auf Themen der Digitalisierung, der Auswirkungen von technologischer Entwicklung auf den Menschen und auf das Verhältnis von menschlicher und maschineller Intelligenz. Wir sind für Künstler_innen verlässlicher Ansprechpartner

und diskutieren mit ihnen, beraten und unterstützen sie, wo wir können.

Die Verwertung von personenbezogenen Daten ist eine ökonomische Technik. Diese hat sich schneller entwickelt als die Kulturtechnik. Das Internet ist kein rechtsfreier Raum und das moderne Bürgerrecht Datenschutz gilt auch hier. Die DS-GVO sagt nicht, dass keine Daten verarbeitet werden dürfen. Sie sagt, wie Daten verarbeitet werden dürfen. Und sie gibt jedem Bürger Mittel an die Hand, mit seinen personenbezogenen Daten selbstbestimmt umzugehen. Soll die Transformation in die digitale Gesellschaft gelingen, dann kommen wir nicht umhin, digitale Rechte und Pflichten zu wahren. Dies gilt insbesondere, wenn Rechte von Kindern tangiert sind. Die DS-GVO anerkennt und untersagt zum Beispiel die Verwertung von personenbezogenen Daten von Kindern zu Werbezwecken.

Die DS-GVO wirkt. Das wird immer klarer. Aber in Europa funktioniert der gemeinsame und einheitliche Vollzug leider noch nicht. Wir haben Defizite in Irland, Luxemburg, Polen und anderen Staaten, auch nimmt der Europäische Datenschutzausschuss seine Befugnisse nach der DS-GVO (Kohärenzverfahren) noch nicht stringent wahr. Dies ist nicht nur ärgerlich, es ist nicht hinnehmbar. Wir müssen dringend darauf hinwirken, dass unsere gemeinsamen europäischen Standards auch einheitlich vollzogen und durchgesetzt werden.
Letztlich gibt die DS-GVO die Marschrichtung beim Datenschutz klar vor. „Wenn es nicht vernünftig ist, dann ist es kein Datenschutz!" So einfach kann das zusammengefasst werden. Den anhaltenden Schwung der DS-GVO nehmen wir Datenschützer weiterhin optimistisch auf – die Grundlagen für unsere Zuversicht finden sich in diesem Tätigkeitsbericht.

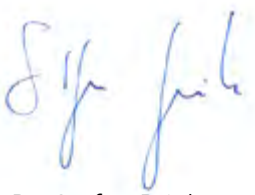
Als Behörde haben wir unsere Aufgaben in diesem Jahr unter besonderen Bedingungen wahrgenommen. Wir haben unsere persönlichen Treffen in Telefon- und Videokonferenzen verlagert. Intensive Absprachen und Flexibilität waren gefragt, um die privaten und dienstlichen Belange bei der zügigen Umstellung zu berücksichtigen. Wir haben eine komplette behördliche Umorganisation vorgenommen und dies gut bewältigt.

Mit Blick auf die Entwicklung des Personals lässt sich sagen: Unsere Behörde ist im vergangenen Jahr weiter gewachsen. Nachdem wir im Jahr 2019 noch 63 Personen beschäftigten, arbeiten derzeit 74 Personen bei uns. Die Besetzung unserer offenen Stellen stellte kein Problem dar, auch im hart umkämpften Bereich Technik nicht. Die Behörde des Landesbeauftragten kann offensichtlich auf eine attraktive Aufgabe und einen guten Ruf bauen. Wir sind offensichtlich auch für Kolleg_innen aus der Verwaltung des Landes, für Interessierte von anderen deutschen Aufsichtsbehörden und auch für Wechselwillige aus der Privatwirtschaft eine Arbeitsstelle mit Anziehungskraft.

Mein Dank gilt allen meinen Mitarbeitenden mit meinem Stellvertreter Herrn Broo an der Spitze für ihre tolle Arbeit, die weit über das Erwartbare hinausgeht – wir Datenschützer sind und bleiben eben „Überzeugungstäter". Nach über 36 Jahren im Dienst für das Land hat sich zum Ende des Jahres Herr Broo in den Ruhestand verabschiedet. Die Pandemie hat verhindert, dass wir ihm als gesamtes Team gebührend und persönlich Dank sagen konnten. Auch ehemalige Weggefährten wollten ihm zum Abschied ihre guten Wünsche persönlich überbringen. Dies alles war jetzt so nicht möglich. So danke ich ihm an dieser Stelle im Namen vieler – und freue mich darauf, diesen Abschied im Jahr 2021 nachzuholen. Herr Broo ist ein exzellenter Beamter mit herausragender Expertise, immer klar, dabei kollegial, zugewandt und hilfsbereit. Wir wünschen ihm für den Ruhestand Glück, Gesundheit, Freude und Zufriedenheit.

Bedanken darf ich mich an dieser Stelle aber auch bei den Abgeordneten des Landtags, welche unsere Aufgabe auch im Jahr 2020 maßgeblich gestaltet, begleitet und gefördert haben. Ich danke auch der Landesregierung, -verwaltung und den Kommunen für die faire und weitgehend einvernehmliche Zusammenarbeit.

Ihr Landesbeauftragter



Dr. Stefan Brink

1. Datenschutz in der Corona-Krise

Die Corona-Pandemie betrifft nahezu alle Lebensbereiche. Dies zeigt anschaulich bereits die Fülle der zur Bewältigung der Corona-Pandemie von der Landesregierung erlassenen Rechtsverordnungen und sonstigen Rechtsvorschriften. Diese wurden teilweise in rascher Abfolge abgeändert, zum Teil im Wochenrhythmus. Wir haben an diesen Regelungen der Landesregierung zur Bewältigung der Corona-Krise mitgewirkt. Auf Grundlage der jeweils gültigen Fassungen der Verordnungen haben wir Ministerien, Kommunen, Verbände, Unternehmen, Vereine, Initiativen und Bürger_innen beraten und ihre Beschwerden bearbeitet.

Aber auch außerhalb der spezifischen Regelungen durch die Corona-Verordnungen hat die Pandemie zahlreiche bereits bekannte und auch neue Fragen des Datenschutzes aufgeworfen. Sie betreffen unter anderem die Grundlagen der Digitalisierung in verschiedenen Bereichen des öffentlichen Lebens, wie etwa in Schulen und Hochschulen, den Beschäftigtendatenschutz, die Ausgestaltung der Corona-Warn-App, sowie das öffentliche Gesundheitswesen.

Der diesjährige Tätigkeitsbericht setzt einen besonderen Schwerpunkt auf den Umgang mit der Corona-Pandemie. Wir sprechen im Folgenden zusammengefasst über wesentliche Themen, welche die Bürger_innen im Corona-Alltag betrafen.

>> Weitere Informationen
Übersicht zu den erlassenen Corona-Verordnungen

https://www.baden-wuerttemberg.de/de/service/alle-meldungen/meldung/pid/aktuelle-aenderungen-der-corona-verordnungen/

1.1 Beteiligung an den Regelungen der Landesregierung zur Bewältigung der Corona-Krise

Die Ministerien haben schon seit jeher nach dem Landesdatenschutzgesetz unsere Behörde bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften, welche die Verarbeitung personenbezogener Daten betreffen, rechtzeitig zu beteiligen (so § 26 Absatz 2 LDSG, vgl. schon § 31 Absatz 4 Satz 2 des Landesdatenschutzgesetzes in der bis zum 20. Juni 2018 geltenden Fassung). Auf diese Verpflichtung weist auch die Verwaltungsvorschrift der Landesregierung und der Ministerien zur Erarbeitung von Regelungen vom 27. Juni 2010 (Az.: 5-05/22, GABl. S. 277, zuletzt geändert durch Verwaltungsvorschrift vom 12.12.2017, GABl. 2018 S. 2) unter Nummer 2.5.3 ausdrücklich hin und weist dem für den jeweiligen Normentwurf jeweils federführende Ministerium die Aufgabe zu, die ordnungsgemäße Beteiligung unserer Behörde sicherzustellen.

Seit Geltung der DS-GVO handelt es sich sogar um eine europarechtliche Verpflichtung: Nach Artikel 26 Absatz 4 DS-GVO konsultieren die Mitgliedstaaten die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, welche die Verarbeitung personenbezogener Daten betreffen.

Zur Bewältigung der Corona-Krise hat die Landesregierung zahlreiche Regelungen geschaffen – insbesondere in den sogenannten Corona-Verordnungen –, welche die Verarbeitung personenbezogener Daten betrafen. Die Entscheidung über solche Regelungen stand nicht immer, aber oft unter hohem politischen Zeitdruck, weil die Landesregierung auf die jeweilige Lage des Infektionsgeschehens und auf den jeweiligen Erkenntnisstand über die Verbreitung des Coronavirus SARS-CoV-2 zu reagieren hatte.

Mit dieser Situation ist die Landesregierung nicht einheitlich umgegangen. In vielen Fällen wurden wir von den Ministerien aufgefordert, innerhalb kurzer bis sehr kurzer Fristen zu den jeweiligen Vorschriftenentwürfen Stellung zu nehmen. Die Kürze der Fristen war dabei jedenfalls oft aufgrund des Entscheidungsdrucks nachvollziehbar. Die Gelegenheit zur Stellungnahme haben wir dann in aller Regel wahrgenommen, um – soweit irgend möglich innerhalb des vorgegebenen Zeitrahmens – durch konstruktiv-kritische Beiträge datenschutzrechtliche Aspekte zur Geltung zu bringen und die Qualität der Regelungsentwürfe insoweit möglichst zu verbessern. In zahlreichen Fällen hat uns die Landesregierung allerdings nicht beteiligt. Dabei scheint es in seltenen Fällen tatsächlich überaus eilbedürftiger Entscheidungen nachvollziehbar zu sein, wenn unsere rechtzeitige Beteiligung angesichts der mit der Corona-Krise verbundenen

Gefahren unausweichlich zu einer politisch nicht vertretbaren Verzögerung des Verfahrens geführt hätte und unsere Beteiligung ausnahmsweise umgehend nachgeholt wurde. Wiederholt vermochten wir indes eine derartige Eilbedürftigkeit nicht zu erkennen. Soweit das Unterlassen der Beteiligung auf der extrem hohen Auslastung der obersten Landesbehörden infolge der enormen Anstrengungen zur Bewältigung der Krise beruhte, haben wir durchaus Verständnis für die Lage und Arbeit der Beteiligten in den jeweiligen Ministerien. Indes scheint uns aber in Teilen auch das Bewusstsein für die Verpflichtung zur Einbindung unserer Behörde nicht gänzlich vorhanden zu sein. Insgesamt halten wir die Verfahren zur Normgebung insoweit für verbesserungswürdig.

Unser umfangreiches Wirken im Zusammenhang mit dem Erlass der Regelungen zur Bewältigung der Pandemie sollen im Folgenden beispielhaft dargestellt werden:

1.2 Die Verarbeitung von Besucher-Daten zur Kontaktnachverfolgung durch die Gesundheitsbehörden nach den Corona-Verordnungen

Am 10. Mai 2020 erließen das Sozialministerium und das Wirtschaftsministerium – ohne uns zuvor zu beteiligen – die erste Version der Corona-Verordnung „Gaststätten", die zum 18. Mai 2020 in Kraft treten sollte. Sie enthielt erstmals eine Bestimmung zur Erhebung der Kontaktdaten von Gästen, die aber weitgehend misslungen war.

Die entsprechende Bestimmung in § 2 Absatz 3 der genannten Verordnung lautete:

„Zu Zwecken der Kontaktnachverfolgung erheben und verarbeiten Betreiber mit Einverständnis der Gäste folgende Daten:
1. *Name des Gastes,*
2. *Datum und Uhrzeit des Besuchs, und*
3. *Kontaktdaten, beispielsweise E-Mail-Adresse oder Telefonnummer.*

Die Daten sind vom Betreiber vier Wochen nach Erhebung zu löschen."

Nachdem wir am 11. Mai 2020 die Verordnung gesehen haben, mussten wir die beteiligten Ministerien darauf aufmerksam machen, dass die genannte Regelung in datenschutzrechtlicher Hinsicht erhebliche Unklarheiten aufwies und nicht rechtskonform war.

So wurde der Begriff „Einverständnis" genutzt. Am ehesten war darunter eine „Einwilligung" im Sinne von Artikel 4 Nummer 11, Artikel 6 Absatz 1 Buchstabe a, Artikel 7 der DS-GVO zu verstehen. Nun ist aber für die Wirksamkeit einer Einwilligung ihre Freiwilligkeit erforderlich (vgl. insbesondere Artikel 7 Absatz 3 DS-GVO), so dass aus der Verweigerung der Einwilligung keine Nachteile folgen dürfen. Die Deutung des „Einverständnisses" als Einwilligung hatte mithin zur Folge, dass die Zulässigkeit der Bewirtung bzw. des Gaststättenbesuchs nicht von der Erteilung der Zustimmung abhängig sein durfte. Dies teilten wir den beteiligten Ministerien mit. Ob vom Verordnungsgeber etwas anderes intendiert war, konnten wir nicht sicher erkennen; es lag uns keine aufklärende Entwurfsbegründung vor. Eine etwaige andere Intention wäre aus unserer Sicht jedenfalls nicht hinreichend im Normtext zum Ausdruck gebracht worden.

Die Regelung enthielt ferner weitere begriffliche Unschärfen. So sollte der/die Betreiber_in die Daten „zu Zwecken der Kontaktnachverfolgung" verarbeiten. Dieser Wortlaut legte nahe, dass die Kontaktnachverfolgung Aufgabe des Betreibers wäre. Vermutlich war aber von Seiten der beteiligten Ministerien gemeint, dass die Kontaktverfolgung (gemäß § 25 des Bundes-Infektionsschutzgesetzes – IfSG) durch das Gesundheitsamt erfolgen soll. Hierzu müsste der Betreiber die Daten dem jeweils zuständigen Gesundheitsamt übermitteln.

Die beteiligten Ministerien reagierten prompt und gaben zu erkennen, dass insbesondere eine Verarbeitung auf Einwilligungsbasis nicht gewollt war, sondern für den Fall eines Gaststättenbesuchs verbindlich. Denn eine gut funktionierende Nachverfolgung durch die Gesundheitsämter im Falle des Auftretens von Infektionen mit SARS-Cov-2 sei Grundvoraussetzung für eine immer weiter voranschreitende Öffnung des öffentlichen Lebens nach dem harten „Lockdown" im Frühjahr 2020.

Zugleich stellte das Sozialministerium dankenswerter Weise auch die übrigen bereits ohne unsere Beteiligung erlassenen Corona-Verordnungen, die ebenfalls die Speicherung von Besucherdaten mit dem Ziel, den Gesundheitsbehörden die Kontaktnachverfolgung zu

ermöglichen, vorsahen, auf den Prüfstand (z. B. die gemeinsam mit dem Kultusministerium erlassenen Verordnungen „Musik- und Jugendkunstschulen" vom 5. Mai 2020 und Sportstätten vom 10. Mai 2020). Hier hat das Sozialministerium umgehend die Beteiligung unserer Behörde nachgeholt.

Im Rahmen der weiteren Erörterungen mit dem Sozialministerium haben wir eine Verpflichtung der Betreiber von Gaststätten, Daten über Besucher_innen und ihre Besuchszeiten zu erheben und zu speichern, im Rahmen einer Rechtsverordnung auf der Grundlage von § 32 IfSG mit Blick auf die Gefahren der Verbreitung von SARS-Cov-2 akzeptiert.

Wir hatten bereits in unseren FAQ vom März 2020 darauf hingewiesen, dass Gesundheitsbehörden entsprechende (Einzel-)Anordnungen gegenüber Veranstaltern auf der Grundlage der §§ 16, 25, 28 ff. IfSG erlassen können. Aus der Regelung einer solchen Pflicht zur Erhebung und Speicherung ergäbe sich sodann auch die Befugnis des Betreibers, dies zu tun (Artikel 6 Absatz 1 Buchstabe c DS-GVO).

Für den potentiellen Übermittlungsvorgang an das Gesundheitsamt hielten wir demgegenüber weitere Regelungen in der Verordnung nicht für erforderlich: Die Befugnis des Gesundheitsamts zur Datenerhebung im Falle des Auftretens einer Infektion folge aus § 25 Absatz 1 und 2 IfSG i. V. m. § 16 Absatz 2 IfSG. Diese Normen regelten zugleich eine Auskunftspflicht der in Anspruch genommenen Person, so dass der/die Gaststättenbetreiber_in im Falle der Inanspruchnahme durch das Gesundheitsamt auf Auskunftserteilung keiner weiteren Übermittlungsbefugnis bedurfte (vgl. wiederum Artikel 6 Absatz 1 Buchstabe c DS-GVO). Dies gelte entsprechend, soweit eine Erhebung der bei der/dem Betreiber_in gespeicherten Daten durch die Gesundheitsbehörden auch zum Zweck der Vorbeugung gegen das Auftreten einer Erkrankung für erforderlich erachtet werden (was das Sozialministerium als Fachbehörde zu entscheiden habe). Dann wäre für diese Auskunftsersuche nach § 16 Absatz 6 IfSG (in Verbindung mit der Verordnung des Sozialministeriums über Zuständigkeiten nach dem Infektionsschutzgesetz in der damals gültigen Fassung) in erster Linie die Ortspolizeibehörde zuständig.

Daher schlugen wir vor zu formulieren, dass die Betreiber zur Erhebung und Speicherung der Daten „ausschließlich zum Zweck der Auskunftserteilung gegenüber dem Gesundheitsamt oder der Ortspolizeibehörde nach §§ 16, 25 IfSG" verpflichtet seien.

Auch die von den Betreibern zu speichernden Datenarten waren zu präzisieren. Insbesondere erschien uns die Datenart „Kontaktdaten" unklar, für die im Normtext nur Beispiele angeführt wurden. Hier sei zu prüfen, welche Daten im Einzelnen hier wirklich benötigt würden. In diesem Zusammenhang wiesen wir darauf hin, dass die Erhebung der E-Mail-Adresse problematisch sei, wenn sie letztlich der Kontaktaufnahme zwischen Gesundheitsamt und Besucher_in diene, weil dem Gesundheitsamt via E-Mail in der Regel keine datenschutzkonforme Kontaktaufnahme möglich sein werde, zumal bei dieser typischerweise zumindest konkludent das Gesundheitsdatum zum Ausdruck gebracht werde, dass der/die Empfänger_in der E-Mail zumindest verdächtig sei, mit dem neuartigen Coronavirus SARS-CoV-2 infiziert zu sein.

Dankenswerter Weise sind das Sozial- und das Wirtschaftsministerium ganz überwiegend unseren Anregungen gefolgt. Sie haben – noch vor ihrem Inkrafttreten – die Corona-Verordnung „Gaststätten" vom 10. Mai 2020 wieder aufgehoben und unter dem 16. Mai 2020 eine neue Verordnung desselben Namens erlassen. Die Bestimmung zur Verarbeitung der Daten der Gäste in § 2 Absatz 3 erhielt die folgende wesentlich verbesserte Fassung:

„Der Betreiber hat, ausschließlich zum Zweck der Auskunftserteilung gegenüber dem Gesundheitsamt oder der Ortspolizeibehörde nach §§ 16, 25 IfSG, die folgenden Daten bei den Gästen zu erheben und zu speichern:

1. *Name und Vorname des Gastes,*
2. *Datum sowie Beginn und Ende des Besuchs, und*
3. *Telefonnummer oder Adresse des Gastes.*

Die Gäste dürfen die Gaststätte nur besuchen, wenn sie die Daten nach Satz 1 dem Betreiber vollständig und zutreffend zur Verfügung stellen. Diese Daten sind vom Betreiber vier Wochen nach Erhebung zu löschen. Die allgemeinen Bestimmungen über die Verarbeitung personenbezogener Daten bleiben unberührt."

Zeitgleich mit der Verkündung der neuen Corona-Verordnung „Gaststätten" haben wir, um den Betreibern die datenschutzkonforme Umsetzung der von ihnen verlangten Verarbeitung von Kundendaten zu erleichtern, eine Musterinformation zur Erfüllung der

Pflichten aus Artikel 13 DS-GVO erstellt und dem Hotel- und Gaststättenverband DEHOGA des Landes Baden-Württemberg zum Zweck der Veröffentlichung auf seiner Internetseite zur Verfügung gestellt.

In der zweiten Juni-Hälfte war sodann die Landesregierung von dem Bestreben getragen, die Corona-Verordnungen neu zu strukturieren, indem offenbar eine Art „allgemeiner Teil" geschaffen werden sollte, der zur Anwendung gelangen sollte, soweit nicht die spezielleren Regelungen der einzelnen Ressorts etwas anderes regelten. Leider wurden wir dabei wieder nicht beteiligt. Vielmehr erhielten wir am 23. Juni 2020 vom Justizministerium „den Text der neuen Corona-Verordnung nebst Begründung" zur Kenntnis übersandt, der noch am selben Tag „im Kabinett beschlossen werden soll". Eine frühere Übersendung sei leider nicht möglich gewesen, da die Abstimmung zwischen den Ressorts erst am Abend zuvor abgeschlossen habe werden können.

Was an dieser zum 1. Juli 2020 in Kraft getretenen Neufassung der Corona-Verordnung derart eilbedürftig gewesen sein soll, dass wir nicht beteiligt werden konnten, war uns nicht ersichtlich. Jedenfalls konnte die Neuregelung der Datenverarbeitung durch Gaststätteninhaber, Veranstalter_innen, Betreiber_innen von Einrichtungen usw., welche die Besuche von „Besucherinnen und Besuchern, Nutzerinnen und Nutzern oder Teilnehmerinnen und Teilnehmern" erfassen und für die Zwecke der Kontaktnachverfolgung durch die Gesundheitsbehörden speichern sollten (§ 6), als wenig gelungen bezeichnet werden, obwohl offenbar das Bestreben bestand, inhaltlich an den bisherigen Regelungen nichts Wesentliches zu ändern und obwohl dem Entwurf der Verordnung erfreulicherweise – nach den vielen ad hoc und ohne begründende Ausführungen erlassenen Regelungen zur Bewältigung der Corona-Pandemie – eine Begründung beigefügt war, der sich weitere wertvolle Hinweise zum Datenschutz entnehmen ließen, namentlich der von uns wiederholt zum Ausdruck gebrachte Umstand, dass die die Daten erhebende Person nicht zur Überprüfung der Richtigkeit der angegebenen Personalien berechtigt oder gar verpflichtet ist.

Die Neuregelung war nicht nur durch ihre Verortung in einem allgemeinen Teil, dessen Verhältnis zum „besonderen Teil" nicht immer klar war, schwer lesbar; sie war auch rechtstechnisch in Teilen defizitär. Beispielsweise sollte sie nach ihrem Wortlaut eingreifen, „soweit durch Regelungen in dieser Verordnung oder aufgrund dieser Verordnung Kontaktdaten zu erheben sind". In der gesamten Verordnung war jedoch nirgends die Rede davon, dass „Kontaktdaten" zu erheben seien. Erneut ist dem Sozialministerium zu danken, dass es uns bei der Überarbeitung der Verordnung zum 28. Juli 2020 die Gelegenheit zur Stellungnahme gab, wodurch nicht alle, aber einige der Mängel behoben werden konnten. Um es deutlicher zu formulieren: Das Sozialministerium war sehr intensiv mit der Pandemie-Bekämpfung befasst, enorm eingebunden und dennoch (wenn leider auch nicht durchweg, so doch) immer wieder in der Lage, wenigstens kurzfristig die Datenschutzbehörde einzubinden. Das konnten wir nicht von jedem Ministerium sagen.

Die obigen Ausführungen benennen keine juristischen Feinheiten. Sie haben eine ganz lebenspraktische Auswirkung. Bürger_innen haben bei uns nachgefragt, Beschwerden eingereicht. Es ging beispielsweise darum, dass Frauen telefonisch belästigt wurden, weil ihre Kontaktdaten in Restaurants herumlagen und zweckwidrig genutzt wurden. Gastronomen haben uns angefragt, als plötzlich die Polizei vor deren Türe stand und Einsicht in die Kontaktlisten verlangten und dergleichen mehr.

FaQ Coronavirus SARS-CoV-2
https://www.baden-wuerttemberg.datenschutz.de/faqs/#FAQ-Corona

1.3 Datenverarbeitung zur Corona-Bekämpfung

„Batman war hier"

Besonders stark betroffen von den Corona-Regelungen war und ist das Gastgewerbe. Von Anfang an haben sich hier wichtige datenschutzrechtliche Fragestellungen aufgetan. Wer erinnert sich nicht an die Diskussionen um die Zettelwirtschaft in Cafés, also das Notieren von Kontakten von Café-Besuchenden zur möglichen Verfolgung eventueller Infektionsketten? Wir haben eben ausführlich darüber berichtet.

Hinzu kamen zu Beginn der Pandemie auch Unklarheiten im Hinblick darauf, welche Bereiche des Gastgewerbes von den jeweiligen Regelungen überhaupt betroffen sind, da die Welt der Gaststätten und gastronomischen Einrichtungen sehr bunt und vielfältig ist:

Datenverarbeitung nach Corona-Verordnung
Hinweis: Es müssen die Daten von allen anwesenden Personen erhoben werden

Herzlich willkommen,

wir freuen uns, Sie bei uns begrüßen zu dürfen. Nach § 6 Abs. 1 CoronaVO sind wir verpflichtet, folgende Daten zu erheben und zu speichern:

Vor- und Nachname	
Anschrift	
Datum und Zeitraum der Anwesenheit	
soweit vorhanden: Telefonnummer	

Datenschutz-Hinweise zur Erhebung personenbezogener Daten gemäß der CoronaVO

Verantwortliche Stelle:
Kontaktdaten Datenschutzbeauftragte*r:

Zu Zwecken der Nachverfolgung von möglichen Infektionswegen gegenüber den zuständigen Behörden erheben und speichern wir folgende Daten von Ihnen:

- Vor- und Nachname,
- Anschrift,
- Datum und Zeitraum der Anwesenheit und
- soweit vorhanden: Telefonnummer

Rechtsgrundlage hierfür ist Artikel 6 Absatz 1 Buchstabe c) der Datenschutz-Grundverordnung (DS-GVO) i.V.m. § 6 Abs. 1 CoronaVO (Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Virus SARS-CoV-2) in ihrer aktuellen Version.
Im Falle eines konkreten Infektionsverdachtes sind die zuständigen Behörden nach dem Bundesinfektionsschutzgesetz Empfänger dieser Daten.
Ihre personenbezogenen Daten werden von uns **vier Wochen** nach Erhalt gelöscht.

Zur Angabe Ihrer persönlichen Daten sind Sie nicht verpflichtet. Eine Prüfung erfolgt nur auf Vollständigkeit und bei handschriftlicher Angabe auf Leserlichkeit. Bei offensichtlich unrichtigen (klar erkennbare Fantasienamen) oder unvollständigen Daten müssen wir nachfragen. Sollten Sie uns Ihre Kontaktdaten allerdings nicht oder unvollständig oder unleserlich oder klar erkennbar unrichtig zur Verfügung stellen, müssen wir Sie vom Besuch oder der Nutzung unseres Betriebes ausschließen.

Hinweis auf Betroffenenrechte:
Sie haben nach der DS-GVO folgende Rechte: Auskunft über die personenbezogenen Daten, die wir von Ihnen verarbeiten; Berichtigung, wenn die Daten falsch sind oder Einschränkung unserer Verarbeitung; Löschung, sofern wir nicht mehr zur Speicherung verpflichtet sind.
Wenn Sie der Meinung sind, dass wir Ihre Daten nicht ordnungsgemäß verarbeiten, steht Ihnen außerdem ein Beschwerderecht beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Königstraße 10a, Stuttgart zu.

Unsere allgemeinen Hinweise zur Verarbeitung personenbezogener Daten finden Sie auf unserer Homepage:

Musterbogen für die DEHOGA.

Gemäß § 1 GastG fallen unter den Begriff „Gastgewerbe“ sämtliche Schank- und Speisewirtschaften, also Restaurants und Gaststätten, aber auch Cafés, Bars, Vergnügungslokale, Eisdielen, Imbisse, Trinkhallen, Shisha- und Raucherbars sowie Kantinen. Teilweise wurde in den Verordnungsregelungen auch innerhalb des Gastgewerbes differenziert. Der Außer-Haus-Verkauf sowie von Abhol- und Lieferdienste waren stets erlaubt, ebenso die Verpflegung im Zusammenhang mit zulässigen Übernachtungsangeboten.

Die in der Corona Verordnung (CoronaVO) enthaltene Kontaktverfolgung im Gastgewerbe stellte nicht wenige Betriebe vor eine große Herausforderung; nicht alle hielten sich an die konkreten Vorgaben der CoronaVO zur Nachverfolgung der Gäste und fragten oftmals „überschießend“ zu viele Daten ab oder legten einfach „Sammellisten“ aus, wodurch man sämtliche vorangegangenen Besucher_innen und Gäste der Gaststätte, samt privater Kontaktdaten, einsehen konnte.

Uns erreichten auch viele Beschwerden von Gästen über diesen datenschutzwidrigen Umgang mit den Kontaktdaten. Wir sind den Beschwerden nachgegangen und haben auf die Einhaltung des Datenschutzes durch die Betreiber hingewirkt und die Verwendung von öffentlich einsehbaren Sammellisten weitgehend eingestellt. Statt Sammellisten sind die Kontakte einzeln zu erfassen, sicher und geschützt vor Dritten zu verwahren und nach vier Wochen zu vernichten – nicht im handelsüblichen Mülleimer, sondern mit Aktenschredder. Nur so können die Vorschriften der CoronaVO datenschutzkonform eingehalten werden.
Um die Arbeit für das Gastgewerbe möglichst gering zu halten, haben wir die DEHOGA Baden-Württemberg dabei unterstützt, ein Standardformular zu entwerfen, das allen Mitgliedern zur Verfügung gestellt wurde. Dieses Muster enthält auch die notwendigen Datenschutzhinweise nach Art. 13 der DS-GVO. Nach § 6 Absatz 1 der CoronaVO in der seit 16. Dezember 2020 gültigen Fassung dürfen nunmehr folgende Daten beim Besuch (Betreten) einer Gaststätte erhoben werden: Name und Vorname des Gastes, seine Adresse, (soweit vorhanden) seine Telefonnummer sowie Datum und Zeitraum der Anwesenheit in der Gaststätte (also Beginn und Ende des Besuchs).

Dass die einzelnen Formulare mit den Daten nach dem Ausfüllen schnell vor unbefugter Einsichtnahme geschützt zu verwahren sind, ergibt sich aus Artikel 24, 25 und 32 DS-GVO und ist ferner in § 6 Absatz 2 der Corona-Verordnung seit der Neufassung vom 23. Juni 2020 noch einmal ausdrücklich bestimmt. Die Verordnung gilt nicht nur mit Blick auf andere Gäste, sondern auch mit Blick auf das Personal, das auch keinen Zugang zu diesen Kontaktdaten haben soll.

Im Sommer 2020 wandte sich eine junge Bürgerin an uns, da diese nach dem Besuch eines Burger-Schnellrestaurants Kontaktversuche via Handy von einem dort angestellten Beschäftigten erhielt. Dieser versuche nun mittels der erhobenen Gastdaten mit ihr privat in Kontakt zu treten. Dieses Verhalten stellt in jedem Fall einen Datenschutzverstoß dar, da gegen das Zweckbindungsgebot verstoßen wurde. Der Vorgang ist in Bearbeitung durch unsere Bußgeldstelle. Daneben ist sehr fraglich, ob der verantwortliche Betreiber des Schnellrestaurants seine Beschäftigten hinsicht-

lich des Umgangs mit den privaten Kontaktdaten ausreichend sensibilisiert und geschult hat.

Wir wurden immer wieder angefragt, ob man denn Phantasienamen in die Formulare einfügen könnte, – etwa aus Sorge vor missbräuchlichen Nutzungen gerade in Fällen, in denen die Formulare nicht sicher verwahrt, sondern z. B. Listen zur Eintragung ausgelegt wurden. Seit der Fassung der Corona-Verordnung „Gaststätten" vom 16. Mai 2020 ist insoweit normiert, dass die Gäste die Gaststätte nur besuchen dürfen, wenn sie ihre Daten dem Betreiber „vollständig und zutreffend" zur Verfügung stellen (vgl. § 6 Absatz 5 der Corona-Verordnung in der aktuellen, ab dem 16. Dezember 2020 geltenden Fassung). Allerdings ist die/der Gaststättenbetreiber_in nicht verpflichtet, die Richtigkeit der angegebenen Personalien zu überprüfen; hierzu hätte sie/er ohnehin nur eingeschränkte Möglichkeiten. Der Betreiber ist vielmehr nach § 6 Absatz 4 der aktuellen Fassung der CoronaVO nur gehalten, Personen, welche die Erhebung ihrer ganz oder teilweise verweigern, von dem Gaststättenbesuch auszuschließen.

Die Angabe von Phantasienamen wie „Batman" oder „Donald Duck" ist – abgesehen davon, dass sie als offensichtliche Verweigerung der richtigen Personalien verstanden werden kann – mit Blick auf die ernste Notwendigkeit der Kontaktverfolgung selbstverständlich kein Ausweg.

Seit der Fassung vom 18. Mai 2020 wurde daher in der (damaligen) CoronaVO „Gaststätten" normiert, dass jeder Gast korrekte Kontaktdaten beim Betreiber der Gaststätte zu hinterlassen hat (nun § 6 Absatz 5 CoronaVO). Mit der Dritten Verordnung der Landesregierung zur Änderung der Corona Verordnung vom 6. Oktober 2020 wurde überdies eingeführt, dass falsche Angaben zu einem Bußgeld gegen den/die Besucher_in führen können.

Zur Angabe seiner persönlichen Daten ist kein Gast im strengen Sinn verpflichtet; auch wird die Richtigkeit seiner Angaben von den Betreibern der Gaststätte nicht überprüft. Sollte der Gast seine persönlichen Daten allerdings nicht zur Verfügung stellen, darf er die Gaststätte nicht besuchen und darin nichts verzehren und lediglich ein evtl. vorhandenes Außer-Haus-Angebot oder einen Lieferdienst nutzen (§ 6 Absatz 4 der CoronaVO in der aktuellen Fassung). De facto besteht also für den Gast die Notwendigkeit, die erforderlichen Angaben wahrheitsgemäß zu machen, um in die Gaststätte einkehren zu können.

>> Weitere Informationen

Zu den verschiedenen Fassungen der (früheren) Corona Verordnung Gaststätten
https://www.baden-wuerttemberg.de/de/service/aktuelle-infos-zu-corona/verordnung-gastronomie/

Formular zur Kontaktnachverfolgung für das Gastgewerbe
https://www.dehogabw.de/servicecenter/servicecenter-details/formular_kontaktnachverfolgung_corona_verordnung.html

„Hilfssheriffs" der Behörden?

Wer ins Restaurant geht, hinterlegt seine Kontaktdaten. Dies dient dazu, den Gesundheitsbehörden zu ermöglichen, Infektionswege zurückzuverfolgen. Zu diesem Zweck dürfen die Kontakt- und Anwesenheitsdaten von den Gesundheitsbehörden (der Ortspolizeibehörde und dem Gesundheitsamt) genutzt werden (§§ 16 und 25 des Infektionsschutzgesetzes; § 6 Absätze 1, 3 CoronaVO). Für andere Zwecke (z.B. Werbung) dürfen diese Daten nicht verwendet werden (§ 6 Absatz 3 Satz 2 CoronaVO).

Die von den Gaststättenbetreibern erhobenen personenbezogenen Daten weckten allerdings auch Begehrlichkeiten bei anderen Behörden, so auch der Polizei. Etliche Fälle in ganz Deutschland sind bekannt geworden, in denen Polizei und Staatsanwaltschaft bei der Ermittlung von Tätern auf die erhobenen Daten der Kontaktnachverfolgung der Gastwirte zurückgegriffen haben. Dies ist mit Blick auf die beschriebene strikte Zweckbindung der Daten, die allerdings nur in einer Landesverordnung geregelt ist, nicht unkritisch gewesen. Allerdings ist zu berücksichtigen, dass diese Zweckbindung in einzelnen Fällen durchbrochen werden konnte, wenn es etwa zur Strafverfolgung erforderlich war.

Als rechtliche Grundlage wurde dabei insbesondere auf die Strafprozessordnung hingewiesen. Nach dieser können Richter sowie unter Umständen auch Staatsanwälte und bestimmte Polizeibeamte anordnen, dass Gegenstände beschlagnahmt werden, wenn diese für Ermittlungen von Bedeutung sind. Die Straf-

prozessordnung ging als Bundesrecht der nur in einer Landesverordnung geregelten engen Zweckbindung vor (vgl. Artikel 31 des Grundgesetzes). Gaststättenbetreibern empfehlen wir, sich schriftlich von der anfragenden Stelle die Ermächtigungsgrundlage bestätigen zu lassen und dies als Nachweis aufzubewahren.

Hier ist aber eine aktuelle Rechtsänderung mitzuteilen, die zu einer Klarstellung führt: Die strenge Zweckbindung der Daten zur Kontaktverfolgung ist seit dem 19. November 2020 auch bundesrechtlich festgeschrieben worden: Im Rahmen des Dritten Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite wurde in § 28a des Infektionsschutzgesetzes eine neue Rechtsgrundlage für Anordnungen zur Verhinderung der Verbreitung des Coronavirus SARS-CoV-2 geschaffen. Nach § 28a Absatz 1 Nummer 17, § 32 IfSG können die Landesregierungen zu diesem Zweck insbesondere Rechtsverordnungen erlassen, die eine „Anordnung der Verarbeitung der Kontaktdaten von Kunden, Gästen oder Veranstaltungsteilnehmern" enthalten, „um nach Auftreten einer Infektion mit dem Coronavirus SARS-CoV-2 mögliche Infektionsketten nachverfolgen und unterbrechen zu können." Für die aufgrund solcher Anordnungen verarbeiteten Daten gilt nunmehr nach § 28a Absatz 4 IfSG eine strenge Zweckbindung; so heißt es in § 28a Absatz 4 IfSG insbesondere:

„Im Rahmen der Kontaktdatenerhebung nach Absatz 1 Nummer 17 dürfen von den Verantwortlichen nur personenbezogene Angaben sowie Angaben zum Zeitraum und zum Ort des Aufenthaltes erhoben und verarbeitet werden, soweit dies zur Nachverfolgung von Kontaktpersonen zwingend notwendig ist […]. Die Daten dürfen nicht zu einem anderen Zweck als der Aushändigung auf Anforderung an die nach Landesrecht für die Erhebung der Daten zuständigen Stellen verwendet werden […]. Eine Weitergabe der übermittelten Daten durch die zuständigen Stellen […] oder eine Weiterverwendung durch diese zu anderen Zwecken als der Kontaktnachverfolgung ist ausgeschlossen."

Damit ist mittlerweile anderen Behörden, auch den Strafverfolgungsbehörden, der Zugriff auf diese Daten verwehrt. Eine gute Entscheidung des Gesetzgebers.

Dokumentationspflichten im Verein

Auch Vereine hatten mit den neuen Anforderungen durch die Pandemie zu kämpfen. Der Umgang mit Dokumentations-Listen und den Inhalten von Hygiene-Konzepten nach der jeweils gültigen, den Sport betreffenden Regelungen der Corona-Verordnungen war und ist eine Herausforderung. Wir wurden regelmäßig angefragt dabei zu helfen, datenschutzkonforme Listen und Fragebögen zu formulieren.

Im Rahmen der den Sport betreffenden Corona-Verordnungen wurden im Lauf des Jahres 2020 den Vereinsverantwortlichen mehrere Maßnahmen auferlegt. Insbesondere waren Vorgänge im Hinblick auf den Zugang zu den Sportstätten gegenüber den Gesundheitsbehörden nach der jeweils geltenden Corona-Verordnung Sportstätten zu dokumentieren.

Wie komplex die Thematik war, zeigt sich an einem Beispiel: Ein Sportverein wandte sich an uns und stellte uns einen Fragebogen vor, der zur Einschätzung von Risiken im Hinblick auf Covid-19-Fälle bei Vereinsmitgliedern herangezogen werden sollte. Dazu wurden neben den Kontaktdaten der Mitglieder auch Fragen zu Vorerkrankungen, zu Kontakten zu bestätigten Covid-19-Fällen, Einzelheiten zu Quarantäneanordnungen, Reisen innerhalb der letzten 14 Tage und bestimmten Symptomen gestellt.

Grundsätzlich darf eine verantwortliche Stelle nach dem Prinzip der Datenminimierung nur diejenigen personenbezogenen Daten erheben, die zur Erreichung eines bestimmten (legitimen) Zwecks erforderlich sind. Den vom Verein verfolgten Zweck sahen wir darin, dass er seinen gesetzlichen Verpflichtungen aus der Corona-Verordnung des Kultusministeriums und des Sozialministeriums über Sportstätten (CoronaVO „Sportstätten") – seinerzeit vom 10. Mai 2020 beim Betrieb von Freiluftanlagen – zu entsprechen hatte.

Von der Teilnahme am Trainings- und Übungsbetrieb ausgeschlossen waren danach Personen, die in Kontakt zu einer infizierten Person stehen oder standen, wenn seit dem Kontakt mit einer infizierten Person noch nicht 14 Tage vergangen sind, oder sie die Symptome eines Atemwegsinfekts oder erhöhte Temperatur aufweisen. Dieser Ausschluss traf bei Sportvereinen oftmals die Trainierenden selbst. Der Verein kann (und sollte) auf den Ausschluss hinweisen, ist aber weder gehalten noch befugt, die entsprechenden Informationen zu Symptomen oder Kontaktpersonen zu eigenen Zwecken zu erheben. Denn der Ausschluss stellt ein unmittelbar an die davon betroffenen Trainierenden gerichtetes Verbot dar, nicht jedoch ein Gebot

an den Verein, die Trainierenden insoweit zu überprüfen. Unter dem Gesichtspunkt des Infektionsschutzes waren – nach einer anderen Vorschrift der Verordnung, welche die Vereinfachung der Kontaktnachverfolgung durch die Gesundheitsbehörden bezweckte, – demgegenüber nur die Namen der Teilnehmenden je Trainingseinheit und des Verantwortlichen.

Durch die dann ab 2. Juni 2020 geltende Corona-Verordnung „Sportstätten" wurde der Umfang der von den Teilnehmenden zu erhebenden und für vier Wochen zu speichernden Daten etwas erweitert und umfasste nunmehr:

- Name und Vorname der Nutzerin oder des Nutzers,
- Datum sowie Beginn und Ende des Besuchs, und
- Telefonnummer oder Adresse der Nutzerin oder des Nutzers.

Der vom Verein zur Überprüfung übersandte Fragebogen durfte also für den Laiensport in Baden-Württemberg in dieser Form nicht verwendet werden. Bei Anwendung der Corona-Verordnungen ist genau zu prüfen, welche Regelungen sich an den jeweiligen Sportstättenbetreiber richten und welche an die Besucher_innen der Anlagen. Ein an die Trainierenden gerichtetes Ge- oder Verbot legitimiert nicht den Verein, (zumal: sensible Gesundheits-)Daten der Besucher_innen zu verarbeiten.

Wir konnten schlussendlich dem Verein mit Hinweisen und Ratschlägen zu einem Fragebogen verhelfen, der sowohl den Anforderungen der CoronaVO als auch der DS-GVO genügte.

>> Weitere Informationen

Übersicht über die im Laufe des Jahres 2020 erlassenen, den Sport betreffenden Corona-Verordnungen

https://km-bw.de/CoronaVO+Sport

Zugang zum Rathaus nur gegen Daten

Auch der Gang in ein Rathaus wird durch Verordnungen auf der Grundlage des Infektionsschutzgesetzes begleitet. In diesen schwierigen Zeiten sind die Gemeinden bestrebt, ihr normales Tagesgeschäft so weit wie möglich aufrecht zu erhalten. Dies ist nicht immer so einfach, was folgendes Beispiel zeigt:

Eine Kommune wollte nach den Sommerferien ihre Beschäftigten besonders schützen und verlangte deshalb von allen Besuchern des Behördenzentrums beim Betreten eine namentliche Erklärung über eventuelle Aufenthalte im Ausland, insbesondere bezüglich solcher Länder, welche zu Risikogebieten erklärt wurden. Ihr Vorgehen sah die Gemeinde gemäß Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe a der DS-GVO als rechtens an. Es wurde angenommen, dass die Bürger_innen mit dem Ausfüllen des Erhebungsbogens in die Verarbeitung ihrer persönlichen Daten einwilligen würden.

Der Gemeinde haben wir mitgeteilt, dass sie damit falsch liegt. Jedenfalls kann sich die Gemeinde nicht auf eine wirksame, d.h. freiwillige Einwilligung in die Datenverarbeitung berufen. Freiwilligkeit scheidet nämlich beispielsweise dann aus, wenn das Erbringen einer Dienstleistung von der Einwilligung in die Datenverarbeitung abhängig gemacht wird. Außerdem ist die Freiwilligkeit einer Willenserklärung zur Datenverarbeitung immer dann genau zu prüfen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, also beispielsweise, wenn es sich bei dem Verantwortlichen um eine Behörde handelt.

In unserem Fall sah die Gemeinde vor, dass die Bürger_innen nur dann das Behördenzentrum betreten können, wenn sie die Erklärung mit ihrem Namen, Adresse und zum Auslandsaufenthalt ausfüllen und abgeben. Somit sah sich, wer etwa seinen Reisepass abholen oder die Miete für die Fahrradbox am Bahnhof verlängern wollte, genötigt, seine personenbezogenen Daten anzugeben. Es liegt auf der Hand, dass Betroffene unter diesen Umständen wohl kaum vollkommen freiwillig ihre Daten preisgeben.

Auch in der Corona-Verordnung des Landes sucht man erfolglos nach einer passenden Rechtsgrundlage für die Datenerhebung bei Eintritt in das Rathaus. Die Corona-Verordnung des Landes regelt, wer welche Daten für welche Zwecke verarbeiten darf die Datenverarbeitung (§§ 6 und 14). Nach § 6 Absatz 1 CoronaVO dürfen die Daten

„ausschließlich zum Zwecke der Auskunftserteilung gegenüber dem Gesundheitsamt oder der Ortspolizeibehörde nach §§ 16, 25 IfSG erhoben und gespeichert werden."

Eine Berechtigung zur Datenerhebung zum Zweck der Nachverfolgung von Infektionsketten, wie sie etwa bei Schwimmbädern oder Gaststätten durch die Rechtsverordnung erfolgt, besteht für Rathäuser danach nicht; Gemeinden sind in dem Katalog nicht enthalten (§ 14, „zur Datenverarbeitung Verpflichteten").

In Ermangelung sonstiger Bestimmungen wäre allenfalls noch § 4 des Landesdatenschutzgesetzes in Betracht zu ziehen. Danach können öffentliche Stellen dann personenbezogene Daten verarbeiten, wenn diese zur Erfüllung der in der Zuständigkeit der öffentlichen Stelle liegende Aufgabe erforderlich sind. Die Erfassung der in § 6 CoronaVO genannten Daten der Besucher_innen von Rathäusern und Bürgerzentren zum Zweck der Auskunftserteilung für die Gesundheitsbehörde oder das Ordnungsamt ist aber keine originäre Aufgabe der Gemeinde. Es gibt somit derzeit (Stand Ende November 2020) keine Rechtsgrundlage für Kommunen, die Daten der Bürger_innen beim Besuch der Verwaltung zur Nachverfolgung von Infektionsketten oder zugunsten des Beschäftigungsschutzes zu erheben.

Für den Gesundheitsschutz der Mitarbeitenden sind beispielsweise Hygiene- und organisatorische Maßnahmen zuvorderst umzusetzen, wie Abstandspflichten, Tragen einer Mund-Nase-Bedeckung und Desinfektionsmöglichkeiten für die Hände.

Den Kommunen, die eine hinreichende Nachverfolgbarkeit der Infektionsketten sicherstellen wollen, ist zu empfehlen, den Publikumsverkehr einzuschränken und Behördengänge nur nach vorheriger Terminvereinbarung zu ermöglichen. Eine umfassende Information zur Rechtslage bezüglich Reiserückkehrern und Quarantänepflichtigen sollte dabei nicht fehlen.

Befreiung von der Maskenpflicht: „Nicht ohne meinen Arzt"

Mit der sechsten Verordnung der Landesregierung zur Änderung der CoronaVO vom 23. April 2020 wurde erstmals die Verpflichtung eingeführt, in bestimmten Bereichen des öffentlichen Lebens (im Einzelnen: im öffentlichen Personennahverkehr, an Bahn- und Bussteigen und in den Verkaufsräumen von Ladengeschäften und allgemein in Einkaufszentren) eine nicht-medizinische Alltagsmaske oder eine vergleichbare Mund-Nasen-Bedeckung zu tragen. Diese Pflicht galt nicht, „wenn dies aus medizinischen Gründen oder aus sonstigen zwingenden Gründen unzumutbar ist oder wenn ein anderweitiger mindestens gleichwertiger baulicher Schutz besteht." Hier tauchte früh die Frage auf, wer prüfen darf oder muss, ob die Voraussetzungen für die Ausnahme gegeben sind, dass das Tragen einer Maske „aus medizinischen Gründen oder aus sonstigen Gründen unzumutbar ist". Eine Pflicht der Betroffenen, die Voraussetzungen gegenüber bestimmten Stellen zu belegen, war in der Corona-Verordnung ursprünglich nicht vorgesehen.

Wir hatten im Rahmen der uns dankenswerter Weise vom Sozialministerium ordnungsgemäß eingeräumten Beteiligung an dem Erlass seiner Verordnung über Besuchsregelungen in Krankenhäusern, Pflegeeinrichtungen und vergleichbaren Einrichtungen (Corona-Verordnung Besuchsregelungen) vom 14. Mai 2020 Gelegenheit, die Frage mit der Landesregierung zu erörtern. Diese Verordnung enthielt in § 2 Absatz 5 – entsprechend der Regelung in der seinerzeitigen Corona-Verordnung – die folgende Bestimmung:

„Besucherinnen und Besucher ab dem vollendeten sechsten Lebensjahr müssen während des gesamten Aufenthalts in der Einrichtung eine nicht-medizinische Alltagsmaske oder eine vergleichbare Mund-Nasen-Bedeckung tragen, sofern dies nicht aus medizinischen Gründen oder aus sonstigen zwingenden Gründen unzumutbar ist."

Im Entwurf der Verordnung war hierfür ergänzend vorgesehen, dass die Leitung der Einrichtung dafür Sorge zu tragen habe, dass die Maßgaben für Besucher_innen (neben der Maskenpflicht z. B. auch die Pflicht zur Händedesinfektion bei Betreten der Einrichtung) eingehalten werden. Sie habe die Besucher_innen im Bereich der Zutrittsstellen der Einrichtung deutlich sichtbar in geeigneter Weise auf diese Maßgaben hinzuweisen. Im Rahmen der Beteiligung haben wir darauf hingewiesen, dass aus dem Entwurf nicht in ausreichend eindeutiger Weise hervorgehe, welche Maßgaben die besuchende Person sicherzustellen hat und welche die Leitung der Einrichtung. Insbesondere werde nicht ausreichend differenziert, inwieweit (also gegebenenfalls auch wodurch) die Leitung der Einrichtung selbst für die Einhaltung der Maßgaben „Sorge zu tragen" habe und inwieweit diese nur Hinweispflichten treffen. In Bezug auf die Maskenpflicht sei normenklar zu regeln, inwieweit die Einrichtung die medizinischen oder sonstigen zwingenden Gründe

der Befreiung von der Maskenpflicht zu prüfen (und möglicherweise zu speichern) habe.

Auf diese Hinweise ist das Sozialministerium erfreulicher Weise eingegangen und hat die pauschale Bestimmung gestrichen, nach der die jeweiligen Leitungen der Einrichtungen dafür Sorge zu tragen hätten, dass die an die Besucher_innen gerichteten Maßgaben eingehalten werden. Die Streichung sei inhaltlich unbedenklich, zumal sich eine vergleichbare Vorgabe für das Sorgetragen bislang auch nicht in der CoronaVO befinde.

Damit war aus unserer Sicht klargestellt, dass sich die in der Verordnung vorgesehene Verpflichtung zum Tragen eine Maske grundsätzlich (zu Ausnahmen siehe z.B. § 1 Absatz 6 und 7 der Verordnung) ausschließlich an die Besucher_innen richtete und namentlich das Vorliegen von medizinischen oder sonstigen zwingenden Ausnahmegründen nicht durch die Leitung der Einrichtung zu überprüfen war.

Mit der zum 1. Juli 2020 in Kraft getretenen Verordnung der Landesregierung über infektionsschützende Maßnahmen gegen die Ausbreitung des Coronavirus SARS-CoV-2 (CoronaVO) vom 23. Juni hat die Landesregierung – wie bereits ausgeführt völlig ohne unsere Beteiligung – die Regelungen zur Bekämpfung der Pandemie völlig neu geordnet. Dabei fanden sich in der Begründung der Verordnung erstmals Ausführungen dazu, wie die Gründe für eine Ausnahme von der Maskenpflicht „glaubhaft gemacht" werden könnten. Mit der insoweit ebenfalls ohne unsere Beteiligung erlassenen Zweiten Verordnung der Landesregierung zur Änderung der CoronaVO vom 22. September 2020 wurde sodann sogar der Text der CoronaVO dahingehend verändert, dass die Verpflichtung zum Tragen einer Mund-Nasen-Bedeckung nur noch für Personen gelten soll,

„die glaubhaft machen können, dass ihnen das Tragen einer Mund-Nasen-Bedeckung aus gesundheitlichen oder sonstigen zwingenden Gründen nicht möglich oder nicht zumutbar ist, wobei die Glaubhaftmachung gesundheitlicher Gründe in der Regel durch eine ärztliche Bescheinigung zu erfolgen hat".

Völlig offen blieb dabei jeweils die datenschutzrechtlich entscheidende Frage, wem gegenüber diese Glaubhaftmachung erfolgen muss, wer also zur Überprüfung der Ausnahmegründe berechtigt oder gar verpflichtet sein soll. Dies hat zu einer Flut von Eingaben bei uns geführt. Neben häufig auszuhaltenden Anfeindungen im öffentlichen Raum geht es den Betroffenen auch um datenschutzrechtliche Fragestellungen. Im Kern der Anfragen an uns ging es daher sowohl um die Frage der Anforderungen an die Glaubhaftmachung sowie einen datenschutzkonformen Umgang mit diesen Erkenntnissen.

Das Kultusministerium hat – ohne unsere Beteiligung – am 15. Oktober 2020 eine Handreichung dazu herausgegeben, wie mit der Maskenpflicht an Schulen umzugehen sei. Darin geht das Kultusministerium (ohne nähere Begründung) davon aus, dass die Schule das Vorliegen eines Ausnahmetatbestandes überprüfen müsse und eine Glaubhaftmachung verlangen könne. Gesundheitliche Gründe seien dabei in der Regel durch die Bescheinigung eines Arztes nachzuweisen, psychisch bedingte Ausnahmegründe könnten auch von approbierten Psychotherapeuten beziehungsweise approbierten Kinder- und Jugendtherapeuten bescheinigt werden. Der Nachweis sei in die an der Schule geführten Schülerakten bzw. Personal-Teilakten aufzunehmen (Kopie genügt).

Immerhin führt das Kultusministerium auch aus, dass die Bescheinigung grundsätzlich keine Diagnose enthalten müsse. Lediglich sofern begründete Zweifel daran bestünden, dass der Bescheinigung eine individuelle medizinische Einschätzung zugrunde läge, die sich an den Vorgaben der CoronaVO orientiere, könne die Vorlage eines qualifizierten Attests verlangt werden, in dem nachvollziehbar medizinisch begründet wird, weshalb gesundheitliche Gründe das Tragen einer Mund-Nase-Bedeckung unmöglich oder unzumutbar machen.

Das Verwaltungsgericht Stuttgart ging in einer Eilentscheidung vom 30.11.2020 (Az. 12 K 5502/20) möglicherweise noch darüber hinaus. Nach der in der zugehörigen Presseerklärung geäußerten Auffassung des Verwaltungsgerichts soll möglicherweise stets eine „aussagekräftige" ärztliche Bescheinigung erforderlich sein, die der Schulleitung und den damit befassten Gerichten eine sachgerechte Entscheidung darüber ermögliche, ob der „Befreiungstatbestand" erfüllt sei. Ein Attest erfülle diese Voraussetzungen nicht, wenn aus ihm nicht hervorgehe, welche gesundheitlichen Beeinträchtigungen durch das Tragen einer Mund-Nasen-Bedeckung jeweils hervorgerufen würden und wie es dazu komme und auf welcher Grund-

lage der attestierende Arzt zu seiner Einschätzung gelangt sei. Es sei nicht vorgeschrieben und auch nicht erforderlich, dass eine genaue Diagnose gestellt wird; die durch das Tragen der Mund-Nasen-Bedeckung hervorgerufenen Symptome seien jedoch vom Aussteller des Attestes fachkundig zu umschreiben.

Die sämtlich ohne unsere Beteiligung erlassenen Corona-Verordnungen „Schule" enthalten leider keine näheren Bestimmungen zu diesen Fragen. Unserer dringenden Bitte, diese mit uns zu erörtern, um zu einer einheitlichen Rechtsauffassung – etwa auch zur Frage der Speicherungsbedürftigkeit vorgelegter Atteste – zu gelangen und möglichst eine normenklare Regelung zu schaffen, ist das Kultusministerium leider bislang nicht nachgekommen.
Mag man bei öffentlichen Schulen grundsätzlich wegen ihrer besonderen Fürsorgepflicht und wegen des Erziehungsauftrages weitergehende Überprüfungsmöglichkeiten hinsichtlich der Einhaltung der Maskenpflicht für vertretbar halten, so ist die mangelnde Bestimmtheit der Corona-Verordnungen zu der Frage, wer sonst noch in welcher Weise zur Überprüfung berechtigt sein soll, unerträglich.

Das Sozialministerium hat insoweit zu der Frage aus dem Antrag der Abgeordneten Sabine Wölfle u. a., SPD, vom 22. Oktober 2020 (LT-Drs.16/9117), welche staatlichen und nichtstaatlichen Stellen bei welchen Kontrollen die Vorlage von ärztlichen Bescheinigungen über die Maskenpflicht verlangen dürfen und inwieweit sie diese prüfen dürfen, am 1. Dezember 2020 wie folgt Stellung genommen:

„Grundsätzlich darf die ärztliche Bescheinigung jeder verlangen. Allerdings besteht gegenüber nichtstaatlichen Stellen, insbesondere Ladenbesitzern, keine Vorlagepflicht. Im Falle der Nichtvorlage darf der Zutritt mittels des Hausrechts verweigert werden. Vorlagepflicht besteht gegenüber der zuständigen Behörde nach § 1 Absatz 6 bzw. 6 a der Verordnung des Sozialministeriums über Zuständigkeiten nach dem Infektionsschutzgesetz vom 14. Juli 2007."

Wirklich erhellend ist diese Antwort nicht. Immerhin ging das Sozialministerium in seiner Stellungnahme davon aus, dass nach der CoronaVO in keiner Weise die Vorlage eines qualifizierten Attests verlangt werde.

Unsere dringende Anregung, diese Fragen in der CoronaVO eindeutig zu regeln (wozu auch nähere Bestimmungen dazu gehören würden, wann genau beurteilende Ärzte von einer Unzumutbarkeit ausgehen sollen), ist das Sozialministerium bedauerlicher Weise bislang nicht nachgekommen.

Die Verarbeitung von sensiblen Gesundheitsdaten, welche nach der DS-GVO als besonders schützenswert gelten, ist nur in engen Grenzen möglich. Abgesehen davon, dass entsprechende gesetzliche Regelungen normenklar sein müssen, ist der Grundsatz der Datenminimierung (Art. 5 Absatz 1 Buchstabe c DS-GVO) hierbei besonders zu beachten und dafür Sorge zu tragen, dass keine überschießenden Informationen, Diagnosen oder Befunde gegenüber Dritten exponiert werden müssen. Soweit nationales Recht die Verarbeitung von Gesundheitsdaten ermöglicht oder vorschreibt, hat es angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person vorzusehen (vgl. Art. 9 Absatz 2 Buchstaben g und i DS-GVO).

Es erscheint insoweit mehr als fraglich, wie ein Gaststättenbetreibender, sonstiger Geschäftsinhaber, eine Personalchefin in einem Unternehmen oder eine nicht medizinisch geschulte Leitung einer Behörde aufgrund eines im Attest beschriebenen Krankheitsbildes entscheiden können soll, ob dieses beim Betroffenen zur Befreiung von der Maskenpflicht führen kann. Diese Entscheidung sollte allein in der Zuständigkeit der dies beurteilenden Ärzte liegen. Den Ärzt_innen sind hierfür klare Maßstäbe an die Hand zu geben, z. B. zu der entscheidenden Frage, für welche Dauer das Tragen einer Bedeckung der betroffenen Person jeweils unzumutbar sein muss, um ein entsprechendes Attest ausstellen zu dürfen. Ein generelles Misstrauen in entsprechende ärztliche Bescheinigungen zum Nachteil auch der Betroffenen erscheint demgegenüber unangemessen. Soweit – über den strafrechtlichen Schutz aus § 278 des Strafgesetzbuchs hinausgehend – verhindert werden soll, dass einzelne Ärzt_innen unberechtigt Atteste ausstellen, käme in Betracht, die Ausstellung derartiger Bescheinigungen (in etwa vergleichbar mit dem Verfahren bei Einstellungsuntersuchungen) nur bestimmten, nicht behandelnden Ärzt_innen vorzubehalten, solange die Gesundheitsämter selbst aus Gründen ihrer Kapazität keine eigenen Prüfungsmöglichkeiten haben.

>> Weitere Informationen

CoronaVO Besuchsregelungen
https://www.baden-wuerttemberg.de/fileadmin/redaktion/m-sm/intern/downloads/Downloads_Gesundheitsschutz/200514_SM_CoronaVO_Besuchsregelungen.pdf

https://www.baden-wuerttemberg.de/fileadmin/redaktion/dateien/PDF/Coronainfos/200623_Corona-Verordnung_Begruendung.pdf

Handreichung zur Maskenpflicht an Schulen, vom 15.10.2020
https://km-bw.de/site/pbs-bw-km-root/get/documents_E-1215370759/KULTUS.Dachmandant/KULTUS/KM-Homepage/Artikelseiten%20KP-KM/1_FAQ_Corona/Schreiben%20Min%20Schuljahr%2020_21/2020%2010%2015%20Anlage%20Handreichung%20Maskenpflicht.pdf

PRESSEMITTEILUNG vom 30. November 2020: Eilantrag gegen Maskenpflicht für Schüler abgelehnt
https://verwaltungsgericht-stuttgart.justiz-bw.de/pb/,Lde/7645658/?LISTPAGE=5597587

1.4 Die Polizei in der Corona-Krise

Der übereifrige Beamte

Als hätte der Polizeivollzugsdienst nicht ohnehin schon alle Hände voll zu tun, um seine Aufgaben bei der Gefahrenabwehr und der Strafverfolgung zu erledigen, wird er in Zeiten der Corona-Pandemie immer wieder gerne zu Hilfsleistungen für andere Behörden herangezogen, die eigentlich selbst für die Bekämpfung der Pandemie zuständig sind. Und allzu oft lassen sich die Beamt_innen dazu verleiten, solche Aufträge anzunehmen, ohne näher darüber nachzudenken, ob sie das eigentlich auch dürfen. Denn klar ist: Der Polizeivollzugsdienst hat im Rahmen der Seuchenbekämpfung keinerlei Zuständigkeiten. Diese ist allein Sache der Gesundheitsämter und der durch Landesverordnung den Ortspolizeibehörden übertragenen Aufgaben als „zuständige Behörde“ nach dem Infektionsschutzgesetz (IfSG). Folgender Fall soll hier exemplarisch für die Problematik stehen:

Ein Bürger deutete in einem Leserbrief an, dass enge Verwandte, die in einer anderen Stadt wohnten, an Covid-19 erkrankt seien. Der Ortsbürgermeister sah sich daraufhin zu „Nachermittlungen“ veranlasst und wandte sich diesbezüglich an das örtliche Polizeirevier. Ein Beamter dieses Reviers suchte umgehend den Briefschreiber auf und befragte ihn sowie dessen Ehefrau zu eventuellen körperlichen Kontakten zwischen ihnen und den Verwandten. Ziel der Befragung war es festzustellen, ob die Ehefrau des Briefeschreibers, die kurz zuvor als Zuhörerin an einer Gemeinderatssitzung teilgenommen hatte, andere anwesende Personen möglicherweise einem Infektionsrisiko ausgesetzt hatte. Der Beamte kam letztlich zum Ergebnis, dass dies nicht der Fall gewesen sei und informierte den Bürgermeister über seine Feststellungen.

Nachdem sich der Bürger bei uns über diese Befragung durch die Polizei beschwert hatte, forderten wir das zuständige Polizeipräsidium unter Hinweis darauf, dass wir die Befragung durch den Polizeibeamten aus datenschutzrechtlicher Sicht für unzulässig hielten, zur Stellungnahme auf. In einer ersten Reaktion beschränkte sich das Polizeipräsidium darauf, lediglich eine Stellungnahme des betroffenen Polizeibeamten kommentarlos zu übersenden.

Diese Vorgehensweise war ungewöhnlich, hatten wir doch das Polizeipräsidium um seine Meinung und nicht um die des Beamten gefragt. Uns konnte auch

die auf unsere Aufforderung nachgereichte rechtliche Bewertung des Polizeipräsidiums nicht zufriedenstellen. Denn dieses kam zum Ergebnis, dass die Datenverarbeitung durch den Polizeibeamten rechtmäßig gewesen sei, wobei man sich dabei auf Bestimmungen des Polizeigesetzes stützte (§ 60 Absatz 2, § 2 Absatz 1, § 20 Absatz 1, § 42 Absatz 1). Aus unserer Sicht allerdings zu Unrecht:

Die Zuständigkeiten für die Verhütung und Bekämpfung übertragbarer Krankheiten und damit auch, wer unter welchen Voraussetzungen personenbezogene Daten für diese Zwecke verarbeiten darf, ergeben sich grundsätzlich aus dem Infektionsschutzgesetz (IfSG).

Schon mit der Schaffung des Bundes-Seuchengesetzes von 1961 wurde klargestellt, dass die Vorschriften des allgemeinen Polizeirechts in diesem Zusammenhang nicht (mehr) gelten sollten (BT-Drs. 1888 vom 27. Mai 1960, Begründung zu dem heutigen § 16 IfSG entsprechenden § 10: „Der Entwurf sieht insoweit eine abschließende Regelung vor."). Dies entspricht auch der derzeitigen Rechtslage. Geht es um Maßnahmen vor dem Auftreten übertragbarer Krankheiten, ist die „zuständige Behörde" nach § 16 Absatz 1 IfSG (nach § 1 Absatz 6 Satz 1 der Verordnung des Sozialministeriums über Zuständigkeiten nach dem Infektionsschutzgesetz grundsätzlich die Ortspolizeibehörde, bei besonders hohen Inzidenzwerten nach Maßgabe von Absatz 6a-6c allerdings ausnahmsweise ebenfalls das Gesundheitsamt) befugt, die notwendigen Abwehrmaßnahmen zu treffen. Geht es um Maßnahmen nach dem Auftreten übertragbarer Krankheiten, liegt die Zuständigkeit, die erforderlichen Ermittlungen anzustellen, nach § 25 Absatz 1 IfSG beim Gesundheitsamt. Erst wenn sich aufgrund solcher Ermittlungen ergibt, dass Schutzmaßnahmen zu treffen sind, weist § 28 Absatz 1 Satz 1 IfSG der „zuständigen Behörde" (Ortspolizeibehörde bzw. – bei hohen Inzidenzwerten – dem Gesundheitsamt) entsprechende Zuständigkeiten zu.

Im hier vorliegenden Fall ging es um die Ermittlung eines Krankheitsverdachts, wofür nach § 25 Absatz 1 IfSG das Gesundheitsamt zuständig gewesen wäre. Die Ortspolizeibehörde war dagegen nicht zuständig. Folglich konnte der Bürgermeister den Polizeivollzugsdienst auch nicht wirksam „beauftragen". Abgesehen davon, dass das Polizeigesetz wegen der abschließenden Regelungen im Infektionsschutzgesetz grundsätzlich nicht anwendbar ist, lagen auch die Voraussetzungen für eine Eilzuständigkeit nach § 60 Absatz 2 PolG nicht vor. Denn offensichtlich hatten die Beamten des Polizeireviers schon gar nicht den Versuch unternommen, das zuständige Gesundheitsamt zu informieren.

Es war in keiner Weise nachvollziehbar, dass keine Möglichkeit bestanden haben sollte, dem Gesundheitsamt den Sachverhalt mitzuteilen, damit dieses prüfen könne, ob und gegebenenfalls was zu veranlassen sei. Der Besuch fand um 10 Uhr vormittags statt, zu einer Zeit also, zu der das Gesundheitsamt jedenfalls arbeitsfähig gewesen war. Die Rechtsfertigungsversuche des Polizeipräsidiums in seiner Stellungnahme erscheinen daher wenig überzeugend.

Gleichfalls unzulässig war die Übermittlung der erhobenen personenbezogenen Daten an den Bürgermeister. Soweit hierfür auf § 42 Absatz 1 PolG verwiesen wurde, scheitert dies schon daran, dass die Bestimmungen des allgemeinen Polizeirechts im Zusammenhang mit der Bekämpfung übertragbarer Krankheiten nicht anwendbar sind. Hinzu kommt, dass die Übertragung von Maßnahmenbefugnissen nach dem IfSG auf die Ortspolizeibehörden nicht mit der Übertragung durch die Polizei (§ 59 PolG) wahrzunehmender „originärer" polizeilicher Aufgaben gleichzusetzen ist. Es handelt sich vielmehr um dem Grunde nach nicht-polizeiliche Aufgaben, die lediglich von einer Polizeibehörde wahrgenommen werden.

Die völlige Verkennung der polizeirechtlichen Befugnisse sowie das Beharren hierauf trotz entsprechender Hinweise durch unsere Behörde veranlasste uns, die Datenverarbeitung zu beanstanden. Die Stellungnahme des Innenministeriums hierzu steht noch aus.

Polizei und SARS-CoV-2 oder: Schau mal, der Zeppelin!

Das Coronavirus SARS-CoV-2 beflügelt nicht nur Gesundheitsbehörden bei der Suche nach Maßnahmen, um die Pandemie einzudämmen. Auch die Polizei entdeckt dabei mitunter ihre kreativen Seiten. So wurden wir von einem Bürger darauf aufmerksam gemacht, dass ein Polizeipräsidium zur Überwachung der Corona-Regeln einen Zeppelin einsetzte. Begründung unter anderem: Ein Zeppelin eigne sich „wegen seines leisen Flugs besonders für eine derartige Mission". Wenn die Polizei auf Mission ist und dabei möglichst unbemerkt bleiben will, ist das für uns immer Anlass,

genauer hinzuschauen. Der Verdacht lag nahe, dass hier mittels verdeckter Maßnahmen personenbezogene Daten erhoben wurden – weswegen wir deren Rechtmäßigkeit prüften. Unsere Nachfrage beim zuständigen Polizeipräsidium erbrachte Folgendes:

Um die Osterzeit 2020 steuerte die Belegung der Krankenhäuser im Zuständigkeitsbereich des Polizeipräsidiums auf einen kritischen Punkt zu. Gleichzeitig bestand aufgrund des guten Wetters eine gewisse Wahrscheinlichkeit, dass sich Bürger_innen vermehrt nicht an die Corona-Regeln halten und Ansammlungen bilden würden. Als der Polizei angeboten wurde, in einem Zeppelin mitzufliegen, der von einer Gemeinde für eine Kampagne gechartert worden war, nahm man dies dankend an. Von Karfreitag bis Ostermontag flogen darauf Polizeibeamte mit, die aus circa 300 Meter Höhe mittels Fotokameras Aufnahmen vom Geschehen am Boden fertigten und Bodenstreifen verständigten, wenn der Verdacht bestand, dass sich mehr als die zulässige Höchstzahl an Personen im öffentlichen Raum aufhielten.

Vom Polizeipräsidium ließen wir uns insbesondere genau erklären, was es mit den Aufnahmen auf sich hatte. So ganz klar wurde uns das letztlich nicht. In seiner Stellungnahme gab das Polizeipräsidium an, dass es sich lediglich um Übersichtsaufnahmen gehandelt habe, die beim Zoomen so stark verpixelt seien, dass eine Identifizierung der abgebildeten Personen nicht möglich sei. Dem entsprechend seien Ordnungswidrigkeitsverfahren auch nicht auf der Grundlage der Fotoaufnahmen, sondern nach Herbeiführen der Bodenkräfte aufgrund deren Feststellungen unmittelbar vor Ort eingeleitet worden. Dies unterstellt, läge kein datenschutzrechtlich relevanter Sachverhalt vor. Gewisse Zweifel waren jedoch angebracht.

So stand etwa im Einsatzbefehl, dass festgestellte Verstöße insbesondere durch Fertigung von Lichtbildern zu sichern seien. Außerdem waren die uns vorgelegten Bilder bei Weitem nicht so unscharf, als dass man mit entsprechenden Zusatzinformationen, die zu beschaffen der Polizei sicher ein Leichtes gewesen wäre, nicht doch einzelne Personen hätte identifizieren können.

Letztlich konnten wir aber nicht mit der nötigen Eindeutigkeit feststellen, dass die Polizei hier datenschutzwidrig gehandelt hat. Wir haben die Sache deshalb auf sich beruhen lassen. Sollte jedoch die Absicht bestehen, eine solche Aktion zu wiederholen, wäre die Polizei gut beraten, im Vorhinein gründlich zu prüfen, ob bzw. unter welchen Rahmenbedingungen hierfür eine Berechtigung besteht. Und uns gegebenenfalls vorher zu befragen.

Die Corona-Verordnungen „Datenverarbeitung“ und „Datenverarbeitung im Auftrag“

Im Frühjahr 2020 zeigte sich, dass der Polizeivollzugsdienst und einige andere Behörden und Institutionen (wie insbesondere Feuerwehr und Rettungsdienst) ein großes Interesse daran hatten zu erfahren, wer nach Kenntnis der Gesundheitsbehörden mit dem neuartigen Coronavirus SARS-CoV-2 infiziert war. Geltend gemacht wurde insoweit nicht nur, dass sich die Einsatzkräfte bei Kontakt mit positiv Getesteten besonders schützen müssten, sondern auch, dass der Polizeivollzugsdienst zur Überwachung von Quarantänemaßnahmen und anderen Anordnungen der Gesundheitsbehörden zuständig sei. Teilweise erfuhren wir, dass die Gesundheitsämter und Ortspolizeibehörden regelmäßig Listen der jeweils aktuell positiv Getesteten oder Infektionsverdächtigen dem Polizeivollzugsdienst übermittelten. Ebenso drängten die Ortspolizeibehörden darauf, von den Gesundheitsämtern auch dann zu erfahren, wer ein positives Testergebnis erhalten hatte, wenn das Gesundheitsamt eine förmliche Quarantänemaßnahme nicht für geboten hielt, weil die getestete Person sich nach Einschätzung des Gesundheitsamts glaubhaft freiwillig in häusliche Absonderung begab.

Hiergegen schritt das Sozialministerium ein. Mit Erlass vom 26. März 2020 (Az.: 51-1443.4 SARS-Cov2) stellte es in Abstimmung mit uns klar, dass Übermittlungen gemeldeter personenbezogener Daten von Gesundheitsämtern an Ortspolizeibehörden dann unzulässig seien, wenn die Gesundheitsämter selbst keine ortspolizeilichen Maßnahmen i. S. v. §§ 16, 28 ff. IfSG vorschlagen bzw. aufgrund von Gefahr im Verzuge selbst angeordnet haben. Eine Datenübermittlung an andere Organisationen, beispielsweise den Polizeivollzugsdienst, die Feuerwehr oder den Rettungsdienst sei nicht zulässig. Insbesondere komme weder eine pauschale Datenübermittlung von sensiblen Gesundheitsdaten nach Gesundheitsdienstgesetz in Betracht noch lasse sich den Regelungen des Infektionsschutzgesetzes eine Befugnis zur Datenübermittlung an die genannten Institutionen entnehmen. Auch könne die Übermittlung nicht damit gerechtfertigt werden, dass

diese zum Selbstschutz der im Einsatz befindlichen Personen erforderlich sei. Es sei vielmehr angesichts der allgemein hohen Ansteckungsgefahr nicht erkennbar, dass im Rahmen von Einsätzen bei einer bekanntermaßen infizierten Person eine weitergehende Schutzausrüstung erforderlich wäre, als im Rahmen von Einsätzen bei Personen, deren Infektionsstatus unbekannt sei.

Dieser Argumentation setzte das Innenministerium entgegen, dass sie die Kenntnis des Polizeivollzugsdienstes von positiv Getesteten für unentbehrlich halte. Denn wenn Informationen über den Verdacht auf eine Covid-19-Infektion bei Fremdpersonen vorlägen, würden die Polizeibeamt_innen – neben dem Verzicht auf engen Körperkontakt – aus Gründen des Infektionsschutzes vor dem Erstkontakt eine persönliche Schutzausstattung anlegen, die eine FFP2-Maske und Einmalhandschuhe umfasse, unter Umständen auch eine Mund-Nasen-Maske sowie zusätzlich einen Schutzoverall sowie eine Schutzbrille. Bestehe kein Verdacht auf eine Covid-19-Infektion würden von den eingesetzten Polizeibeamt_innen – auch um die vorhandene Verunsicherung in der Bevölkerung nicht zu erhöhen und um Bürgernähe zu vermitteln – lediglich die allgemeinen Hygienemaßnahmen im Umgang mit den Bürger_innen beachtet (möglichst das Einhalten des empfohlenen Mindestabstandes von 1,5 Meter, Desinfektion der Hände nach Beendigung der Maßnahme). Im Übrigen werde der Polizeivollzugsdienst bei Gefahr im Verzug sowie in Amts- und Vollzugshilfe ebenfalls im Rahmen von Maßnahmen nach dem Infektionsschutzgesetz tätig und benötige auch aus diesem Grund die Kenntnis über den Status Infizierter.

Zur Lösung dieses Konflikts beschlossen die beiden beteiligten Ministerien nach Beratung durch unsere Dienststelle, auf der Grundlage einer Verordnung nach § 32 IfSG ein Abrufsystem für den Polizeivollzugsdienst einzurichten, durch das der Polizeivollzugsdienst unter genau geregelten Voraussetzungen im konkreten Einzelfall abfragen kann, ob das Gesundheitsamt oder die Ortspolizeibehörde gegen eine bestimmte Person auf der Grundlage eines positiven Testergebnisses aktuell eine Maßnahme nach dem Infektionsschutzgesetz angeordnet hat.

Bei der Ausgestaltung dieser Verordnung unterstützten wir die beteiligten Ministerien nach Kräften, weil wir darin die Chance sahen, die Praxis der Übermittlung von ganzen Listen Infizierter und Infektionsverdächtiger einzuschränken und zu kanalisieren. Zugleich drängten wir darauf, auch die Ortspolizeibehörden in das (sichere) Übermittlungssystem einzubeziehen und zu bestimmen, dass die Übermittlung mittels dieses Systems alle anderen Übermittlungsformen ausschließt. Auf diese Weise sahen wir im Interesse des Datenschutzes die Möglichkeit, dass der bis dahin nach unserer Kenntnis bestehende Wildwuchs an Übermittlungsformen zwischen Gesundheitsamt und der für den Infektionsschutz grundsätzlich zuständigen Ortspolizeibehörde, die beispielsweise per Fax oder ungesicherter E-Mails kommunizierten, durch eine sichere Übermittlungsform ersetzt werden könnte.

Dabei sollte das Landesgesundheitsamt das System als „Datenverarbeiter im Auftrag“ für die Gesundheitsämter und die Ortspolizeibehörden tätig werden. Damit nicht jedes Gesundheitsamt und jede Ortspolizeibehörde mit dem Landesgesundheitsamt hierfür einen Vertrag zur Auftragsverarbeitung abschließen müsste, rieten wir zu prüfen, ob die Landesregierung von der Möglichkeit aus Artikel 28 Absatz 3 DS-GVO Gebrauch machen und die Bestimmungen zur „Datenverarbeitung im Auftrag“ durch eine Rechtsverordnung als „anderes Rechtsinstrument“ festlegen könne. Bei der Formulierung der entsprechenden Corona-Verordnung „Datenverarbeitung im Auftrag“ standen wir sodann wieder mit Rat und Tat zur Seite. Es zeigte sich einmal mehr: Bei kluger Anwendung eröffnet die DS-GVO durchaus praktikable Lösungen.

Auch bei der anschließenden Einrichtung des Abrufverfahrens unterstützten wir das Landesgesundheitsamt bei vielen aufkommenden Einzelfragen. Nach dem zu urteilen, was uns von Seiten der Gesundheitsämter zugetragen wird, hat sich das vielfach so genannte „Quarantäneregister“ insbesondere mit Blick auf die Kommunikation zwischen den Gesundheitsämtern und den Ortspolizeibehörden bei der Bewältigung der Pandemie zwar nicht als perfekt, aber als durchaus hilfreich erwiesen. Vielfach wird sogar sein Ausbau um weitere Funktionalitäten und Schnittstellen für sinnvoll erachtet.

>> Weitere Informationen
Corona-Verordnung „Datenverarbeitung“

https://www.baden-wuerttemberg.de/de/service/aktuelle-infos-zu-corona/corona-verordnung-datenverarbeitung/#:~:text=Verordnung%20des%20Sozialministeriums%20und%20des%20Innenministeriums%20zur%20Verarbeitung,Datenverarbeitung%20%E2%80%93%20CoronaVO%20Datenverarbeitung%29%20vom%204.%20Mai%202020

1.5 Datenschutz bei Corona-Testzentren

„Übersicht Corona-Tests: Behalten Sie den Durchblick!“ Diese Ankündigung im Internetangebot der Kassenärztlichen Vereinigung Baden-Württemberg (KVBW) klingt vielversprechend, wenn man bedenkt, dass es seit dem Anstieg der Zahlen von Covid-19-Infektionen im Frühjahr 2020 ein breit gefächertes Angebot unterschiedlicher Anlaufstellen zur Durchführung von Corona-Tests gibt: Mit ein paar Mausklicks können sich etwa Reiserückkehrende oder Patienten mit Verdacht auf eine Corona-Infektion auf der interaktiven Karte der KVBW die verschiedenen in Baden-Württemberg eingerichteten Teststationen anzeigen lassen, welche diese (mit-)organisiert. Wer sich ebenso leicht zugängliche Antworten auf die Fragen erhofft, wer für die Verarbeitung der durch den Test erhobenen sensiblen Daten verantwortlich ist, an wen die erhobenen Daten weitergeleitet werden, was mit den Teströhrchen und mit dem gleichzeitig erhobenen Genmaterial passiert, der wird indes enttäuscht.

Nachdem uns das Coronavirus SARS-CoV-2 nun schon seit vielen Monaten belastet und uns wohl auch noch eine ganze Zeit lang verfolgen wird, können wir Nachlässigkeiten beim Datenschutz, die mit überlasteten Kapazitäten und der Ausnahmesituation begründet werden, nicht länger hinnehmen. Insbesondere bei der Transparenz und bei der Art und Weise der Übermittlung von Befundmitteilungen sehen wir erheblichen Nachbesserungsbedarf.

Die KVBW wandte sich im März 2020 an uns, als während der ersten Pandemiewelle vermehrt Testungen durchgeführt werden mussten und erkennbar wurde, dass die vorhandenen Kapazitäten im Bereich des öffentlichen Gesundheitsdienstes und im vertragsärztlichen Bereich hierfür nicht ausreichten. Die KVBW beabsichtigte, zur Entlastung der bestehenden Test-Infrastruktur die negativen Testergebnisse durch eigene nicht-ärztliche Mitarbeitende der KVBW oder durch Mitarbeitende aus den Notfallpraxen zu übermitteln. Die hiermit verbundene Verarbeitung der mit dem Abstrich erhobenen Gesundheitsdaten sollte auf Grundlage einer Einwilligung der zu Testenden erfolgen.

Wir berieten die KVBW bei der konkreten Ausgestaltung der Einwilligungserklärung. Dabei war ebenfalls Gegenstand unserer Beratungen, inwieweit sichergestellt werden könne, dass die Einwilligung in eine Datenverarbeitung durch nicht-ärztliches Personal der KVBW auch freiwillig erfolgte. Wir wiesen darauf hin, dass die zu Testenden spätestens im Zeitpunkt der Abstrichentnahme über diese Tatsache informiert werden müssten, um sich dann gegebenenfalls noch dafür entscheiden könnten, den Corona-Test alternativ bei einem niedergelassenen Hausarzt machen zu können.

Um nach den Sommerferien ab August 2020 zusätzlich zu den Verdachtsfällen auch die Personengruppen der Reiserückkehrenden, der Lehrerschaft und von Erzieher_innen auf das Coronavirus SARS-CoV-2 testen zu können, etablierte die KVBW nach eigenen Angaben im Auftrag des Landes Baden-Württemberg und teilweise zusammen mit anderen Akteuren des Gesundheitsbereichs viele zusätzliche Corona-Abstrichstellen an Verkehrsknotenpunkten wie Flughäfen, Bahnhöfen und Autobahnraststätten. Laut KVBW seien die hierin involvierten Ärzt_innen zu diesem Zeitpunkt nicht in der Lage gewesen, bei bis zu 2000 Abstrichen am Tag jeweils mit dem Patienten Kontakt aufzunehmen, um ihnen den Befund mitzuteilen.

Vor diesem Hintergrund wandte sich die KVBW erneut an uns insbesondere mit der Frage, ob den Getesteten der Befund nicht nur telefonisch oder per Post, sondern alternativ auf Grundlage einer Einwilligung auch per E-Mail mitgeteilt werden könnte. Wir hatten das Anliegen der KVBW im Kern wie folgt verstanden: Das Ziel, trotz der massenhaften Testungen den getesteten Patienten möglichst zeitnah ihr Testergebnis mitteilen zu können, könne nach Einschätzung der KVBW nur dann erreicht werden, wenn das Gros der Testergebnisse rasch per E-Mail übermittelt würde.

Wir wiesen die KVBW in unserer Antwort darauf hin, dass es nicht mit dem datenschutzrechtlichen Grund-

satz der Integrität und Vertraulichkeit (vgl. Artikel 5 Absatz 1 Buchstabe f DS-GVO) vereinbar ist, dass personenbezogene (Gesundheits)Daten per nicht Ende zu Ende verschlüsselter E-Mail übermittelt werden. Unserer Rechtsauffassung zufolge kann auf die jeweils angemessene Sicherheit der Verarbeitung grundsätzlich nicht, auch nicht in Form einer schriftlichen „Einwilligung", verzichtet werden. Dies haben wir auch in der Vergangenheit in Erörterungen diesbezüglich mit dem Datenschutzbeauftragten der KVBW immer gesagt: Nicht Ende zu Ende verschlüsselte E-Mails sind für die Kommunikation über Gesundheitsdaten nicht ausreichend sicher. Aber, und das haben wir als Ausnahmeregelung vorgeschlagen, um das Verfahren datenschutzkonform zu beschleunigen in Anbetracht der Notsituation: Die zu testenden Patienten könnten ausnahmsweise zum Zweck der Übermittlung des negativen Testergebnisses auf die Sicherheit der Datenverarbeitung schriftlich verzichten. Auf dieser Grundlage könne den Patienten ein negatives Testergebnis auch per E-Mail übermittelt werden. Bei positiven Testergebnissen müsste, so die nicht ausreichend verschlüsselte Mail die Alternative sei, weiterhin die telefonische oder postalische Übermittlung stattfinden. Diese Gestaltungsmöglichkeit war an die Bedingung geknüpft, uns eine ausgearbeitete Datenschutzerklärung zukommen zu lassen, welche sämtliche Informationen des Artikels 13 der DS-GVO beinhaltete (sie dient der Transparenz der Datenverarbeitung nach Artikel 5 Absatz 1 Buchstabe a DS-GVO).

Nach der Regelung des Artikels 13 DS-GVO teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung von personenbezogenen Daten unter anderem den Namen und die Kontaktdaten des Verantwortlichen, die Rechtsgrundlage für die Verarbeitung, gegebenenfalls die Empfänger der personenbezogenen Daten und die Dauer, für welche die personenbezogenen Daten gespeichert werden, mit.

Die hohe praktische Relevanz der Informationspflichten des Verantwortlichen zeigt sich ganz deutlich daran, dass sich Betroffene aus datenschutzrechtlicher Sicht eine ganze Reihe von Fragen stellten und sich nach wie vor stellen; hier eine Auswahl:

- Wer ist für die Datenverarbeitung verantwortlich? Das Land Baden-Württemberg, die KVBW, das Abstrich entnehmende Personal oder etwa die die Befunde auswertenden Labore?

© Daniel Beckemeier – stock.adobe.com

Wer sich testen lässt, muss wissen, wer seine sensiblen Daten erhält und was mit dem gleichzeitig erhobenen Genmaterial passiert.

- Wie lange werden die erhobenen Kontaktdaten gespeichert?
- Wie sind die Datenlöschung und deren Überwachung festgelegt?
- Erhalten außer den Gesundheitsämtern und den Testlaboren noch andere Dritte diese Daten?
- Was passiert mit den Teströhrchen und insbesondere mit dem gleichzeitig erhobenen Genmaterial?
- Wie erfolgt deren Vernichtung und wer überwacht das?
- Werden genetische Auswertungen gemacht und mit den Personendaten verknüpft?

Den zu Testenden müssen in jedem Fall die in Artikel 13 DS-GVO vorgesehenen Informationen mitgeteilt werden. Darüber hinaus wäre es mehr als wünschenswert, wenn auch alle weiteren Fragen, die in diesem Kontext gestellt werden, in einer Datenschutzerklärung transparent und verständlich erläutert würden. Zu den verpflichtend mitzuteilenden Informationen gehört die Frage der Verantwortlichkeit, welche Ausgangspunkt jeder datenschutzrechtlichen Prüfung ist und in Artikel 13 Absatz 1 Buchstabe a DS-GVO auch zuerst benannt ist.

Angesichts der undurchsichtigen Landschaft unterschiedlicher Abstrichstellen in Baden-Württemberg, an denen Akteure des Gesundheitswesens mitwirken, stellt sich diese Frage zu Recht. Auf das Coronavirus SARS-CoV-2 kann man sich laut Internetseite der KVBW testen lassen in ausgewiesenen Corona-Schwerpunktpraxen, in eigens eingerichteten Fieberambulanzen und Test-/Abstrichzentren, in Corona-Radiologie-Praxen bis hin zu mobilen Corona-Teststationen. Die interaktive Karte auf der Homepage der KVBW enthält zwar eine farblich gekennzeichnete Aufzählung der verschiedenen Anlaufstellen, teilweise differenziert nach Personen, die Symptome aufweisen und solchen, die (noch) keine Symptome aufweisen. Diese Differenzierung hilft jedoch nicht weiter mit Blick auf die Frage, wer aus datenschutzrechtlicher Sicht die verantwortliche Stelle ist.

Laut eines Berichts des Staatsanzeigers hat die Landesregierung in Zusammenarbeit mit der KVBW, dem Deutschen Roten Kreuz (DRK) und dem Technischen Hilfswerk (THW) die Corona-Testzentren eingerichtet. Doch selbst bei Kenntnis aller mitwirkenden Akteure wird anhand der folgenden Beispiele deutlich, dass für Patienten mitnichten klar ist, an welchen der Beteiligten sie sich mit ihren Fragen zum Datenschutz wenden können und in welchem Verhältnis diese zueinander stehen.

Bei der vom Sozialministerium eröffneten und von der KVBW mitbetriebenen Teststation am Hauptbahnhof Stuttgart nahmen Mitarbeitende des Deutschen Roten Kreuzes Reiserückkehrern den Abstrich ab, am Flughafen Stuttgart wiederum führen offenbar Mitarbeiter der KVBW die Tests durch. Den Patienten mit Verdacht auf eine Covid-19-Infektion testet hingegen der niedergelassene Arzt der Corona-Schwerpunktpraxis auf den Virus. Welcher dieser Akteure für den Betrieb der Corona-Testzentren verantwortlich ist, bleibt unklar. Letztlich kann jedoch nur ein Patient, der Zugang hat zu den Informationen, wer welche Daten in welcher Art und Weise von ihm verarbeitet, selbstbestimmt darüber entscheiden, ob und gegebenenfalls welche Teststation (seines Vertrauens) er ansteuert.
Leider hat uns die KVBW trotz mehrmaliger Aufforderung bis zum Redaktionsschluss dieses Beitrags keine entsprechenden Datenschutzerklärungen vorgelegt. Ebenso wenig ist bislang unsere Nachfrage beantwortet worden, inwiefern und bis wann die KVBW beabsichtigt, angesichts der auf unabsehbare Zeit fortdauernden Corona-Pandemie bei der Mitteilung der Befunde auf eine datenschutzkonforme Lösung, beispielsweise auf den Abruf über ein Webportal, umzustellen. Die Befundmitteilung per passwortgeschütztem pdf-Dokument, welche nach unseren letzten Informationen der KVBW aktuell praktiziert werde, erfüllt jedenfalls nicht die rechtlichen Vorgaben an die Datensicherheit. Die KVBW muss in diesen Punkten dringend nachbessern.

Wichtige Voraussetzungen dafür, dass dies gelingt, sind jedoch zunächst einmal, dass der Informationsfluss mit unserer Behörde deutlich verbessert wird; des weiteren muss auch innerhalb der KVBW ihr eigener behördlicher Datenschutzbeauftragter (DSB) ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden; schließlich muss der interne DSB sodann alle für die Erfüllung seiner Aufgaben erforderlichen Ressourcen und den Zugang zu Daten und Verarbeitungsvorgängen erhalten. Dies war nach unserem Eindruck im Zusammenhang mit den Corona-Testzentren leider nicht der Fall. Für die KVBW besteht daher dringender Handlungsbedarf.

1.6 Die Digitalisierung des (öffentlichen) Gesundheitswesens zur Pandemiebekämpfung

Die Corona-Pandemie offenbarte einen erheblichen Digitalisierungsbedarf des öffentlichen Gesundheitsdienstes. Die Übermittlung von Meldungen nach §§ 6 ff. des Infektionsschutzgesetzes (IfSG) an die Gesundheitsämter erfolgte vielfach noch per Fax, den Gesundheitsämtern standen kaum Tools zur sicheren Kommunikation mit Bürger_innen (z. B. zur Abfrage von Kontakten im Falle positiver Testergebnisse) und mit Einrichtungen wie Krankenhäusern, Alten- und Pflegeheimen, Schulen und Kindergärten zur Verfügung.

Für die Kommunikation zwischen Gesundheitsämtern und Ortspolizeibehörden sowie dem Polizeivollzugsdienst konnte mit dem auf der Grundlage der Corona-Verordnungen „Datenverarbeitung und Datenverarbeitung im Auftrag" geschaffenen Bereitstellungs- und Abrufverfahren, dem sogenannten „Quarantäne-Register", bei dessen Einführung wir beratend zur Seite standen (siehe Hinweis „Die Corona-Verordnungen Datenverarbeitung und Datenverarbeitung im Auftrag" in Kap 1.4) eine deutliche Verbesserung erzielt werden. Darüber hinaus gab es mehrere Initiativen mit dem Ziel, die Arbeitsabläufe bei den Gesundheitsämtern durch Digitalisierungstools zu verbessern. Wir haben hier verschiedentlich versucht, mit Rat und Tat zur Seite zu stehen, um eine rechtzeitige Berücksichtigung der datenschutzrechtlichen Anforderungen in diesem sensiblen Bereich sicherzustellen. Leider waren einige dieser Initiativen nicht erfolgreich; vielfach wurden datenschutzrechtliche Belange nicht frühzeitig mitbedacht oder nicht mit den erforderlichen Ressourcen verfolgt.

Die Datenplattform der Björn-Steiger-Stiftung – digitale Ablösung der analogen Arbeit der Gesundheitsämter in der Corona-Pandemie?

Als im Frühjahr 2020 durch den Anstieg der Corona-Infektionszahlen die Gesundheitsämter große Mühe hatten, die Infektionsketten händisch und analog im Einzelnen nachzuverfolgen, hatte sich die in Winnenden ansässige Björn-Steiger-Stiftung, eine Stiftung des bürgerlichen Rechts mit dem Zweck, die Notfallhilfe in Deutschland zu verbessern, ein ehrgeiziges Ziel gesetzt: Sie beabsichtigte, eine digitale Plattform zu entwickeln, über die sämtliche in einer Pandemie typischerweise beteiligten Akteure des Gesundheitswesens – vom Patienten zu den Ärzten über Anlaufstellen wie die Telefonseelsorge oder Ärztlichem Bereitschaftsdienst, den Gesundheitsämtern, den Kassenärztlichen Vereinigungen, den Corona-Testzentren, bis hin zum Robert-Koch-Institut (RKI) – miteinander vernetzt werden sollten. Über diese digitale Plattform sollten notwendige Informationsflüsse zwischen diesen Beteiligten beschleunigt werden. Potentiell Covid-19-Erkrankten sollte diese Plattform außerdem die Möglichkeit bieten, ihr Risiko, sich infiziert zu haben, schnell einschätzen zu können und erforderlichenfalls einen raschen Zugang zu einem Testzentrum in der Nähe erhalten.

Die Stiftung hatte sich März 2020 zunächst an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) in Bonn gewandt mit der Bitte um datenschutzrechtliche Prüfung dieser Konzeptidee. Auch die Bremer Landesbeauftragte für den Datenschutz war mit der Prüfung dieser Projektidee befasst, da die Stiftung erstmals in Bremen mit der Plattform an den Start gehen wollte. Da die Stiftung in Baden-Württemberg ihren Sitz hat, waren im weiteren Verlauf gleichermaßen auch unsere Beratungen und Expertise gefragt. Die Stiftung beabsichtigte, bereits Ende März/Anfang April 2020 den Echtbetrieb zu testen und so drängte sie, ihre Konzeptidee rasch zu prüfen.

Grundlage unserer Prüfung waren verschiedene Präsentationsfolien sowie eine Anlage mit der Datenschutzerklärung und dem Mustertext für die Einwilligung. Anfang April 2020 teilten wir der Björn-Steiger-Stiftung schließlich mit, dass wir in Bezug auf das Projekt in der uns aktuell dargelegten Ausgestaltung sowohl in datenschutzrechtlicher als auch in technischer Sicht erhebliche Bedenken hatten. Wir rieten dringend dazu, diese Bedenken auszuräumen, bevor das Projekt in den Echtbetrieb geht.

Die Unterlagen vermittelten uns im Ergebnis den Gesamteindruck, dass die Stiftung mit dieser Plattform als Verantwortliche zusammen mit sämtlichen in Betracht kommenden Akteuren des Gesundheitswesens – von den etablierten Akteuren bis hin zu sich spontan formierenden Akteuren (Stichwort: Testzentren) – während der auf unbestimmte Zeit andauernden Corona-Pandemie potentiell sämtliche personenbezogene (Gesundheits-)Daten erheben, speichern, auswerten und übermitteln können sollte. Eine derart weit verzweigte, unbestimmte und sich jederzeit in ihrer

Form potentiell veränderbare Datenverarbeitung hielten wir für datenschutzrechtlich unzulässig und für einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung.

Es gab zu der Plattform im Einzelnen aus unserer Sicht viele ungeklärte Fragen, insbesondere Folgende:

- Wer sind die verantwortlichen Stellen bei dieser Plattform?
  Die Björn-Steiger-Stiftung selbst, die Gesundheitsämter und/oder das Robert-Koch-Institut?
- Welche Rolle spielen aus datenschutzrechtlicher Sicht die anderen beteiligten Akteure wie das Software-Unternehmen als Betreiber der Plattform, die Abstrich nehmenden Ärzte, Anlaufstellen wie die Telefonseelsorge oder die Labore, welche die Tests auswerten?
- Welche Stelle übermittelt dem Patienten das Testergebnis? Das Testzentrum (wer ist das genau?) oder das örtlich zuständige Gesundheitsamt?
- Auf welcher/welchen Rechtsgrundlage/n verarbeitet die Björn-Steiger-Stiftung die personenbezogenen Daten der Patienten?
- Ist die Benachrichtigung über positive sowie negative Testergebnisse via E-Mail oder SMS vorgesehen?
- Ist es zulässig, dass über den Zugang zum Corona-Test ausschließlich ein Algorithmus entscheiden soll?
- Erfolgt eine Verschlüsselung der Daten auf den Servern?
- Ist bei der Übermittlung der Daten eine ordentliche Transportverschlüsselung vorgesehen?
- Ist die Speicherung der personenbezogenen Daten bei privaten (Cloud-)Anbietern zulässig?

Besonders problematisch erschienen uns hieraus die folgenden Aspekte, auf die wir die Stiftung hinwiesen: Für die von ihr zunächst favorisierte Lösung, dass die Stiftung selbst verantwortlich sein sollte, kam als mögliche Rechtsgrundlage nur eine Einwilligung in Betracht. Die Björn-Steiger-Stiftung als eingetragener Verein privaten Rechts kann sich offensichtlich nicht auf dieselben Rechtsgrundlagen stützen wie hoheitliche Beteiligte des Gesundheitswesens, z. B. das örtliche Gesundheitsamt, oder etwa ein von einem Klinikum betriebenes Testzentrum. Die Stiftung zählt, anders als ein Gesundheitsamt, gerade nicht zum Kreis der nach dem Infektionsschutzgesetz (IfSG) Meldepflichtigen und kann sich folglich auch nicht auf § 8 IfSG stützen.

Generell ist es jedoch problematisch, bei der Datenverarbeitung im Rahmen der öffentlichen Gesundheitsversorgung auf eine Einwilligung des Patienten zurückzugreifen. In jedem Fall muss eine Versorgung auch solcher Patienten sichergestellt werden, die eine solche Einwilligung nicht erteilen wollen.

Wir wiesen darauf hin, dass es möglicherweise günstiger sein könnte, wenn die Björn-Steiger-Stiftung Auftragsverarbeiterin für das jeweilige Gesundheitsamt wäre, so dass das Gesundheitsamt die Datenerhebung dann aufgrund gesetzlicher Aufgabenzuweisung (§ 25 IfSG) vornehmen würde. Ein solches Konstrukt bedingt jedoch, dass erforderliche Verträge zur Auftragsverarbeitung (Artikel 28 der Datenschutz-Grundverordnung, DS-GVO) vor dem Betrieb abgeschlossen sein müssten. Solche Verträge wurden uns im weiteren Verlauf nicht vorgelegt.

Es stieß ferner auf wesentliche Bedenken, wenn über den Zugang zum Test ausschließlich ein Algorithmus (bzw. künstliche Intelligenz) anstelle einer Einschätzung bzw. einer Diagnose durch einen Arzt entscheiden soll. Wir konnten insoweit nicht erkennen, dass der Betrieb der Plattform die Vorgaben des Artikels 22 DS-GVO einhält.

Die Benachrichtigung über Testergebnisse via E-Mail oder SMS ist problematisch. Die Benachrichtigung lässt auch dann, wenn das Testergebnis negativ ist, unter Umständen Rückschlüsse auf den Gesundheitszustand des Betroffenen zu. Hier sind besondere technische und organisatorische Maßnahmen zu treffen, um sicherzustellen, dass es nicht zu Fehlübermittlungen kommt und die Korrespondenz nicht von Unberechtigten eingesehen werden kann. Die Versendung von Gesundheitsdaten per E-Mail an andere Verantwortliche (Gesundheitsämter, RKI, Ärzte, Labore etc.) darf ausschließlich per Ende-zu-Ende-Verschlüsselung nach aktuellem Standard stattfinden.

Im Übrigen fehlten uns für eine genauere Prüfung neben der erforderlichen Datenschutzfolgenabschätzung ebenfalls das Sicherheitskonzept, das Löschkonzept sowie die Schnittstellenbeschreibung, die uns allesamt nicht zur Prüfung vorgelegt worden sind. Somit blieben im Ergebnis viele der oben aufgeworfenen Fragen unbeantwortet.

Schließlich erfuhren wir wenige Wochen später, dass die Plattform der Björn-Steiger-Stiftung in Bremen

politisch gescheitert war und das Projekt nicht weiter verfolgt werden sollte.

Die Software SORMAS des Helmholtz-Instituts zur Kontaktnachverfolgung

Mitte Mai 2020 wandte sich das Landesgesundheitsamt (LGA) an uns: Zur Vereinfachung und Verbesserung der Kontaktnachverfolgung bei der Bekämpfung der Verbreitung des Coronavirus SARS-Cov-2 durch die Gesundheitsämter – auch über die örtlichen Zuständigkeitsgrenzen der Gesundheitsämter hinweg – werde die landesweite Einführung der Software SORMAS („Surveillance Outbreak Response Management and Analysis System") für den Öffentlichen Gesundheitsdienst in Erwägung gezogen. Hierzu bat das Landesgesundheitsamt uns um eine datenschutzrechtliche Beratung. Dabei beruhte die Intention zur Einführung von SORMAS, wie wir später erfuhren, auf einem entsprechenden Beschluss der Lenkungsgruppe „SARS-CoV-2 (Coronavirus)" der Landesregierung von Anfang Mai 2020.

Das System SORMAS wurde – nach Internet-Informationen des Helmholtz-Zentrum für Infektionsforschung (HZI) in Braunschweig – zusammen mit dem Robert-Koch-Institut und einigen weiteren Institutionen ursprünglich 2014 im Zuge des Westafrikanischen Ebola-Ausbruchs entwickelt und kam anschließend bereits bei der Bekämpfung verschiedener Epidemien in afrikanischen Staaten zum Einsatz. Die Variante SORMAS-ÖGD sei sodann vom HZI speziell für die Bedürfnisse des öffentlichen Gesundheitsdienstes (ÖGD) in Deutschland angepasst, um ein effektives Kontaktpersonenmanagement während der SARS-CoV-2-Pandemie zu ermöglichen.

Für die Zwecke unserer Beratung stellte uns das LGA zunächst nur den Entwurf des für SORMAS-ÖGD zu verwendenden Auftragsverarbeitungsvertrages mit der Software-Firma und verschiedene Links zu Internet-Informationen über SORMAS zur Verfügung.

Wir wiesen sogleich darauf hin, dass diese Informationen zur datenschutzrechtlichen Beurteilung nicht ausreichend seien. Zu den erforderlichen Unterlagen würden insbesondere folgende gehören:

- eine schematische Darstellung, welche personenbezogenen Daten durch den Einsatz der Software auf welche Weise verarbeitet werden sollen, möglichst auch unter Angabe einer eigenen Einschätzung, auf welcher Rechtsgrundlage dies geschehen soll,
- das vorgesehene Datensicherheitskonzept,
- etwaige Auftragsdatenverarbeitungsverträge im Entwurf,
- die beabsichtigte Ergänzung des Verarbeitungsverzeichnisses im Entwurf,
- die vorgesehenen Informationen nach Artikel 13 und 14 DS-GVO im Entwurf
- und idealerweise eine Datenschutzfolgenabschätzung im Entwurf.

In Absprache mit dem LGA wandten wir uns auch an das Sozialministerium, um möglichst eine Beschleunigung bei der Beschaffung der erforderlichen Unterlagen zu bewirken. Außerdem nahmen wir im Rahmen des Arbeitskreises Gesundheit und Soziales der Datenschutz-Konferenz Kontakt zu den anderen deutschen Datenschutzbehörden auf, um in Erfahrung zu bringen, ob bei diesen bereits weitere Informationen und eigene Beurteilungen vorlägen, wodurch wir viele nützliche Hinweise von den Kolleg_innen erhielten.

Ende Mai konnte uns das LGA weitere Unterlagen des HZI zukommen lassen, wobei allerdings bereits die eigene Datenschutzbeauftragte des LGA bei ihrer Prüfung – zu Recht – zu dem Ergebnis gekommen war, dass noch wesentliche Teile fehlten.

Wir forderten detailliert die fehlenden Informationen an und rügten bereits anhand der uns zugänglichen Unterlagen feststellbare Mängel, wie z. B. die Lückenhaftigkeit des vorgelegten Dokuments zur Datensicherheit insbesondere mit Blick auf die Angaben zu den technischen und organisatorischen Maßnahmen, die Verwendung schwacher „Cipher Suites" und veralteter Protokolle, Widersprüche in der Risikoanalyse und zahlreiche Mängel des als Muster überlassenen Auftragsdatenverarbeitungsvertrages. Ferner wiesen wir darauf hin, dass das HZI auf seinen Internetseiten davon spricht, dass das System eine DS-GVO-Zertifizierung habe, obwohl ein Verfahren für eine solche Zertifizierung gar nicht existiert. Vor allem machten wir deutlich, dass die erwogene Variante, das System bei landesweitem Einsatz für alle Gesundheitsämter zentral beim LGA zu führen, datenschutzrechtlich nicht zulässig wäre, weil das LGA dann mehr personenbezogene Informationen erhalten würde als im Infektionsschutzgesetz des Bundes vorgesehen. Insoweit fehle es schlicht an den gesetzlichen Voraussetzungen, die auch durch landesrechtliche Regelun-

gen nicht ohne weiteres geschaffen werden könnten. In der Folge führten wir Besprechungen mit der Leitung des HZI und dem Geschäftsführer der zur Ausführung vorgesehenen Softwarefirma, in denen es nochmals um die Zulässigkeit der zentralen Variante von SORMAS und um die fehlenden Unterlagen für die datenschutzrechtliche Beurteilung der nicht zentralen, gesundheitsamtsübergreifenden Variante. Das HZI sagte die Zusendung zu, ließ die Zusendung innerhalb der jeweils angekündigten Fristen aber jeweils fruchtlos verstreichen.

Anfang August sandte das HZI uns schließlich überarbeitete Unterlagen zu, die immer noch unzureichend waren und aus denen hervorging, dass unsere Hinweise z. T. gar nicht berücksichtigt worden waren. Außerdem wurden weitere Mängel offenbar, wie die Einbindung von Google Analytics, für die wir keine Rechtsgrundlage erkennen konnten. Auch dies spiegelten wir an das HZI, das Landesgesundheitsamt und das Sozialministerium. An verschiedenen Besprechungen auch mit dem Landkreistag nahmen wir teil, bevor wir Ende August erfuhren, dass die Lenkungsgruppe der Landesregierung wegen der datenschutzrechtlichen Problematik und aus weiteren fachlichen Erwägungen heraus von der Absicht der landesweiten Einführung von SORMAS wieder Abstand genommen hatte.

Das Bundesgesundheitsministerium fördert allerdings nach wie vor die Entwicklung und Einführung des Systems SORMAS – parallel u. a. zu der vom Robert-Koch-Institut entwickelten Software survnet@rki –, sodass die Einführung einer Variante von SORMAS immer noch zu erwarten ist, zumal einzelne Gesundheitsämter im Land die Variante SORMAS dezentral bereits in einer Art Pilotbetrieb verwenden. Das HZI wandte sich Mitte Oktober 2020 mit zum Teil erneuerten Unterlagen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und alle Landesbehörden, um eine gemeinsame datenschutzrechtliche Prüfung anzustoßen. Doch auch dem Bundesbeauftragten genügten die zunächst übersandten Informationen nicht. Zuletzt hat das HZI Ende Dezember 2020 weitere Unterlagen übersandt. Wir bringen uns in die datenschutzrechtliche Prüfung nach wie vor intensiv ein und finden es sehr bedauerlich, dass bei der Entwicklung einer möglicherweise sinnvollen und für die Gesundheitsämter relevanten Software offenbar trotz Förderung durch erhebliche Bundesmittel derart wenig Ressourcen dafür investiert werden, den notwendigsten datenschutzrechtlichen Dokumentations-Anforderungen gerecht zu werden, und sich das Prüfungsverfahren deswegen derart in die Länge zieht – was auch an unserer Behörde erheblichen zusätzlichen Aufwand auslöste. Diesen haben wir mit Blick auf die Bedeutung des Themas zwar stets aufgebracht; bei besserer Zuarbeit seitens des HZI wäre er aber durchaus vermeidbar gewesen.

>> Weitere Informationen
https://www.sormas-oegd.de

Die Überarbeitung der Software survnet@rki des Robert-Koch-Instituts zur Verbesserung der Kontaktnachverfolgungsfunktion

Schon seit vielen Jahren stellt das Robert-Koch-Institut (RKI) den Gesundheitsämtern und anderen Landesbehörden eine kostenlose Software namens survnet@rki zur Verfügung, die zur Erfassung, Auswertung und Weiterleitung der Meldedaten nach dem Infektionsschutzgesetz dient und auch schon bisher einige Funktionen zur Erleichterung der Kontaktnachverfolgung bot. Ein Teil der Gesundheitsämter des Landes nutzt sie seit jeher insbesondere zur Übermittlung der Meldedaten an das Landesgesundheitsamt.

Mit einem im September 2020 erschienenen update (Version 0.9.29) wurde die Verwaltung von Kontaktpersonen umfangreich geändert und erweitert. Die Gesundheitsverwaltung des Landes kam daraufhin mit der Bitte um datenschutzrechtliche Beratung auf uns zu, ob die flächendeckende Einführung der Software mit dem neuen Update datenschutzrechtlich zulässig wäre. Das Sozialministerium plante vor dem Hintergrund eines entsprechenden Beschlusses der Lenkungsgruppe „SARS-CoV-2 Coronavirus“ der Landesregierung sogar, die Verwendung der Software den Gesundheitsämtern verbindlich vorzugeben.

Wir baten daraufhin das Landesgesundheitsamt und das Sozialministerium, uns die zur datenschutzrechtlichen Beurteilung erforderlichen Unterlagen zukommen zu lassen. Das Landesgesundheitsamt verwies uns an das RKI, das wir daraufhin ebenfalls baten, uns die Dokumentation zu übersenden.

Das RKI teilte im Gespräch mit uns unsere Auffassung, dass für die Einführung des neuen Updates u.a.

wegen der grundlegenden Änderungen der Funktionen zur Kontaktnachverfolgung an sich eine Datenschutzfolgenabschätzung durch die jeweils die Software verantwortlich einsetzenden Stelle erforderlich wäre. Für diese müsste das RKI den Gesundheitsämtern entsprechende Informationen zur Verfügung stellen. Zu unserer Überraschung gab das RKI indes zu erkennen, dass es eine entsprechende Dokumentation noch nicht erstellt habe, das Update gleichwohl aufgrund des hohen politischen Drucks angesichts der Corona-Pandemie bereits herausgegeben habe. Auf unserer Nachfrage, bis wann spätestens die Dokumentation nachträglich erstellt würde, sagte uns das RKI eine Übermittlung bis spätestens Ende November 2020 zu.

Wir konnten daher dem Sozialministerium und dem Landesgesundheitsamt nur mitteilen, dass die Verwendung des Updates an sich die vorherige Durchführung einer Datenschutz-Folgenabschätzung durch die die Software einsetzende Stelle erfordere. Im Rahmen einer solchen Datenschutz-Folgenabschätzung seien die Datenverarbeitungsvorgänge unter Berücksichtigung der konkreten Verhältnisse im einzelnen Gesundheitsamt darzustellen und datenschutzrechtlich zu bewerten. Dies werde den Gesundheitsämtern einschließlich des Landesgesundheitsamts infolge der fehlenden Dokumentation seitens des RKI schwerlich möglich sein; und unsere Behörde könne aus demselben Grunde keine Vorprüfung zur Unterstützung der Gesundheitsämter vornehmen.
Andererseits können wir die zwingende Notwendigkeit der Installation des Updates zur Erfüllung der Aufgaben der Gesundheitsämter und des Landesgesundheitsamtes im Rahmen des Infektionsschutzes während der aktuellen Corona-Pandemie nicht aus eigener Fachkenntnis beurteilen.

Die Gesundheitsämter und das Landesgesundheitsamt würden daher in eigener Verantwortung prüfen und entscheiden müssen, ob sie trotz Nichterfüllung der formalen datenschutzrechtlichen Anforderungen aus zwingenden Gründen eine Installation vornehmen sollten. Dabei wiesen wir ausdrücklich darauf hin, dass die ursprünglich beabsichtigte Vorprüfung durch uns ebenso wenig wie eine formelle Freigabe durch uns förmliche Voraussetzung für den Einsatz der Software sei. Wir konnten absehbar angesichts der pandemiebedingten Sondersituation und unserer eigenen personellen Auslastung eine Prüfung der Gesundheitsämter hinsichtlich der Verwendung der Software nicht vor Mitte Dezember 2020 durchführen. Wir gingen dabei davon aus, dass das RKI seine Zusage einhalten würde, die Dokumentation bis Ende November 2020 nachzureichen. Allerdings wandten wir uns vor dem Hintergrund dieses Sachverhalts gegen die Absicht der Lenkungsgruppe, die Verwendung von survnet@rki verbindlich vorzuschreiben, so lange die rechtlichen Voraussetzungen für den Einsatz der aktuellen Software nicht hinreichend geklärt sei.

Leider hat das RKI seine Zusage, die Unterlagen bis Ende November 2020 zu erstellen und nachzureichen, nicht eingehalten. Auf mehrfache Sachstandsanfrage gab das RKI zu erkennen, dass aufgrund der hohen Auslastung des RKI infolge der aktuellen Pandemie-Situation auch sehr dringliche Aufgaben derzeit leider etwas liegenbleiben würden. Es solle nunmehr die Dokumentation so überarbeitet und vervollständigt werden, dass sie auch alle in den letzten Wochen bzw. Monaten am Meldesystem eingeführten Änderungen enthalte. Das RKI gehe davon aus, dass bis etwa Mitte Januar die wesentlichsten Arbeitspakete für die Überarbeitung der Dokumentation abgeschlossen sein werden und diese uns dann zur Verfügung gestellt werden könne.

Auch insoweit müssen wir mit Bedauern feststellen, dass im Rahmen der Bestrebungen zur Digitalisierung des öffentlichen Gesundheitsdienstes offensichtlich auch auf Bundesebene nicht genug Ressourcen dafür verwendet werden, die grundlegenden datenschutzrechtlichen Anforderungen zu erfüllen.

>> Weitere Informationen
Software - SurvNet@RKI:
https://www.rki.de/DE/Content/Infekt/IfSG/Software/software_inhalt.html

https://survnet.rki.de/Content/Service/Documentations.aspx.

1.7 Fernunterricht an Schulen während der Corona-Krise

Durch die Corona-Krise waren ab März die Schulen auf Fernunterricht-Methoden angewiesen. Bei den Lösungen der Schulen spielt der Datenschutz häufig leider eine geringe Rolle. Uns erreichten sehr viele datenschutzrechtliche Anfragen und Beschwerden von Schulen, Lehrkräften und vor allem von Eltern zu den eingesetzten technischen Systemen. Wir konnten vielfach die rechtlichen Rahmenbedingungen mit den Schulen klären und Empfehlungen aussprechen.

Die Lehrkräfte kommunizierten mit den Schüler_innen und organisierten die Verteilung von Aufgaben. Dazu wurden alle möglichen Versandwege eingesetzt. Neben klassischen Lernmanagementsystemen, wie z.B. Moodle, wurden in der Not auch digitale Wege gewählt, die datenschutzrechtlich eher problematisch waren. Dies war zwar einerseits nachvollziehbar, da viele Schulen auf die Situation des Lockdowns nicht vorbereitet waren und sich nunmehr plötzlich vor die Notwendigkeit gestellt sahen, den Schüler_innen zu Hause den Lehrstoff zu vermitteln. Andererseits wurde hier vielfach das Kind mit dem Bade ausgeschüttet, indem Grundrechte wie die informationelle Selbstbestimmung nicht beachtet wurden. Ein datenschutzkonformer Fernunterricht der Schüler_innen war indes auch unter den Bedingungen des Lockdowns möglich, wie einige Schulen zeigten, welche auf die Situation gut vorbereitet waren, weil sie z.B. bereits seit Längerem ein datenschutzkonformes Lernmanagementsystem wie etwa Moodle einsetzen.

Ein großer Bedarf bestand vor allem an Videokonferenzsystemen, über welche die Lehrkräfte mit den Schüler_innen möglichst direkt in Kontakt bleiben wollten. Es wurden dabei von den Schulen jedoch aufgrund der Eilbedürftigkeit viele datenschutzrechtlich problematische Lösungen gewählt.

Gespräche mit den Schulen zeigte die Not, die dort herrschte, aber auch zum Teil die Unkenntnis der datenschutzrechtlichen Anforderungen. Schulen verweisen auf das Kultusministerium, das ihnen signalisierte, dass sie über den Einsatz auch problematischer Software selbst zu entscheiden hätten. Nicht beachtet wurde dabei, dass bei einer solchen Entscheidung die Schule als datenschutzrechtlich Verantwortliche die gültige Rechtslage prüfen und beachten muss,

© Taken-Pixabay

Schüler_innen hatten häufig Fernunterricht statt Präsenzunterricht.

insbesondere also die DS-GVO. Vor dem Hintergrund, dass die Schulen innerhalb kurzer Zeit dafür zu sorgen hatten, dass sie in der Situation des Lockdowns funktionsfähig blieben, stellte diese notwendige rechtliche und technische Prüfung vielfach eine Überforderung der Schulen dar.

Dies schien im weiteren Verlauf auch das Ministerium erkannt zu haben, da im Anschluss allen Schulen im Land Moodle – betrieben von Belwü (dem vom Land gehosteten Landeshochschulnetz Baden-Württemberg) – kostenlos zur Verfügung gestellt wurde. Das Lernmanagement Moodle wurde schon vor einigen Jahren von uns Haus in rechtlicher sowie technischer Hinsicht allgemein geprüft und in der Konfiguration, wie sie bei Belwü vorliegt, als datenschutzkonform eingestuft. Wir gehen davon aus, dass auch die seitdem erfolgte Weiterentwicklung – insbesondere datenschutzrechtlich – vom Kultusministerium begleitet wurde.

Zusätzlich wurde ab dem Frühjahr im Auftrag des Ministeriums das Videokonferenzsystem BigBlueButton in kurzer Zeit aufgebaut und – unter Erweiterung der zur Verfügung stehenden Kapazitäten – in Moodle integriert und so allen Schulen im Land ebenfalls kostenlos zur Verfügung gestellt. Wie Gespräche mit den Verantwortlichen zeigen, scheint hier der Datenschutz beachtet worden zu sein. (Zu technischen Einstellungen siehe Kap. 1.9 „Datenschutzfreundliche Kommunikationsdienste und Videokonferenzen“)

In der zweiten „Lockdown“-Phase, bei der dieses Mal die Schulen zwar grundsätzlich offen blieben, aber dennoch vermehrt Fernunterricht beispielsweise aufgrund des Auftretens von Infektionen in der Schule oder bei Zugehörigkeit von Lehrpersonal oder Schüler_innen zu Hochrisikogruppen erforderlich wurde, zeigte sich immer noch, dass viele Schulen nicht auf den digitalen Unterricht vorbereitet waren und erneut unter besonderem Zeitdruck Lösungen für einen gelingenden Unterricht erarbeiten mussten. Die Beschulung muss gelingen, darin sind sich alle Beteiligten einig.

Wir beraten nicht nur das Kultusministerium, sondern auch die datenschutzrechtlich verantwortlichen Schulen beim Einsatz der Technik und möglicher Datenschutz-Folgenabschätzungen beim Einsatz von digitalen Tools. Wir bieten Lehrenden, Eltern und Schüler_innen zudem an, über datenschutzkonformen Unterricht zu informieren, damit sie bei der Wahl und dem Einsatz der Softwaretools bestmöglich entscheiden können. Denn: die Schulen sind verantwortlich – und müssen so auch handeln.

Rechtliche Rahmenbedingungen und Empfehlungen für Videokonferenzen im Unterricht

Bei der Verwendung eines Videokonferenzsystems im Unterricht stellen sich neben der Frage nach der datenschutzgerechten Auswahl des technischen Systems (siehe Kap. 1.9 „Datenschutzfreundliche Kommunikationsdienste und Videokonferenzen) auch grundsätzliche Fragen zum Einsatz eines solchen Systems. Dabei muss geklärt werden, welche Rechtsgrundlage(n) die Verwendung der Systeme mit Schüler_innen erlauben. Diese Rechtsgrundlagen können sich von denen unterscheiden, die gelten, wenn nur Lehrerkräfte beteiligt sind, beispielsweise bei Lehrerkonferenzen.

Zwar kann im Allgemeinen eine Schule die personenbezogenen Daten ihrer Schüler_innen insoweit verarbeiten, als es zur Erfüllung des Erziehungs- und Bildungsauftrags erforderlich ist (vgl. Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe e DS-GVO i.V.m. § 1 des Schulgesetzes Baden-Württemberg - SchG). Die rein passive Teilnahme (d.h. ohne Übertragung des eigenen Bildes und Tons) und die Nutzung der Funktion des Text-Chats können gegebenenfalls aufgrund des Erziehungs- und Bildungsauftrags der Schule erfolgen. Soweit allerdings beim Einsatz von Videokonferenzsystemen Bild und Ton von Schüler_innen erfasst und übertragen werden, stellt dies einen tieferen Grundrechtseingriff dar, der einer besonderen Rechtsgrundlage bedarf. Das hat der Gesetzgeber des Schulgesetzes grundsätzlich auch gesehen, indem er eine spezielle Ermächtigung zur Herstellung und Weiterverarbeitung von Bild- und Tonaufnahmen von Schüler_innen geschaffen hat (vgl. § 115 Absatz 3a SchG), deren Anwendungsbereich hier allerdings nicht eröffnet ist.

Außerdem muss bei Video- und Tonübertragungen aus dem häuslichen Umfeld zusätzlich berücksichtigt werden, dass dieser Bereich besonders geschützt ist (vgl. Schutz der Wohnung in Artikel 13 des Grundgesetzes). Auch deswegen kann aus datenschutzrechtlicher Sicht zwar eine passive Teilnahme am Videounterricht über den Erziehungs- und Bildungsauftrag gerechtfertigt werden, nicht jedoch eine aktive Teil-

nahme – das heißt eine Teilnahme, bei der Bilder und Töne von zu Hause an die Schule (und andere Schüler_innen) übertragen werden. Diese aktive Teilnahme ist nach geltender Rechtslage nur mit Einwilligungen nach Artikel 7 DS-GVO sowohl Schüler_in als auch der mitbetroffenen, zu Hause wohnenden Eltern (unabhängig vom Alter der/die Schüler_in) zulässig. Auch nach Erklärung der Einwilligung muss dem/r Schüler_in jederzeit freigestellt sein, die eigene Kamera oder das Mikrofon auszuschalten – denn datenschutzrechtlich ist jede Einwilligung jederzeit mit sofortiger Wirkung für die Zukunft widerruflich.

Allerdings sind Einwilligungen vor dem Hintergrund des Erwägungsgrundes Nummer 43 zur DS-GVO wegen des Über- / Unterordnungsverhältnisses zwischen Schule und Schüler_innen nicht unproblematisch. Der Freiwilligkeit einer solchen Einwilligung kann auch ein sozialer Druck seitens der Klassenangehörigen entgegenstehen. Dabei ist außerdem zu berücksichtigen, dass die Schüler_innen rechtlich einen Anspruch auf Erziehung und Bildung haben. Die Erfüllung dieses Rechts darf – mit Blick auf die erforderliche Freiwilligkeit – nicht davon abhängig gemacht werden, dass eine Einwilligung erteilt wird. Deswegen muss einem Schüler, der sein Videobild bzw. seinen Ton nicht übertragen möchte, die Teilnahme (hörend, sehend) trotzdem ermöglicht oder ein vergleichbares Bildungs- und Erziehungsangebot unterbreitet werden. Ansonsten wäre eine Einwilligung datenschutzrechtlich nicht wirksam.

Ohnehin sollten Lehrkräfte unter dem Gesichtspunkt der Datenminimierung in jedem Einzelfall prüfen, inwieweit die Bild- und Tonübertragung pädagogisch geboten ist oder andere Angebote ausreichen (wie z.B. Text-Chats oder Lernmanagementsysteme).

In formaler Hinsicht muss die Schule ferner für den rechtmäßigen Betrieb eines Videokonferenzsystems ein entsprechendes Verzeichnis der Verarbeitungstätigkeiten führen (vgl. Art. 30 DS-GVO). Soweit sie das System nicht selbst hostet, sondern einen Fremdanbieter verwendet, hat die Schule außerdem mit diesem einen Vertrag zur Auftragsdatenverarbeitung (Art. 28 DS-GVO) abzuschließen. Bei der Auswahl eines solchen Verarbeiters hat sie insbesondere darauf zu achten, dass dieser personenbezogene Daten nur insoweit verarbeitet, als es zur Erfüllung des Auftrags erforderlich ist, und dabei angemessene technische und organisatorische Maßnahmen zum Schutz der Daten umsetzt. Sofern es zur Datenverarbeitung außerhalb des Geltungsbereichs der DS-GVO kommt, sind überdies weitere Anforderungen zu beachten (siehe Kapitel 4 zum „Schrems II- Urteil").

Um die Schulen zu unterstützen und die vielen Fragen rund um das Thema Fernunterricht und Videokonferenzen zu klären, haben unsere Referent_innen viele Schulen und Eltern beraten und standen auch in einem Online-Seminar des Landesmedienzentrums Baden-Württemberg den Lehrkräften Rede und Antwort. Aus den Ausführungen zur Rechtslage ergeben sich folgende Empfehlungen:

Das Videokonferenzsystem muss möglichst datensparsam konfiguriert werden (Privacy by Default). Das System muss die Möglichkeit bieten, das Mikrofon und die Kamera durch den einzelnen Benutzer gesteuert ein- und auszuschalten. Weiterhin muss die Möglichkeit bestehen, seinen Bildschirm (bzw. die Oberfläche einzelner Programme) aktiv freizugeben. So kann beispielsweise die Lehrkraft etwas in einem Programm erklären oder ein Schüler seine Lösung allen vorstellen. Es sind also folgende Funktionen der Software zu unterscheiden:

1. Freigabe des Videobildes eines Teilnehmenden,
2. Freigabe des Tons eines Teilnehmenden,
3. Freigabe des Bildschirms bzw. der Oberfläche eines Programms eines Teilnehmenden und
4. Nutzung der Funktion eines Text-Chats.

Diese Funktionen sollte die Lehrkraft für den einzelnen Teilnehmenden freigeben oder sperren können. Hierzu gehört auch das Wissen aller Teilnehmenden

© phonlamaiphoto – stock.adobe.com

Digitaler Unterricht und Schutz der Schüler gehören zusammen.

über die aktuell bzw. potentiell beteiligten Teilnehmer, um bewusst zu entscheiden, ob er oder sie seinen Ton und sein Videobild frei gibt.

Häufig bieten die Videokonferenzsysteme auch die Möglichkeit, die Konferenzen aufzunehmen (Recording). Hierfür besteht im Unterricht grundsätzlich keine Erforderlichkeit. Außerdem stellt die Speicherung einen weiteren Eingriff in das Recht auf informationelle Selbstbestimmung dar, der von der bloßen Einwilligung zur Übertragung von Bild oder Ton nicht gedeckt ist. Diese Funktion sollte daher grundsätzlich technisch deaktiviert werden.
Eine grundsätzlich nicht zu rechtfertigende Vertiefung des Eingriffs in das Recht auf informationelle Selbstbestimmung stellt auch das Abfilmen des Monitors durch eine Kamera oder das Mitschneiden des Tons durch separates Mikrofon dar – auch soweit dies durch die (Mit-)Schüler_innen geschieht.

Die Anfertigung solcher Mitschnitte – die sich technisch allerdings kaum unterbinden lässt – hat die Schule als Verantwortliche durch organisatorische Maßnahmen – wie beispielsweise eine klare Untersagung in der Nutzungsordnung – weitestgehend zu verhindern. Auch ein sonstiges überschießendes Verarbeiten personenbezogener Daten (vor allem aus dem häuslichen Schülerumfeld) ist möglichst zu unterbinden.

So sind klare Regeln etwa in einer Nutzungsordnung aufzustellen (und gegebenenfalls mit Blick auf die ersten beiden Punkte mit Sanktionen zu belegen), welche den Teilnehmenden vorschreiben

- nicht im Beisein anderer Personen teilzunehmen, soweit räumlich möglich – so auch nicht in öffentlich zugänglichen Räumen, wie z.B. Cafés, Kneipen, Restaurants, ÖPNV, Warteräumen, Arztpraxen, Läden, etc.;
- Mitschnitte nicht anzufertigen (gilt auch für das Abfilmen per Smartphone).

und ihnen empfehlen,

- die Kamera so aufzustellen, dass möglichst wenig aus dem häuslichen Umfeld übertragen wird, sowie nach Möglichkeit das Videokonferenzsystems auf geringe Schärfentiefe bzw. auf Weichzeichnung des Hintergrunds einzustellen oder einen virtuellen Hintergrund zu verwenden.

Häufig sehen sich die Schulen auch personell überfordert, das (datenschutz-)rechtliche Know How aufzubieten, das für die Nutzung von Videokonferenzsystemen im Unterricht benötigt wird. Zwar hat jede Schule seit dem Mai 2018 einen sog. behördlichen Datenschutzbeauftragten zu berufen – häufig fehlt es dieser Person jedoch am Zeitbudget und an praktischem Wissen. Aus der Perspektive des Datenschutzes ist es daher nicht hilfreich, wenn lediglich eine Person als Datenschutzbeauftragte_r zwischen 100 und 150 Schulen betreut.

Das war vor der Pandemie eine unzureichende personelle Ausstattung der Schulen; im Jahr 2020 zeigte sich durch die Pandemie nun deutlich, dass digitaler Unterricht nicht nur „Laptops für alle“ bedeutet, sondern dass für einen funktionierenden digitalen Unterricht Schulen, Lehrende, Schülerschaft und Elternschaft sich auf eine gemeinsame Grundlage verständigen müssen, damit der Unterricht auch tatsächlich funktioniert. Dafür ist es auch notwendig, dass alle Beteiligten Rechtssicherheit haben und wissen, dass die Daten, die digital erzeugt werden, bestmöglich geschützt sind. Eltern sollen nicht befürchten müssen, dass ihre Schutzbefohlenen im Netz bloßgestellt werden. Kinder selbst sollen nicht unter Druck stehen, ihre möglicherweise wenig attraktive Wohnung anderen zu zeigen, vielleicht offenbaren zu müssen, kein eigenes Zimmer zu haben. Lehrende müssen sich darauf verlassen können, dass ihre Kommunikation sicher ist. All diese Aspekte des Schutzes der personenbezogenen Informationen stärkt und fordert die DS-GVO. Wir wirken mit unserer Arbeit darauf hin, dass dabei insbesondere auch der Wille der Betroffenen berücksichtigt wird.

Die Corona-Pandemie hat gezeigt, dass viele Schulen noch intensiver begleitet werden müssen, etwa bei der Organisation des Fernunterrichts; vor allem: Schulen müssen in die Lage versetzt werden, für die Schülerschaft das bestmögliche Bildungsangebot vorzuhalten. Dafür brauchen sie technischen Support und die personellen Ressourcen, ihre datenschutzrechtliche Verantwortung konsequent selbst wahrnehmen zu können (mehr zur Bildungsplattform in Kap. 3).

1.8 Fragen an den betrieblichen Datenschutz

Urlaubsrückkehr aus Risikogebieten

Insbesondere zu Beginn der Pandemie im Frühjahr 2020 spielten sich viele Beratungen primär vor dem Hintergrund der Prävention und Reichweite des Fragerechts von Arbeitgebern ab, etwa ob Urlaubsrückkehrer vor der Rückkehr in den Betrieb zu ihrem letzten Reise-/ und Aufenthaltsort befragt werden dürfen. Arbeitgeber trifft auf Grund der Fürsorgepflicht und nach dem Arbeitsschutzgesetz die Verpflichtung, alle erforderlichen Maßnahmen zu treffen, um die Sicherheit und Gesundheit der Belegschaft im Betrieb zu gewährleisten. Daher ist es zulässig, Urlaubsrückkehrer zu befragen, ob sie sich in einem durch das Robert Koch-Institut festgelegten Risikogebiet aufgehalten haben.

Beratung und Unterstützung bei datenschutzkonformem Pandemieschutz

Den Umgang mit diesen sensiblen Daten und eine verantwortungsvolle Vorgehensweise bei der Eindämmung, Ermittlung und Nachverfolgung von Infizierten beschäftigen sämtliche Betriebe. So waren wir Anlaufstelle für öffentliche und private Arbeitgeber sowie Institutionen, Behörden und Verbände. Aber auch viele Beschäftigte und Arbeitnehmervertretungen standen vor der Frage, welche Gesundheitsinformationen im betrieblichen Umfeld weitergegeben werden müssen, um der Gefahr von Covid-19-Infektionen effektiv entgegenzutreten.

Die Sensibilität der Personalverwaltung für die Art der verarbeitenden Daten ist hierbei unerlässlich. Es handelt sich um die Verarbeitung von Gesundheitsdaten, welche von vornherein als sogenannte besondere Kategorien von personenbezogenen Daten nach Art. 9 Abs. 1 DS-GVO besonders schützenswert gelten. Ferner ist zu berücksichtigen, dass die Covid-19-Erkrankung eines Beschäftigten für diesen oftmals zu einer Stigmatisierung in der übrigen Belegschaft führen kann.

Grundsätzlich ist es richtig, dass die Gesundheitsämter den Hut aufhaben und entscheiden, wer welche Informationen erhält und wer als Kontaktperson angesprochen wird und wer besser zuhause bleibt, um mögliche Infektionsketten zu unterbrechen. Der Beschäftigte hat dem oder der Arbeitgeber_in im Falle einer Infektion zunächst nur mitzuteilen, dass er/sie krankgeschrieben ist. Das Gesundheitsamt erlangt Kenntnis von einer Infektion und geht dann auf die Arbeitgeber zu und veranlasst alles Weitere. Arbeitgeber sind gut beraten, auf die Weisungen der Gesundheitsbehörde zu hören. Die Fürsorgepflicht von Betrieben nimmt nur dann eine höhere Gewichtung ein, wenn Gesundheitsämter völlig überfordert sind und ihre Aufgaben nicht mehr wahrnehmen können. Natürlich entscheidet ein Beschäftigter grundsätzlich (von besonderen Umständen wie z. B. in Krankenhäusern abgesehen, in denen besondere Anforderungen der Überwachung von Infektionen zu beachten sind) selbst frei, seinen Betrieb konkret über eine Covid-19-Erkrankung zu informieren.

Unsere Dienststelle war eine der ersten Aufsichtsbehörden überhaupt, die mit einer Orientierungshilfe „FAQ – Corona“ auf die Problematik des Umgangs mit Corona im Betrieb eingegangen ist. Folgefragen, etwa des Fragerechts des Arbeitgebers nach dem Aufenthalt in Risikogebieten, der Nachverfolgung von Kontaktpersonen oder der Übermittlung an Gesundheitsämter, beantwortet die Orientierungshilfe „FAQ – Corona“ dabei ebenfalls.

Die Anfragen diesbezüglich sind nach wie vor zahlreich und die Relevanz der Beratungen nimmt keineswegs ab. Zu beobachten ist allerdings, dass sich die Maßnahmen vieler Betriebe sowohl „professionalisiert“ als auch „standardisiert“ haben und sich viele Betriebe auf Grund der nun schon lange anhaltenden und dynamischen Entwicklung der Pandemie durch Maßnahmenpakete und konkrete Meldewege besser vorbereitet haben.

>> Weitere Informationen
FaQ Beschäftigtendatenschutz
https://www.baden-wuerttemberg.datenschutz.de/faq-corona/

Homeoffice – Datenschutzkonformer Umgang am Heimarbeitsplatz

Dauerthema der vergangenen Monate ist die datenschutzkonforme Gestaltung des Homeoffice. Viele Betriebe ermöglichten ihren Beschäftigten Heimarbeit. Die Gestaltung des Homeoffice ist aber mit viel Vorbereitung verbunden, sowohl für die Beschäftigten, als auch für Unternehmen. Darunter fällt unter an-

derem die Schulung und Sensibilisierung der Beschäftigten für den Datenschutz und die Vertraulichkeit der Arbeitsvorgänge im Homeoffice, die Einrichtung des Heim-Arbeitsplatzes und einer sicheren betrieblichen EDV. Aus der Praxis der Aufsichtsbehörde zeigt sich, dass der Beratungsbedarf diesbezüglich nach wie vor sehr hoch ist.

Zu Beginn des ersten Lockdowns fehlte es vielen Betrieben noch an den technischen Voraussetzungen, wie etwa einer genügenden Anzahl an Laptops oder Lizenzen für VPN-Zugänge. Ein vollständig datenschutzkonformes Homeoffice war daher eine Seltenheit. Grundsätzlich sollte etwa klar sein, dass Familienangehörige zu keinem Zeitpunkt auf die personenbezogenen Daten oder Dokumente auf dem Dienstrechner Zugriff haben dürfen und der Laptop und Speichermedien passwortgeschützt sein müssen.

Die Arbeit im Homeoffice bedeutet häufig auch die Teilnahme an Videokonferenzen. Ob ein Vorgesetzter verlangen kann, dass der Arbeitnehmer in einer Schaltkonferenz die Kamera einzuschalten hat, etwa weil die Identität der Teilnehmenden der Videokonferenz geprüft werden muss oder um zu gewährleisten, dass während der Konferenz keine Unbefugten teilnehmen, ist eine Frage des Einzelfalls (z. B. mit Blick auf den Inhalt des Gesprächs) und der tatsächlichen und rechtlichen Rahmenbedingungen (etwa in Einzel- oder Betriebsvereinbarungen). Eine Identifikation kann z. B. auch durch die Stimme, durch Codes oder andere Zugangssicherungen oder sonst durch nur kurzes Einschalten der Kamera erfolgen. Ohnehin sollte stets geprüft werden, ob eine Teilnahme durch Video wirklich erforderlich ist oder ob nicht eine Teilnahme nur mit Tonübertragung ausreicht. Einer besonderen datenschutzrechtlichen Rechtfertigung bedarf es in jedem Fall, wenn Videokonferenzen aufgezeichnet werden sollen; zumeist ist hierfür eine Rechtsgrundlage nicht gegeben. Besonders problematisch ist es auch, wenn die Videokonferenz unverschlüsselt übertragen werden soll und damit Dritte auf die personenbezogenen Daten zugreifen können. Soweit die Übertragung von zu Hause aus erfolgt, ist überdies – auch bei privaten Arbeitgebern mit Blick auf die Drittwirkung von Grundrechten – das Grundrecht aus Art. 13 GG (auf „Unverletzlichkeit der Wohnung“) zu berücksichtigten.

>> Weitere Informationen

„Tipps für sicheres mobiles Arbeiten“
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.html

Passwortschutz im Homeoffice
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/Hinweise-zum-Umgang-mit-Passwoertern-1.0.1.pdf

© len44ik – stock.adobe.com

Homeoffice: Genug Platz haben, gut sitzen, Kinder beschulen – und auf die Sicherheit der (persönlichen) Daten achten…

Fiebermessen am Werkstor?

Im Zuge des sprunghaften Anstiegs von Corona in Schlachtbetrieben kam es vermehrt zu Anfragen hinsichtlich der Möglichkeit der Temperaturmessung bei Beschäftigten am Werkstor. Dies ist aus datenschutzrechtlicher Sicht bedeutsam, da Fieber zwar grundsätzlich symptomatisch für das Coronavirus SARS-CoV-2 ist, allerdings weder eine notwendige Begleiterscheinung dieser Erkrankung darstellt noch das Vorhandensein von Fieber mit hinreichender Wahrscheinlichkeit auf eine Covid-19 Infektion hinweist. Überdies variiert die Messgenauigkeit. Für den flächendeckenden Einsatz von Temperaturmessung besteht daher keine hinreichende Rechtsgrundlage. Ferner stellen sich, insbesondere im Beschäftigtenkontext, oftmals arbeitsrechtliche Folgefragen der Lohnfortzahlung, sollte ein Beschäftigter schlicht „am Werkstor" zurückgewiesen werden. Gemeinsam mit der Datenschutzkonferenz DSK haben wir diesbezüglich einen eigenen Beschluss gefasst, welcher als Orientierungshilfe vorliegt. Insgesamt ist Fiedermessen am Werkstor kaum datenschutzkonform darstellbar und eine Temperaturmessung nur in Ausnahmekonstellationen und vulnerablen Branchen und Institutionen, etwa bei Einrichtungen im Bereich der Gesundheitsversorgung oder der Pflege – hier allerdings in Verbindung mit weiteren, einen Verdacht auf Covid-19 spezifisch abklärenden Untersuchungen – und auf freiwilliger Basis denkbar.

>> Weitere Informationen

Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie

https://www.datenschutzkonferenz-online.de/media/dskb/20200910_beschluss_waeremebildkameras.pdf.

Sonderfall: Schlachtbetriebe

Im Sommer 2020 veranlasste der enorme Anstieg an infizierten Beschäftigten von Schlachtbetrieben die Landesregierung Baden-Württemberg dazu, die Vorgehensweisen zum Pandemieschutz in der Branche der Schlachtbetriebe und Fleischverarbeitung in einer eigenen Corona-Verordnung – „CoronaVO Schlachtbetriebe und Fleischverarbeitung" – zu regeln. Wir wurden bei Erlass der Verordnung vom Sozialministerium beteiligt, da die Verordnung an vielen Stellen intensive Eingriffe in sensible Beschäftigtendaten vorsieht. Leider wurden nicht alle wesentlichen Hinweise von uns insoweit beachtet. Die Verordnung sieht neben der Erhebung der Kontaktdaten der Beschäftigten und Besucher_innen des Betriebs vor auch Corona-Test bei den Beschäftigten mittels PCR-Verfahren vor der erstmaligen Arbeitsaufnahme und danach einmal wöchentlich durch den Arbeitgeber vor. Die Datenverarbeitung betrifft sensible Gesundheitsdaten. Wir haben daher darauf hingewirkt, dass die Corona-Testungen nur durch geschultes Personal und damit regelmäßig nur durch die Betriebsmedizin erfolgen dürfen – was jedoch leider nicht seinen Weg in den Normtext der CoronaVO fand. Zudem bleiben wir dabei: Eine Corona-Testung stellt einen Eingriff in die körperliche Unversehrtheit der Beschäftigten dar – und in diese darf der Verordnungsgeber (vgl. § 32 IfSG) unstreitig nicht eingreifen.

1.9 Datenschutzfreundliche Kommunikationsdienste und Videokonferenzen

Angesichts der Situation um Covid-19 standen im vergangenen Jahr zahlreiche Verantwortliche vor der Aufgabe, technische Möglichkeiten der Online-Kommunikation einzuführen oder auszuweiten. Hierbei stellen sich auch einige Herausforderungen bei der Einhaltung geltender Datenschutzgesetze ebenso wie beim Schutz von Dienst-, Betriebs- und Geschäftsgeheimnissen.

Bei den vielen eingeführten Diensten für Videokonferenzen und andere Online-Kommunikations- und Kollaborationsformen stand für viele zunächst die

© ake1150 – stock.adobe.com

Videokonferenzsysteme sind nützlich und fordernd zugleich.

© jd-photodesign – stock.adobe.com

Die DS-GVO gilt auch bei Videokonferenzsystemen.

Funktionalität im Vordergrund, getreu dem Motto: Hauptsache es läuft. Aber: Verantwortliche haben auch datenschutzrechtliche Vorgaben zu beachten und sollten schon aus eigenem Interesse Wert auf Vertraulichkeit des Inhalts der Kommunikation legen. Wer digitale Techniken nutzt sollte auch wissen, welche Einstellungen notwendig sind, damit die Daten nicht wild durch die Gegend gejagt werden und schlussendlich bei irgendwem auf der Festplatte landen.

Auch bei Videokonferenzsystemen gilt die DS-GVO, auch dann, wenn man einen Dienstleiter beauftragt, der die technische Abwicklung organisiert. Insbesondere ist bei der Auswahl von Kommunikationslösungen im speziellen darauf zu achten, dass die Verantwortlichkeit, gegebenenfalls die gemeinsame Verantwortlichkeit, geklärt ist und nötige Verträge geschlossen werden. Es sollte auch geklärt sein, dass Datenverarbeitung (auch von Analyse-, Telemetrie- und Diagnosedaten unter jeglicher Bezeichnung) nur aufgrund und im Rahmen einer Rechtsgrundlage stattfindet, dass die Datenverarbeitung fair und transparent ist und Übermittlungen in das Ausland außerhalb des Europäischen Wirtschaftsraums (EWR) nur unter den besonderen einschlägigen Voraussetzungen stattfindet (vgl. Art. 44 ff. DS-GVO). Hierzu sollten sich Verantwortliche vorab einen Überblick über Vertragsverhältnisse und Datenflüsse (Zwecke, übertragene Daten, Empfänger) verschaffen.

Häufig sind Anwendungen datenschutzfreundlicher, wenn sie vom Verantwortlichen selbst betrieben werden können („On Premises"), beispielsweise auf eigenen Servern oder mit Hilfe von Dienstleistern mit Auftragsverarbeitungsverträgen und ausschließlich auf Weisung des Verantwortlichen. Der Vorteil ist, dass dort personenbezogene Daten wie Metadaten oder Inhaltsdaten der Kommunikation grundsätzlich nicht an Dritte oder den Hersteller übertragen werden.

Zur Übersicht: Bei Kommunikations- und Videokonferenzdiensten sind in Bezug auf Datenschutz bei der Wahl des Produkts oder Anbieters mehrere Herausforderungen zu bewältigen:

- **Transfer in Drittstaaten (z.B. in die USA) oder Zugriff von Drittstaaten auf die Daten**

Viele Videokonferenzdienste werden von Unternehmen angeboten, die ihren Sitz oder Haupt-Sitz außerhalb des Geltungsbereichs der DS-GVO haben. Damit gehen eine Reihe von Herausforderungen einher, insbesondere nach dem Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 in der Rechtssache C-311/18 („Schrems II"). Auf das Schrems II Urteil gehen wir in Kapitel 2 ein.

Echte Ende-zu-Ende-Verschlüsselung kann bei Drittstaatentransfers zwar das Risiko minimieren, zu beachten ist aber, dass Diensteanbieter weiterhin Zugriff auf Metadaten der Kommunikation haben.

- **Verarbeitung von Metadaten: Wer hat (technisch und rechtlich) Zugriff auf die Metadaten?**

Bei Kommunikationsdiensten fallen immer auch Metadaten an. Diese enthalten unter anderem Informationen, wer wann mit wem kommuniziert hat, aber möglicherweise auch Standortdaten und mehr. In der breiten Diskussion sind diese Daten im Zusammenhang mit der unzulässigen Vorratsdatenspeicherung bekannt. Diese Daten sind technisch relativ einfach auszuwerten und daher ein beliebtes Ziel, um Kommunikations-Netzwerke auszuforschen. Da dem Diensteanbieter diese Daten in der Regel im Klartext vorliegen müssen, ist es insoweit schwer, sich vor nicht vertrauenswürdigen Dienstleistern zu schützen.

- **Verarbeitung von Inhaltsdaten: Ist die Vertraulichkeit der übertragenen Inhalte gewährleistet?**

Inhaltsdaten sind die eigentlichen Kommunikationsdaten. Also beispielsweise die Gespräche oder Videos bei Videokonferenzen. Diese können besonders sensible Informationen enthalten wie Dienst-, Betriebs- oder Geschäftsgeheimnisse – oder eben geschützte personenbezogene Daten. Je nach Schutzbedarf sind diese besonders zu vorsichtig zu verarbeiten, insbesondere gilt dies bei Daten nach Artikel 9 DS-GVO, also z.B. personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen,

religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Zu beachten ist: Teilweise kann eine solche Information aber auch schon aus den Metadaten hervorgehen.

Inhaltsdaten können via Ende-zu-Ende-Verschlüsselung effektiv geschützt werden. Im Bereich der Echtzeit-Videokonferenz ist es schwer, echte Ende-zu-Ende-Verschlüsselung durchzuführen und zu garantieren. Der effektivste Schutz ist, entsprechende Dienste vor allem bei sensiblen Inhalten selbst oder durch einen vertrauenswürdigen Dienstleister unter Kontrolle des Verantwortlichen zu betreiben – vorzugsweise an Standorten innerhalb der EU.

- Werden Daten durch den Anbieter zu eigenen Zwecken verwendet?

Viele Diensteanbieter erheben Daten zu eigenen Zwecken, beispielsweise zur Produktverbesserung oder zu anderen gewerblichen Zwecken. Diese Daten werden häufig Analyse-, Telemetrie- oder Diagnosedaten genannt und erschließen meist das gesamte Nutzungsverhalten der Anwender. Aber auch die Inhalts-Daten werden von einigen Anbietern für eigene Zwecke genutzt. Dies kann z.B. die Verbesserung von eigenen Diensten wie Transkription oder Übersetzung sein.
Diese Verarbeitungen bedürfen grundsätzlich einer eigenen Rechtsgrundlage. Dafür kommt in der Regel nur die wirksame Einwilligung der betroffenen Person in Frage, und das wiederum heißt: die vorherige, informierte und transparente, freiwillige, aktiv für den Einzelfall und separat von anderen Erklärungen abgegebene sowie widerrufliche Einwilligung. Insbesondere an der Informiertheit und Transparenz scheitern viele Einwilligungserklärungen. Da es sehr schwierig ist, dafür eine rechtssichere Einwilligung einzuholen, sollten Verantwortliche auf Diensteanbieter verzichten, die entsprechende Verarbeitungen zu eigenen Zwecken durchführen.

- Werden Daten an Dritte weitergegeben oder mit anderen Daten verknüpft?

Einige Anbieter geben Nutzungsdaten an Dritte weiter. Entweder als Teil ihres Geschäftsmodells oder zur Ermittlung von Statistiken („Web Analytics“). Auch wenn diese nur nicht-personalisierte Statistiken enthalten, können die Anbieter der Analyseplattformen die Daten in der Regel oftmals eindeutig bestimmten Personen/Personengruppen zuordnen und nutzen die so ermittelten Daten beispielsweise zur Profilbildung für gezielte Werbung.
Auch solche Verarbeitungen bedürfen in der Regel einer eigenen Rechtsgrundlage, die wiederum grundsätzlich nur eine wirksame Einwilligung der betroffenen Personen sein kann.

Bei den meisten in der breiten Öffentlichkeit bekannten Diensten bestehen Herausforderungen in allen fünf genannten Punkten. Nur weil kein Dienst perfekt funktioniert, bedeutet dies aber nicht, dass es egal ist, welchen Dienst man nutzt und wie die vorgenommenen Einstellungen aussehen. Es bleibt die Forderung an jeden Verantwortlichen, bestmögliche Sicherheit der Inhaltsdaten herzustellen.

Praktische Tipps

Bei der Auswahl von Video- oder Telefonkonferenzsystemen sollte aus technischer Sicht darauf geachtet werden, dass der Anbieter weder Metadaten noch die Inhaltsdaten der Kommunikation für eigene Zwecke auswertet oder an Dritte weitergibt. Ebenso sollte ausgeschlossen sein, dass der Anbieter oder Hersteller Daten zu eigenen Zwecken verwendet oder an Dritte weitergibt. Dies können datenschutzrechtlich Verantwortliche am besten sicherstellen, wenn sie oder ihr Dienstleister (im öffentlichen Bereich sind das z.B. BITBW bei Landesbehörden oder Komm.ONE bei Kommunen) eine entsprechende Softwarelösung „On Premises“ – also im eigenen Rechenzentrum und nicht in einer Cloud – bereitstellen oder aufbauen. Dadurch ist es möglich, alle Datenflüsse und Datenerhebungen selbst zu kontrollieren. Dafür stehen auch zahlreiche Lösungen auf Basis von Open-Source-Software zur Verfügung, die prinzipiell datenschutzgerecht einsetzbar sind und in der Regel keine Datentransfers zum Hersteller oder in Drittstaaten mit sich bringen. Dienstleister sollten sich befähigen, entsprechende Dienste unter eigener Regie zu betreiben und den Kunden anzubieten.

Verantwortliche sollten nur solche Auftragsverarbeiter beauftragen, die Daten nur auf Weisung und ausschließlich im Europäischen Wirtschaftsraum (EWR) verarbeiten sowie keine Überwachung des Nutzungsverhaltens der Anwender durchführen.

Aufgrund der Schwierigkeiten mit zahlreichen bekannten Diensteanbietern empfehlen wir, auf selbst betriebene Angebote oder solche von vertrauenswürdigen lokalen Anbietern zu setzen. Es gibt mehrere Softwareprodukte aus dem Bereich der Open-Source Software, bei denen die genannten Schwierigkeiten nicht auftreten und die selbst betrieben werden können.
Wir selbst nutzen für die Online-Schulungsangebote unseres Bildungszentrums die Open-Source Software BigBlueButton auf einem selbst betriebenen Server. Diese Software ist insbesondere für Lehr- und Lernveranstaltungen ausgelegt und wir haben bisher gute Erfahrungen damit gemacht.

Es empfiehlt sich sehr, Nutzer_innen den Hinweis zu geben, wie eine App möglichst datensparsam eingesetzt werden kann (z.B. Deaktivierung der Erhebung von Statistikdaten oder Absturzberichten). Dieses ist insbesondere deshalb sinnvoll, weil wir bei einer ersten kursorischen Prüfung von verschiedenen Apps Datenübertragungen festgestellt haben, bei denen Verantwortlicher, Zweck, Datenkategorien und Rechtsgrundlage unklar bleiben. In Datenschutzhinweisen ist teilweise auch zu lesen, dass Daten für eigene Zwecke erhoben werden, die nicht für die Diensterbringung erforderlich sind, sondern unter anderem für die „Produktentwicklung" genutzt werden. Oftmals erheben die Web-Versionen von Videokonferenz-Diensten weniger Daten als Desktop-Anwendungen oder Smartphone-Apps.

Ein datenschutzkonformer und sicherer Betrieb einer Kommunikationslösung kann nur durch entsprechende technische und organisatorische Maßnahmen erreicht werden. Dazu zählen unter anderem:

- Alle Datenflüsse sind per Transportverschlüsselung (TLS) nach dem Stand der Technik abzusichern. Dies schützt vor dem Mitschneiden durch unbeteiligte Dritte auf dem Transportweg.

- Bei sensiblen Daten oder wenn ein nicht vollständig vertrauenswürdiger Dienstleister verwendet wird, sollte der Inhalt zusätzlich per Ende-zu-Ende-Verschlüsselung (E2EE) geschützt sein.

Bei Videokonferenzen sollte die Aufzeichnung von Sprache und Video deaktiviert sein und nur bei Vorliegen einer Rechtsgrundlage aktiviert werden. In einem solchen Fall ist eine aktive Aufzeichnung allen Teilnehmenden eindeutig zu signalisieren. Das unbefugte Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes ist strafbewehrt (§ 201 StGB). Funktionen, welche die Aktivität von Nutzer_innen überwachen, erfordern ebenfalls eine gesonderte Rechtsgrundlage und Transparenz. Aus unserer Sicht sollte Teilnehmenden die Möglichkeit angeboten werden, auch ohne aktive Videokamera an einer Konferenz teilzunehmen, gerade dann, wenn diese aus ihrer Privatwohnung heraus erfolgt.

Trotz der Verwendung selbst betriebener Kommunikationslösungen kann es sein, dass personenbezogenen Daten erhoben werden (insbesondere Hersteller beim Analyse-, Telemetrie- und Diagnosedaten), beispielweise durch die Einbindung von Tracking-Pixeln in Webseiten oder einer serverseitigen Übermittlung von personenbezogenen Daten an den Hersteller, mit weiterer Verarbeitung für eigene Zwecke. Stichproben haben ergeben, dass einige Apps für mobile Endgeräte neben der Kommunikation mit der selbst gehosteten Anwendung auch eine Kommunikation mit dem Hersteller der App oder mit Dritten durchführen. Daten werden dann sowohl vom Anwender als Betreiber des Servers als auch vom Hersteller der App und von Dritten verarbeitet.

>> Weitere Informationen

Datenschutzfreundliche technische Möglichkeiten der Kommunikation
https://www.baden-wuerttemberg.datenschutz.de/datenschutzfreundliche-technische-moeglichkeiten-der-kommunikation/

Orientierungshilfe Videokonferenzsysteme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK)
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/11/OH-Videokonferenzsysteme_final.pdf

Kompendium Videokonferenzsysteme des Bundesamts für Sicherheit in der Informationstechnik BSI
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf?__blob=publicationFile&v=4

1.10 Konfliktgebiet „Corona-Warn-App“

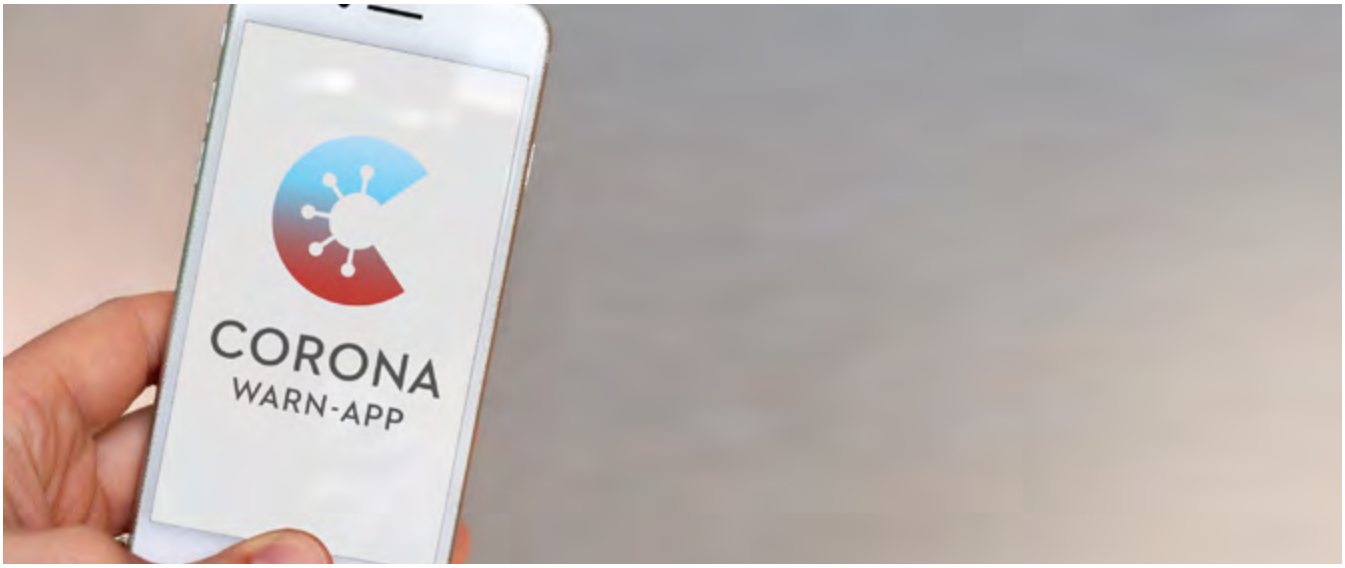
Die von der Bundesregierung in Auftrag gegebene Corona-Warn-App (CWA) soll helfen, Infektionsketten nachzuverfolgen und zu unterbrechen. Sie sorgt seit geraumer Zeit für kontroverse Diskussionen. Wir begleiten die App konstruktiv-kritisch. Wir halten die App grundsätzlich für sinnvoll und hilfreich. Wir lehnen es aber ab, sich bei der Pandemie-Bekämpfung allein auf die App zu konzentrieren. Die App kann weder die wichtige Arbeit der Gesundheitsämter ersetzen, noch ist zu erwarten, dass ein überwiegender Teil der Bevölkerung diese App freiwillig nutzt. Auch ist klar: Es ist absolut kontraproduktiv, die Attraktivität der App durch das Versprechen von Vergünstigungen zu steigern – etwa so: Wenn Sie die App nutzen, dürfen Sie auch ins Theater.

Ein solches Vorgehen schwächt die App, weil sie das Vertrauen in die App unterminiert. Statt mit Vergünstigungen zu arbeiten, sollten ihre Vorteile hervorgehoben werden. Das sind die Anonymität und die Freiwilligkeit der Nutzung. Eine Bezugnahme auf asiatische Länder in Zusammenhang mit der Warn-App ist besonders heikel. Wer Südkorea, Taiwan oder gar China als gutes Beispiel bei der Pandemie-Bekämpfung sieht, der sollte auch erklären: In Südkorea wird die massiv eingesetzte öffentliche Videoüberwachung zur Kontaktverfolgung genutzt, ebenso Kreditkartendaten. Nicht zuletzt hat die Polizei eine herausragende Rolle bei der Pandemie-Bekämpfung, weniger das Gesundheitsamt. Online werden Corona-Infizierte diffamiert und schikaniert. Zu China erübrigt sich jeder weitere Kommentar. Das chinesische Modell der Pandemie-Bekämpfung kann uns nicht als Beispiel dienen.

Wir mussten feststellen, dass wenig praktisch an der App gearbeitet wurde, es stattdessen immer stärkere dem asiatischen Modell hinterherschauende Wünsche gab. Der Datenschutz wurde als Hindernis bei der Pandemie-Bekämpfung gesehen. Doch anstatt die App konkret zu verbessern, wurde sie von vielen schlecht geredet.

Wir haben im Herbst im Austausch mit dem Ministerpräsidenten Winfried Kretschmann zügig umsetzbare und wirksamen Vorschläge formuliert, wie die Attraktivität der App gesteigert werden kann ohne ihre Sicherheit und Freiwilligkeit zu relativieren. Wir haben aber leider erkennen müssen, dass – statt konkrete Verbesserungen an der App vorzunehmen – verkündet wurde, den Datenschutz müsse grundsätzlich geschwächt werden, da die bisherigen Vorrichtungen zum Schutz der Daten der Bürger_innen zur Untauglichkeit der App führten. Wir dagegen haben fachkundige und konstruktive Vorschläge zur Corona-Warn-App formuliert, die wir nach wie vor für ein taugliches Mittel zur Bekämpfung der Pandemie halten.

Welche Vorschläge haben wir in die öffentliche Debatte eingebracht? Wir haben darauf hingewiesen, dass alle Labore an die App angeschlossen werden müssen und den Nutzer_innen angeboten wird, Testergebnisse auch über die App zu erhalten. Hierfür muss allerdings das bislang unzureichende Verfahren zur Einholung



© PhotoGranary - stock.adobe.com

Die Corona Warn App hilft bei der Pandemiebekämpfung.

der Einwilligung der Testperson in die Übermittlung des Testergebnisses an das Robert-Koch-Institut als Betreiber der App überarbeitet und datenschutzkonform ausgestaltet werden. Und weiter haben wir vorgeschlagen:

- Bereits dann, wenn die App heruntergeladen wird, kann die Einwilligung eingeholt werden, dass im Falle eines von einem Labor eingehenden positiven Befundes der App die Person als infiziert gemeldet wird. Wenn tatsächlich ein positiver Befund vorliegt und die Person darüber informiert wird, wird sie sodann gefragt, ob die Einwilligung fortgelten oder widerrufen werden soll. Voraussetzung dafür ist unter anderem: Es muss wenigstens ärztlich abgeklärt sein, ob die Mitteilung via App bei dem Betroffenen überhaupt verantwortbar ist oder ob bei dem Betroffenen voraussichtlich eine Übermittlung durch einen Arzt erforderlich sein wird.

- Für diejenigen, die zur Zeit des Downloads ihre Einwilligung zur Weitergabe eines positiven Testergebnisses an die übrigen App-Nutzer nicht erteilen, verbleibt es beim bisherigen Verfahren (erneuter Versuch der Einholung der Einwilligung nach Eingang eines positiven Testergebnisses). Reagiert der Betroffene auf die Nachfrage nach Eingang eines positiven Testergebnisses nicht, wird er hieran in bestimmten Abständen noch mehrfach erinnert.

- Die Liste der Kontakt-IDs Infizierter sollte von der App nicht wie bisher alle 24 Stunden, sondern in kürzeren Intervallen, idealerweise stündlich aktualisiert werden. Dazu müssen gegebenenfalls Serverkapazitäten erhöht werden. Das ist technisch schnell umzusetzen.

- Die App kann den Nutzer_innen dazu dienen, einfach und komfortabel die eigenen Kontakte der letzten Tage zu protokollieren. Die Speicherung und Verarbeitung dieser Daten muss dabei ausschließlich auf dem lokalen Gerät erfolgen.

- Der zuständigen Gesundheitsbehörde kann ermöglicht werden, sicher mit Nutzer_innen der App zu kommunizieren, um einwilligungsbasiert beispielsweise Informationen aus dem Kontakt-Tagebuch zu erbitten. Lehnt ein Nutzer dies ab, wird er wie im bisherigen analogen Vorgehen weiter aufgefordert, Informationen zu seinen Kontakten zu übermitteln.

- Eine weitgehende Einführung von festen und spontan erzeugten QR-Codes ist möglich: Man kann bei einem persönlichen Zusammentreffen mit weiteren Personen einmalig einen QR-Code scannen. Die Information, dass eine Person Teil einer Zusammenkunft war, wird dabei ausschließlich auf dem eigenen Gerät gespeichert. Wird bekannt, dass bei dem Zusammentreffen Infizierte bzw. positiv Getestete anwesend waren, kann dies in Bezug auf den Code über die App bekannt gegeben werden, ohne dass dies für Dritte, die nicht auf der Veranstaltung waren, erkennbar wäre. Auf diese Weise könnten die Teilnehmenden gewarnt werden, dass sie eine Veranstaltung mit Infizierten/positiv Getesteten besucht hätten. Mit dieser Meldung kann ein Hinweis zum Umgang mit der gelieferten Information ergänzt werden, was den Betroffenen sehr helfen kann.

Auf Veranstaltungen kann über einen weiteren QR Code – dies ist mittlerweile teilweise üblich – auch die Erfassung der Kontaktinformationen erfolgen und technisch sichergestellt werden, dass der Gastwirt bzw. Veranstalter keinen Zugriff auf diese Informationen hat. Möglich ist auch, dass über die App ein Pseudonym für den/die Nutzer_in festgelegt wird und der Person sodann gestattet wird, anstelle der unverschlüsselten Kontaktdaten das Pseudonym beim Veranstalter zu hinterlegen. Der zuständigen Gesundheitsbehörde wird die Möglichkeit eingeräumt, die Pseudonymisierung aufzulösen und so auf die Kontaktdaten zuzugreifen.

- Wenn die App dem/der Nutzer_in einen Kontakt mit einer infizierten Person meldet, sollte sie nähere Informationen zur Meldung liefern und zum Beispiel erläutern, was ein Kontakt mit geringem Risiko genau bedeutet.

- Eine umfangreiche Informationskampagne der App-Anbieter verweist klar auf die selbstbestimmte Entscheidung eines jeden und wirbt zugleich für Gemeinsinn. Das erhöht die Akzeptanz der App. Ein klarer Appell an die Bürgerschaft ohne jegliche Drohung ist ein wirksames Instrument, um das Vertrauen in die App zu stärken. Datenschutz und Freiwilligkeit sind zentrale Attribute der App: Nutzer_innen entscheiden selbst, ob sie ihre Daten teilen wollen. Sie dürfen aber Zutrauen haben, dass sie zu keinem Zeitpunkt bloßgestellt oder diffamiert werden können, weil die Anonymität gewährleistet ist. Sie müssen somit keine Nachteile erwarten, wenn sie sensible Informationen von sich preisgeben. Dabei muss es bleiben.

- Die App muss mit der/dem Nutzer_in interagieren und kann zu einer Informations-Stelle ausgebaut werden. Sie kann die aktuelle 7-Tages-Inzidenz in allen Landkreisen darstellen, den Verlauf der Entwicklung visualisieren und ähnliches. Damit erhalten Nutzer_innen einen praktischen Mehrwert und haben einen Grund, die App (weiter) zu nutzen.

Die Nutzung der App ist also unterstützungswürdig. Viele unserer Vorschläge wurden bereits oder werden noch umgesetzt, was sehr erfreulich ist.

Dennoch gibt es unabhängig davon aus datenschutzrechtlicher Sicht nach wie vor Mängel, die wir trotz der grundsätzlichen Unterstützung der App nicht einfach beiseitelegen können. Diese betreffen vor allem auch die technische Seite, und hierbei den technischen Rahmen, in den die App eingebettet ist. Dieser Rahmen wird von Apple und Google bestimmt, weil die allermeisten Smartphones mit einem der beiden Betriebssysteme der beiden Unternehmen funktionieren. Aus Datenschutzsicht kann europäischen Contact-Tracing-Apps ein positives Urteil ausgestellt werden. Zu diesem Urteil kommt die im Juli 2020 veröffentlichte Studie „Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps", die im Auftrag der nationalen Gesundheitsbehörden durchgeführt wurde. In der Studie haben zwei Forscher das Datensendeverhalten europäischer Contact-Tracing-Apps untersucht – darunter auch die Lösung aus Deutschland. Insgesamt attestieren die Forscher den Apps, die im Auftrag der nationalen Gesundheitsbehörden entwickelt wurden, fast durchgehend eine datenschutzfreundliche Umsetzung. Die deutsche Lösung schneidet unter Datenschutzaspekten technisch sogar am besten ab. Das ist auch kein Zufall, denn gerade die deutschen Datenschützer haben intensiv an ihrer Entwicklung mitgewirkt.

Gleichwohl bleibt die Verwendung der Contact-Tracing-Apps problembehaftet, was weniger an den Apps selbst liegt, sondern an den Systemfunktionen, auf die sie zwangsläufig zurückgreifen müssen. Die Contact-Tracing-Apps funktionieren nämlich nur im Zusammenspiel mit dem von Google und Apple speziell entwickelten „Google/Apple Exposure Notification (GAEN) Framework" zur Kontaktverfolgung. Dieses Framework ist bei Android wiederum Teil der Google Play Services – ein Bündel an proprietären Hintergrunddiensten und Schnittstellen (APIs) für Android-Geräte. Damit Contact-Tracing auf Android und iOS funktioniert, sind folglich zwei Komponenten notwendig:

- eine Contact-Tracing-App (der Client)
- und das GAEN-Framework von Google bzw. Apple.

Erst ein Zusammenspiel beider Komponenten ermöglicht den Austausch von Kontakt-IDs bzw. den notwendigen Bluetooth-Informationen mit anderen Smartphones. Während die Client-Komponente (App) in den meisten europäischen Staaten datenschutzfreundlich umgesetzt wurde, ist die andere Komponente, also die proprietäre Schnittstelle der Betreiber, hinsichtlich der Wahrung der Privatsphäre durchaus problematisch. Unter Android ist das GAEN-Framework in den sog. „Google Play Services" implementiert. Diese müssen also aktiviert sein, damit die CWA funktioniert. Laut Studie sind diese beim Privatsphärenschutz allerdings als besonders problematisch einzustufen, da Android-Smartphones damit etwa alle zwanzig Minuten Verbindung mit Google-Servern aufnehmen und dabei etliche personenbezogene Daten übermitteln – und das selbst bei einer „datenschutzbewussten" Android-Konfiguration, wie es die Forscher nennen. Zu den von den Google Play Services übermittelten Daten zählen unter anderem:

- Telefonnummer
- SIM-Kartennummer
- eindeutige Gerätenummer (IMEI)
- Seriennummer des Geräts
- WLAN-MAC-Adresse
- Android-ID
- E-Mail-Adresse des Google-Kontos
- IP-Adresse

Aus diesen Informationen könnte Google die Nutzung der Contact-Tracing-App sehr genau verfolgen und mit weiteren Kennungen verknüpfen. Allein die IP-Adresse, die regelmäßig an Google zur „Verbesserung der Ortsbestimmung" übermittelt wird, genügt im Grunde, um relativ genau nachzuverfolgen, wo sich ein Nutzer aufhält. Die Datenschutzversprechen seitens Google, keine Daten aus dem GAEN-Framework bzw. den darauf aufbauenden Contact-Tracing-Apps aufzuzeichnen, fallen daher kaum ins Gewicht.

Die dauerhafte Datenübermittlung an Google wird durch die Nutzung einer Contact-Tracing-App unter Umständen sogar noch ausgeweitet. Contact-Tracing-Apps benötigen nämlich dauerhaft Zugriff auf

die „Standortermittlung“ bzw. Ortungsfunktion, damit sie Bluetooth-Signale mit anderen Smartphones austauschen können. Dadurch fallen zwar keine Standortdaten an, allerdings muss der Standort dennoch dauerhaft aktiv sein, damit die Contact-Tracing-Apps funktionieren.

Nun könnte man sagen: „Das ist alles bekannt, das gehört zu Googles branchenüblicher Praxis und hat nichts mit der Corona App zu tun“. Diese Meinung ist natürlich nicht falsch, sie lässt allerdings außer Acht, dass die Contact-Tracing-Apps einen wertvollen Baustein bei der Bekämpfung der Pandemie bilden. In Anbetracht der aufgezeigten Datenschutzproblematik, verursacht von den Google Play Services, stellt sich nun allerdings die Frage, wie technische Verbesserungen möglich sind, die den Schutz der personenbezogenen Daten erhöhen. Letztendlich könnte die Möglichkeit weitgehender Ausspähung durch Google zahlreiche Nutzer davon abhalten, solche Apps überhaupt anzuwenden. Auf massive Kritik der Datenschützer hat Google inzwischen reagiert und die Android-Version so angepasst, dass die App nicht auf die Standortdaten zugreift. Gleichwohl bleiben zahlreiche Konflikte mit der DS-GVO bei der Betrachtung der Google Services (Art. 5 Abs. 1 Buchstabe a) und c), Art. 25 Abs. 2 DS-GVO).

Es geht nämlich auch datensparsamer. Im Dezember kam dann wie erwartet die Ankündigung, dass die deutsche Corona-Warn-App nun auch in dem freien alternativen Android-Appstore F-Droid bereitsteht. Die App lässt sich damit komplett ohne die proprietären Google-Play-Dienste verwenden. Die Free Software Foundation Europe (FSFE) begrüßte die Erneuerungen, einige wenige Entwickler haben offenbar hinbekommen, was öffentlichen Stellen nicht zu leisten vermochten.

Aber nicht nur hinsichtlich des Datenschutzes im engeren Sinne zeichnen sich beim Einsatz der Corona-Warn-App diverse Defizite ab, sondern auch in Bezug auf die IT-Sicherheit. Die in Smartphones integrierte Bluetooth-Schnittstelle ist immer mal wieder von (schwerwiegenden) Sicherheitslücken betroffen, die es einem Angreifer erlauben, sogar die Hoheit über das Gerät zu erlangen. Ein wirksamer Schutz gegen solche Angriffsszenarien ist der Verzicht auf die Bluetooth-Schnittstelle bzw. deren Nutzungsreduzierung. Für die Warn-App hingegen ist es unerlässlich, dass Bluetooth dauerhaft aktiv bleibt.

Ein Beispiel für solch eine kritische Sicherheitslücke bei Bluetooth ist BlueFrag (CVE-2020-0022), von der alle Android-Geräte mit der Betriebssystem-Version ab 8.0 bis einschließlich 9.0 betroffen sind. Die Schwachstelle ermöglicht eine sogenannte „Remote-Code-Execution“, also die Ausführung beliebigen Programmcodes durch einen entfernten Angreifer. Sofern ein Android-Gerät nicht mindestens den Sicherheitsupdate-Stand von Februar 2020 aufweist, ist es für diesen Angriff weiter anfällig. In Anbetracht der Android-Welt und seiner veralteten Geräte bzw. der Update-Problematik ist die Nutzung der App daher mit einem mittleren bis hohen Risiko verbunden – sofern nicht die aktuellen Sicherheitsupdates bzw. mindestens von Februar 2020 eingespielt sind.

Es zeigt sich: Statt den Datenschutz zu relativieren wäre es sehr hilfreich gewesen, seit der Einführung der App kontinuierliche Updates anzubieten, Weiterentwicklungen zu fördern und die Nutzer_innenfreundlichkeit zu erhöhen. Dass die Warn App kritisch zu sehen ist, liegt zu allererst daran, dass zu wenig Expertise und digitaler Wille in die App eingeflossen ist. Wir haben in Deutschland herausragende Entwickler, die zukünftig besser in die Fortentwicklung der App eingebunden werden sollten.

>> Weitere Informationen

Studie zu Tracing Apps vom Juli 2020
https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf

Golem.de „Corona-Warn-App ohne Google-Dienste verfügbar“
https://www.golem.de/news/f-droid-corona-warn-app-ohne-google-dienste-verfuegbar-2012-152667.html

2. Das Schrems II – Urteil: ein Paukenschlag

Das mit großer Spannung erwartete Urteil des Europäischen Gerichtshofs (EuGH) vom 16. Juli 2020 (Rechtssache C-311/18 – sogenanntes Schrems II-Urteil) hat erneut den Blick dafür geschärft, dass der Transfer personenbezogener Daten in Länder außerhalb Europas nicht der Selbstläufer ist, für den er bislang überwiegend gehalten wurde und dass die diesbezüglichen Regelungen in Kapitel 5 der DS-GVO erheblichen Sprengstoff in sich bergen.

Einerseits erwarten Bürger_innen, Wirtschaftsunternehmen und öffentliche Stellen in Europa in einer zunehmend globalisierten Welt zu Recht, dass sie personenbezogene Daten im Interesse ihrer Freizügigkeit und wirtschaftlichen Betätigung und um kulturellen und wissenschaftlichen Austausch zu ermöglichen in Empfängerstaaten außerhalb Europas versenden und dort verarbeiten lassen können. Andererseits macht das Informationsinteresse staatlicher Stellen in diesen außereuropäischen Ländern (etwa der Sicherheits- und Geheimdienste oder von Gerichten und Strafverfolgungsbehörden) vor den personenbezogenen Daten europäischer Bürger_innen, die in den jeweiligen Drittstaat gelangt sind, nicht halt. Die DS-GVO misst solche Zugriffe grundsätzlich an den Vorgaben des Europäischen Rechts, weil sie die Daten über ihre gesamte Verwendungszeit hinweg auch bei einer Verbringung außerhalb des räumlichen Anwendungsbereichs der DS-GVO durch ein einheitliches hohes Schutzniveau sichern will.

Mit Urteil vom 16. Juli 2020 hat der EuGH die Angemessenheitsentscheidung der Europäischen Kommission für die USA, den sogenannten EU-US Privacy-Shield, mit sofortiger Wirkung für unwirksam erklärt und sich auch zu Transfers in die USA auf der Grundlage der übrigen Transferinstrumente des Kapitels 5 der DS-GVO geäußert:

Existiert für das Zielland eine Angemessenheitsentscheidung der Europäischen Kommission, ändert sich für den Datenexporteur im Vergleich zur bisherigen Rechtslage nichts. Es gibt gültige Angemessenheitsentscheidungen der Europäischen Kommission, die ein ausreichendes, dem europäischen Datenschutzrecht im Wesentlichen gleichartiges allgemeines Datenschutzniveau für alle denkbaren Transferkonstellationen attestieren, für die folgenden Länder: Andorra, Argentinien, Australien (BNR-Daten), Färöer-Insel, Guernsey, Isle of Man, Israel, Jersey, Kanada, Neuseeland, Schweiz, Uruguay sowie Japan. In alle übrigen Länder ist ein Transfer personenbezogener Daten nunmehr ohne nähere Prüfung des dortigen staatlichen Rechts oder der Praxis, soweit Auswirkungen auf die Datenschutzrechte Betroffener denkbar sind - das betrifft insbesondere die Reichweite der Zugriffsbefugnisse oder tatsächlich erfolgende Zugriffe staatlicher Sicherheitsbehörden und den Rechtsschutz europäischer Betroffener hiergegen – nur in den in Artikel 49 der DS-GVO abschließend geregelten Fallgruppen ausnahmsweise zulässig.

Dabei geht es insbesondere um Übermittlungen, die auf der Grundlage einer Einwilligung des Betroffenen erfolgen. Die Einwilligung muss ausdrücklich sein, hinreichend bestimmt, das heißt: sie muss für einen klar umrissenen Fall einer Datenübermittlung beziehungsweise einer Reihe von Übermittlungen erteilt werden. Zudem muss sie informiert, das heißt in Kenntnis der Sachlage erfolgen, insbesondere, was die möglichen Risiken der Übermittlung betrifft. Daraus folgt eine Verpflichtung zur Information des Betroffenen über die spezifischen Risiken, die sich daraus ergeben, dass seine Daten in ein Land übermittelt werden, das keinen angemessenen Rechtsschutz bietet und in dem keine geeigneten Garantien zum Schutz der Daten vorgesehen sind.

Weiter fallen unter Artikel 49 Übermittlungen, die für die Erfüllung eines Vertrages mit der betroffenen Person erforderlich sind, Übermittlungen, die für die Wahrung der zwingenden berechtigten Interessen des Verantwortlichen erforderlich sind sowie Übermittlungen aus wichtigen Gründen des öffentlichen Interesses. Im Fall eines Vertrags mit dem Betroffenen oder einer Übermittlung zur Wahrung der zwingenden berechtigten Interessen des Verantwortlichen darf die Übermittlung nach Erwägungsgrund 111 Satz 1 nur gelegentlich beziehungsweise nach Artikel 49 Absatz 1 Satz 2 DS-GVO nicht wiederholt erfolgen und nur eine begrenzte Zahl betroffener Personen betreffen.

Gerade bei der Übermittlung personenbezogener Daten – etwa von Kunden oder Mitarbeitenden – in Zusammenhang mit der Nutzung von Cloud-Diensten oder dem Einsatz bestimmter Software werden die Grenzen des nach Artikel 49 DS-GVO Zulässigen häufig überschritten sein. Der EuGH hat klargestellt, dass die Nutzung alternativer Transferinstrumente – wie etwa der Standardvertragsklausel der Europäischen

Kommission oder sogenannter ad-hoc-Verträge, das heißt individueller Vertragsklausel (Art. 46 Abs. 3 Buchstabe a DS-GVO) oder verbindlicher Unternehmensrichtlinien – stets unter dem Vorbehalt steht, dass die Verhältnisse im jeweiligen Zielland die vertraglich zwischen dem Datenexporteur und dem Datenimporteur vereinbarten Datenschutzgrundsätze und Datenschutzrechte für Betroffene nicht aushebeln, etwa durch zu weit reichende Zugriffsbefugnisse der dortigen Sicherheitsbehörden oder unzureichenden Rechtsschutz für Betroffene im Fall, dass es zu solchen Zugriffen kommt (EuGH, Urteil vom 16. Juli 2020, Rd. Nr. 92).

Für die USA hat der Europäische Gerichtshof in seinem Urteil einen Teil der von der Europäischen Kommission in ihrem Rechtsakt zum EU-US Privacy Shield aufgeführten Zugriffsbefugnisse für die Sicherheitsbehörden der USA und den hiermit im Zusammenhang stehenden Rechtsschutz Betroffener aus Europa geprüft und ist zu dem Ergebnis gekommen, dass es insoweit an einer hinreichend klaren und präzisen Eingrenzung des Umfangs der Datenerhebung durch die Sicherheitsbehörden fehlt, ohne dass die Zugriffe irgend einer gerichtlichen Kontrolle unterlägen.

Das betrifft zum einen das auf Sektion 702 FISA gestützte sogenannte PRISM-Programm, das es US-Sicherheitsdiensten gestattet, Dienstleister für elektronische Kommunikation mit Sitz in den USA zur Herausgabe aller dort vorhandenen Informationen mit Bezug zu bestimmten Verdachtspersonen, die nicht US-Bürger_innen sind, zu verpflichten. Verdachtsgründe können sich unter den Gesichtspunkten bewaffneter Angriff auf die USA, Spionage, Terrorismus und Verbreitung von Massenvernichtungswaffen ergeben.

Das ebenfalls auf Sektion 702 FISA gestützte sogenannte Upstream-Programm verpflichtet die Unternehmen, die den Internet-Backbone in den USA und für den Datentransfer dorthin betreiben, dazu, der National Security Agency (NSA), dem größten Auslandsgeheimdienst der USA, den Zugriff auf sämtliche übertragenen Meta- und Inhaltsdaten zum Zweck der Filterung nach bestimmten Selektoren (vor allem Kommunikation von oder über bestimmte Personen) zu gestatten. Darüber hinaus gibt es eine Dienstanweisung (EO 12333), die Sicherheitsbehörden der USA zum Zweck der Auslandsaufklärung den Zugriff auf Daten elektronischer Kommunikation auf dem

© Song about summer – stock.adobe.com

Wer als Datenverarbeiter künftig auf dem europäischen Markt agieren will, muss europäische Datenschutzstandards erfüllen.

Transitweg in die USA oder während der Durchleitung durch die USA gestattet. Das ermöglicht der USA Zugang zu den Tiefseekabeln auf dem Grund des Atlantischen Ozeans, in denen Daten elektronisch von Europa in die USA übertragen werden. Allerdings gibt es bislang keinen Beweis dafür, dass die NSA von dieser Möglichkeit tatsächlich Gebrauch gemacht hat.

Der EuGH hat in seinem Urteil auch darauf hingewiesen, dass Verantwortliche das Ergreifen zusätzlicher Maßnahmen prüfen können, um einen Transfer doch noch rechtmäßig zu ermöglichen, wenn das Recht des Drittstaates dem dortigen Datenimporteur aus der Union übermittelter personenbezogener Daten Verpflichtungen auferlegt, die den vertraglich übernommenen Pflichten in den Standarddatenschutzklauseln oder verbindlichen Unternehmensrichtlinien und damit dem Europäischen Datenschutz widersprechen (EuGH, Urteil vom 16. Juli 2020, Rd. Nr. 133 bis 135).

Insoweit sind – abhängig von den konkreten Umständen des jeweiligen Einzelfalls – sowohl technisch-organisatorische Maßnahmen wie etwa eine weitgehende Verschlüsslung der Daten als auch rechtliche Maßnahmen, wie die Übernahme zusätzlicher vertraglicher Pflichten durch den Datenimporteur, denkbar. Im Rahmen von letzterem könnte beispielsweise die Transparenz erhöht werden, indem der Datenimporteur sich verpflichtet, dem Datenexporteur und dem Betroffenen Informationen über Zugriffsbefugnisse staatlicher Stellen auf die übermittelten Daten in seinem Land zur Verfügung zu stellen. Zudem könnten die Informationspflichten gegenüber dem Betroffenen verstärkt werden, indem dieser unverzüglich in jedem Einzelfall über seine Daten betreffende Herausgabeverlangen einer staatlichen Behörde im Zielland informiert wird oder der Importeur und/oder Exporteur sich verpflichten, den Betroffenen durch rechtliche Beratung und Vertretung bei der Wahrnehmung seiner Rechte vor den Gerichten und Kontrollstellen im Empfängerstaat zu unterstützen.

Auf die verständliche Unsicherheit unter Verantwortlichen und Auftragsverarbeitenden, welche konkreten Folgen das Urteil hat und wie künftige notwendige Datenübermittlungen in Drittstaaten rechtssicher gehandhabt werden können, haben wir frühzeitig mit einer Orientierungshilfe reagiert, die Vorschläge für ein mögliches Vorgehen und eine Prüfungsreihenfolge vorlegt, wenn weiterhin personenbezogene Daten aus der Europäischen Union oder dem europäischen Wirtschaftsraum in Drittstaaten übermittelt werden sollen. Auch der Europäische Datenschutzausschuss hat inzwischen Empfehlungen zu zusätzlichen Maßnahmen im technischen, organisatorischen und vertraglichen Bereich herausgegeben.

Entscheidend ist, dass möglichst bald einheitliche Bewertungen bezüglich sämtlicher relevanter Zugriffsbefugnisse von Sicherheitsbehörden und des diesbezüglichen Rechtsschutzes für Betroffene aus Europa zumindest für die wichtigsten Zielländer personenbezogener Daten aus Europa gefunden werden, also etwa für die USA, China, Brasilien und Russland. Die Datenschutzaufsichtsbehörden der Europäischen Mitgliedstaaten können und sollen dafür einen wichtigen Beitrag leisten. Anders wird sich die dringend notwendige Rechtssicherheit auf dem Gebiet des internationalen Datentransfers kaum (wieder-)herstellen lassen.

Das EuGH-Urteil führt nicht nur Unsicherheit für Datenverarbeiter, sondern bedeutet auch: Wenn ein datenverarbeitendes Unternehmen künftig auf dem europäischen Markt agieren will, muss es europäische Rechtsstandards erfüllen, insbesondere die DS-GVO einhalten. Umso erfreulicher war es, das im November Microsoft als einer der zentralen Anbieter global vernetzter IT-Produkte für Unternehmen einige Vorschläge für Garantien gemacht hat, die unmittelbar die Nutzerrechte stärken.

Die neuen Vertragsklauseln von Microsoft enthalten Regelungen über den Anspruch auf Schadensersatz für die betroffene Person, deren Daten unrechtmäßig verarbeitet wurden und die dadurch einen materiellen oder immateriellen Schaden erlitten hat. Auch informiert das Unternehmen betroffene Personen, wenn Microsoft durch eine staatliche Anordnung rechtlich bindend dazu verpflichtet wurde, Daten an US-Sicherheitsbehörden herauszugeben. Der Software-Konzern verpflichtet sich auch, den Rechtsweg zu beschreiten und die US-Gerichte anzurufen, um die behördliche Anordnung zur Herausgabe der Daten anzufechten.
Damit ist zwar die Transferproblematik in die USA nicht generell gelöst – denn eine Ergänzung der Standardvertragsklauseln kann eben nicht dazu führen, dass der vom Europäischen Gerichtshof als unverhältnismäßig beanstandete Zugriff der US-amerikanischen Geheimdienste auf die Daten unterbunden wird.

Aber Microsoft bewegt sich in die richtige Richtung. Weitere Schritte von Microsoft müssen folgen. Und weitere Unternehmen müssen folgen. So können wir wirklich konkret mit der DS-GVO den europäischen Standard durchsetzen.

>> Weitere Informationen

Orientierungshilfe „Was jetzt in Sachen Internationaler Datentransfer“
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/08/Orientierungshilfe-Was-jetzt-in-Sachen-internationaler-Datentransfer.pdf.

Empfehlungen des Europäischen Datenschutzausschuss zum Internationalen Datentransfer
https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_de

© goeremith – stock.adobe.com

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

3. Eine Bildungsplattform für Schulen

Die Digitale Bildungsplattform, welche das Kultusministerium seit geraumer Zeit plant, beschäftigt uns bis in diese Tage. Es ist zu begrüßen, dass das Kultusministerium Angebote zur Verfügung stellt, welche den Schulen das digitale Arbeiten, gerade - aber nicht nur - in der Pandemie erleichtern. Dies ist auch aus Sicht des Datenschutzes sinnvoll, denn so können übergreifend Lösungen angeboten werden, welche sicher funktionieren und die Rechte der Beteiligten achten.
Unzählige Arbeitssitzungen und Besprechungen haben wir im Rahmen der datenschutzrechtlichen Beratung des Kultusministeriums absolviert und zum Teil sehr umfangreiche Stellungnahmen erarbeitet. Bereits seit Anfang 2019 fanden hierzu Besprechungen statt, welche im Jahr 2020 deutlich intensiviert wurden. Insgesamt haben wir das Kultusministerium im Rahmen der Digitalen Bildungsplattform in den Bereichen

- Sofortnachrichten-Dienst,
- Lernmanagementsystem (LMS),
- E-Mail, Online-Speicher, Textverarbeitung, Tabellenkalkulation etc. und
- Identity and Access Managementsystem (IdAM)

beraten.

Nach datenschutzrechtlicher Prüfung durch uns wurde der Sofortnachrichten-Dienst Threema bereits im April für alle Lehrkräfte in Baden-Württemberg durch das Kultusministerium zur Verfügung gestellt. Anders als der weit verbreitete US-Messenger WhatsApp funktioniert Threema datenschutzkonform und ist dabei zuverlässig und nutzerfreundlich.

Die Ausschreibung des Lernmanagementsystems hingegen erfolgte ohne eine datenschutzrechtliche Beratung durch uns. In das anschließende Verhandlungsverfahren im Bereich Datenschutz wurden wir dann beratend einbezogen. Dadurch konnten wir wichtige datenschutzrechtliche Impulse einbringen und Korrekturen vornehmen, welche bei der zuvor erfolgten Erstellung des Ausschreibungstextes leider nicht beachtet wurden. Weiterhin berieten wir aktiv in den Bieterrunden das Kultusministerium, um ein datenschutzkonformes Lernmanagementsystem für die Schulen in Baden-Württemberg zu erhalten. Wieweit diese Impulse und Hinweise vom Kultusministerium berücksichtigt wurden, wird sich bei der Entscheidung für ein Produkt zeigen.

Der Schwerpunkt der Beratungen lag auf Microsoft Office 365, welches das Kultusministerium als Teil der Digitalen Bildungsplattform einführen möchte. Damit soll den Lehrkräften die Möglichkeit zur Kommunikation per E-Mail, ein Online-Speicher, eine Textverarbeitung, eine Tabellenkalkulation, eine Präsentationssoftware und Weiteres zur Verfügung stehen. Es war dabei unstrittig, dass das Kultusministerium eine Datenschutz-Folgenabschätzung (DSFA) erstellen muss. Darin erfolgt nach Artikel 35 Absatz 7 DS-GVO eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung in Bezug auf den Zweck, eine Bewertung der Risiken für die Rechte und Freiheiten der betroffen Personen und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Eine erste Version der Datenschutzfolgeabschätzung (DSFA) wurde Ende April 2020 vorgelegt. Darin waren als Anwender primär nur Lehrkräfte vorgesehen, wobei das Videokonferenzsystem auch Schüler_innen nutzen sollten, ohne dass diese jedoch in die Risikobetrachtung integriert wurden. Anfang Juli 2020 legten wir eine umfangreiche Stellungnahme zu dieser DSFA dem Kultusministerium vor. Im Vordergrund standen einerseits strukturelle Kritikpunkte, wie Abflüsse personenbezogener Daten zu Zwecken von Microsoft sowie die rechtlichen Rahmenbedingungen für den internationalen Datenverkehr, andererseits Mängel in den Ausführungen der DSFA nach Artikel 35 DS-GVO, wie z.B. eine unzureichende Beschreibung, zu welchen Zwecken welche Verarbeitungen erfolgen. Bei Letzterem spielt auch die Rechtsgrundlage für die Verarbeitungen eine zentrale Rolle, da die Schule – als verantwortliche Stelle – hierüber rechenschaftspflichtig ist (vgl. Artikel 5 Abs. 2 DS-GVO). Weiterhin bezog sich dieser erste DSFA nur auf Dokumente, welche Microsoft zur Verfügung gestellt hatte. Eine technische Überprüfung dieser Angaben, auch nur stichprobenweise, war nicht erfolgt.

Im Ergebnis sollten daher die in unserer umfangreichen Stellungnahme enthaltenen Punkte geprüft und

eine überarbeitete Datenschutzfolgenabschätzung vorgelegt werden. Mitte Oktober haben wir vom Kultusministerium eine zweite, ergänzte Version und erheblich überarbeitete Risiko-Abschätzung erhalten, die zwar noch nicht alle datenschutzrechtliche Fragen beantwortet, aber eine hinreichende Grundlage für den Praxistest der Software im Rahmen eines Pilotprojektes darstellt.

Im Pilot sollen die in der DSFA beschrieben Datenflüsse mit den tatsächlich messbaren verglichen werden und es ist zu prüfen, ob Microsofts Zusagen auch eingehalten werden.

Dabei bleiben allerdings – gerade beim Einsatz von US-Dienstleistern – erhebliche Unwägbarkeiten: Mit Blick auf das Schrems II-Urteil des Europäischen Gerichtshofes vom Juli 2020 ist derzeit offen, wie zukünftig Datentransfers aus der EU in die USA überhaupt legal möglich sind. Und diese Frage wird nicht in Baden-Württemberg, sondern letztlich auf europäischer Eben entschieden. Auch dies ist ein wichtiger Grund, warum Schulen bei den genutzten Softwarelösungen immer auf verfügbare und verlässlich einsatzbare Alternativen schauen sollten. Dass Microsoft im November zusätzliche Garantien zu den Standardvertragsklauseln formuliert hat, ist zu begrüßen und war notwendig. Gleichwohl sind nicht alle Fragen damit geklärt.

In unseren Gesprächen mit Microsoft konnten wir durchaus weitere Fortschritte erzielen: Das Angebot des Kultusministeriums wird auf spezielle Softwareversionen bauen, welche hinsichtlich des Abflusses von Daten an den Anbieter (sogenannte Diagnose- oder Telemetriedaten) und der Beobachtung der Nutzer den bisher an unseren Schulen eingesetzten Versionen wesentlich überlegen, also datensparsamer sind. Microsoft kommt zudem unserer Forderung nach, die Verschlüsselung der Daten zu verbessern, die eigenen Verarbeitungszwecke zu reduzieren und auch eine Anleitung der Lehrkräfte zu datensparsamer Nutzung (Nutzerführung) zu implementieren. Zum Baustein Identity and Access Managementsystem (IdAM) der Bildungsplattform gab es erste Gespräche. Dort sollen die zentralen Identitätsdaten gespeichert und allgemeine Zugriffe verwaltet werden.
Es bleibt den Schulen aber weiterhin unbenommen, auch eigene Kommunikationsmöglichkeiten zu finden und datenschutzkonforme Alternativen zu nutzen. Wir haben im vergangenen Jahr sehr deutlich formuliert, dass das Kultusministerium alternative datenschutzkonforme Kommunikationsmöglichkeiten bereitstellen sollte, damit Schulen eine echte Wahl haben. Bereits jetzt steht allen Schulen kostenlos die vom Land selbst betriebene und auf die Bedürfnisse der Lehrkräfte zugeschnittene Webkonferenz-Software BigBlueButton, das Lernmanagement-System Moodle und der Messenger Threema zur Verfügung. Das Landeshochschulnetz BelWü bietet zudem allen Schulen schon länger E-Mail-Adressen unter eigener Adresse der jeweiligen Schule. Hinzunehmen will das Kultusministerium außerdem das Open-Source-Office-Paket „OnlyOffice“ für das gemeinsame und zeitgleiche Arbeiten an Dokumenten. Weitere datenschutzkonforme Alternativen können zum Beispiel die Videokonferenz-Software Jitsi und der Cloud-Dienst Nextcloud sein.

Um solche datenschutzkonform nutzbare Alternativen aber auch tatsächlich nutzen zu können, müssen Schulen die Möglichkeiten und Kapazitäten erhalten, sich mit den Softwarelösungen genauer zu befassen, die Produkte technisch zu betreuen und Schulungen und Fortbildungsangebote zu nutzen. Unter anderem deswegen haben wir noch einmal darauf hingewiesen, dass das Kultusministerium endlich die schon bislang völlig unzureichende personelle Ausstattung der Schulen mit Datenschutzbeauftragten erheblich aufstocken muss. Diese – bereits im 34. Tätigkeitsbericht 2018 kritisierten – Verhältnisse werden mit zunehmender Komplexität und Digitalisierung immer weniger tragbar. Die Schulen müssen als datenschutzrechtlich Verantwortliche auch faktisch in die Lage versetzt werden, im Einvernehmen mit der Schüler- und Elternschaft über den konkreten datenschutzkonformen Einsatz einer Software entscheiden zu können.

Eine zentral vom Kultusministerium verantwortete digitale Bildungsplattform ist auch aus datenschutzrechtlicher Sicht sinnvoll, um die Schulen zu entlasten. Allerdings ist gerade dabei ein entsprechendes datenschutzrechtliches Niveau erforderlich, damit sich die Schulen auf die Rechtskonformität der Plattform verlassen können. Wie weit dies in den hier geplanten Komponenten umgesetzt werden kann, ist noch nicht entschieden. Deswegen darf das Kultusministerium Alternativen nicht vernachlässigen und muss die Schulen auch personell in ihren Datenschutzkompetenzen stärken.

4. Der europäische Blick

Die Corona-Pandemie hat natürlich auch die Arbeiten auf europäischer Ebene und in unserer Stabsstelle Europa im Jahr 2020 vor erhebliche Herausforderungen gestellt. Neben einem neuen Format vom Grundlagen-Schulungs-Videos auf unserer Homepage, mit denen wir Interessierten die Möglichkeit zur Online-Information geben, wurden auch Projekte der Arbeitsgruppen des Europäischen Datenschutzausschusses in den digitalen Bereich verlagert und neue Wege entwickelt, um Zielgruppen anzusprechen.

Gemeinsame Verantwortlichkeit und Auftragsverarbeitung

Nach wie vor wird unterschätzt, was sich hinter der Formulierung „gemeinsame Verantwortlichkeit" in Artikel 26 der DS-GVO verbirgt. Gemeinsame Verantwortung kann bedeuten: Betreibt eine Kommune eine Facebook-Seite, so ist sowohl sie als auch Facebook dafür verantwortlich, was auf dieser Seite passiert. Werden Daten illegal verarbeitet? Kommune und Facebook sind rechenschaftspflichtig! Nicht nur Facebook mit europäischem Sitz irgendwo im fernen Irland. Und nach allem, was wir wissen: Die Datenverarbeitung von Facebook ist spätestens seit dem Schrems II Urteil vom Juli 2020 ohne zusätzliche Garantien nicht DS-GVO konform. Das bedeutet: Kommunen, die Facebook-Seiten betreiben, sollten ihre Praxis prüfen und anpassen.

Bereits im vorvergangenen Jahr hatten wir durch das erste europäische Muster zur Erstellung eines Vertrages über die gemeinsame Verantwortlichkeit die komplexen Vorgaben der DS-GVO umsetzbar gemacht. Anhand eines konkreten Projekts von öffentlichen und privaten Stellen des Landes war es uns zudem möglich, die für die Abgrenzung im Rahmen gemeinsamer Verantwortlichkeit relevanten Aspekte herauszuarbeiten und dadurch die zugehörigen Schwerpunkte für die Vertragsgestaltung zu identifizieren.

So haben wir ein Vertragsmuster entworfen, das durch eine Aufschlüsselung der verschiedenen Verarbeitungsprozesse in sogenannte Wirkbereiche im Einklang mit der aktuellen Rechtsprechung des EuGH zu den Voraussetzungen und Grenzen der gemeinsamen Verantwortlichkeit steht. Durch genaue Zuordnung der Pflichten der einzelnen Verantwortlichen und transparente Bereitstellung aller notwendigen Informationen wird die Vorlage den Anforderungen des Artikels 26 DS-GVO gerecht und verhilft den betroffenen Personen zu einem umfassenden Schutz ihrer Rechte. Die Konstrukte der gemeinsamen Verantwortlichkeit und der Auftragsverarbeitung waren bereits nach der alten Rechtslage der EG-Datenschutzrichtlinie von 1995 bekannt, wurden dort aber nicht so sehr im Detail normiert wie in den neuen Regelungen der DS-GVO. Artikel 26 und 28 der DS-GVO formulieren diese Regelungen nun ausdrücklich aus und formulieren explizite Vorgaben. Für die datenschutzrechtliche Praxis und die Gestaltung von Verträgen erlangen diese Formen der Verantwortlichkeitsverteilung damit umso größere Bedeutung.

Unsere tägliche Arbeit zeigt, dass die Abgrenzung der verschiedenen Formen datenschutzrechtlicher Verantwortlichkeit jedoch komplex und auch die Gestaltung entsprechender Verträge Verantwortliche vor Probleme stellen kann. Deshalb wurden mittlerweile sowohl unser Muster zur Erstellung eines Vertrages über die gemeinsame Verantwortlichkeit als auch das Muster zur Erstellung eines Vertrages über die Auftragsverarbeitung in englische Sprache übersetzt.

Der Europäische Datenschutzausschuss hat im September 2020 noch weitere Abhilfe geschaffen und 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. Zu diesen hilfreichen und umfassenden neuen Leitlinien hat die Stabsstelle Europa FAQs erstellt, in denen die Kernaussagen zusammengefasst werden. Indem die FAQs die Leitlinien ergänzen und zugänglicher machen, geben sie einen verständlichen Überblick über die doch recht komplexen Rechtsfragen. Damit erleichtert der Frage-Antwort-Katalog auch dem Laien den Einstieg in das umfassende Dokument des Europäischen Datenschutzausschusses und stellt Querverweise zur Verfügung, um die im Einzelfall relevanten Ausführungen zu finden. Zusätzlich tragen konkrete Praxisbeispiele zum Verständnis bei und helfen bei der praktischen Umsetzung. Noch vor der amtlichen Übersetzung ins Deutsche wurden die Kernaussagen der Guideline den Bürger_innen und verantwortlichen Stellen auf diese Weise in ihrer Landessprache zur Verfügung gestellt.

Daneben hat die Stabsstelle, die sich auch mit Grundsatzfragen befasst, unsere Fachreferate unterstützt

und die Grundlage für dort entstandene Handreichungen, wie beispielsweise die Orientierungshilfe zu der EuGH-Rechtssache „Schrems II“, geschaffen.

Europäische Gremienarbeit

Auf seiner 15. Plenumssitzung am 12. November 2019 hat der Europäische Datenschutzausschuss das neue Coordinated Supervision Committee für die Aufsicht über europäische IT-Großsysteme und Agenturen geschaffen. Dieses tagte am 3. Dezember 2019 zum ersten Mal und verfolgt einen halbjährlichen Sitzungsturnus. Die Stabsstelle Europa nimmt für unsere Behörde in diesem Gremium als Repräsentant für Deutschland teil.

Im Coordinated Supervision Committee arbeiten der Europäische Datenschutzbeauftragte sowie die nationalen Aufsichtsbehörden aktiv zusammen, um eine wirksame Aufsicht über IT-Großsysteme und über Organe, Einrichtungen und sonstige Stellen der Union zu gewährleisten. Dazu zählen zum Beispiel das Binnenmarkt-Informationssystem IMI (Internal Market Information System), die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) und die Europäische Staatsanwaltschaft (EPPO). Der horizontale Ansatz soll die koordinierte Überprüfung dieser Systeme im Lichte des jeweils einschlägigen europäischen und nationalen Rechts gewährleisten. Der Fokus liegt dabei insbesondere auf den Schwerpunktthemen Grenzen, Asyl & Migration, Polizeiliche und justizielle Zusammenarbeit sowie Digitaler Binnenmarkt. Zu allen Fragen in diesem Zusammenhang, wie beispielsweise zur Verteilung von Verantwortlichkeiten oder der Gewährleistung von Betroffenenrechten, erarbeitet das Komitee Berichte, Richtlinien, Empfehlungen und andere Praxishilfen. Zusätzlich kann es neben einem Austausch mit den verantwortlichen Stellen auch Kontrollen vornehmen. Neben dieser neu hinzugekommenen Position als Ländervertretung nehmen wir weiterhin eine Koordinierungsposition in der Social Media Expert Subgroup des Europäischen Datenschutzausschusses wahr. Zudem sind wir in den Bereichen internationale Zusammenarbeit im Verwaltungsverfahren (Cooperation Expert Subgroup) und im Bereich der Grundsatzfragen (Key Provisions Expert Subgroup) Teil der europäischen Familie.

© Mohamed Hassan - pixabay

Der Landesbeauftragte koordiniert die Social Media Expert Subgroup des Europäischen Datenschutzausschusses.

Grenzüberschreitende Verwaltungsverfahren

Auch die internationale Zusammenarbeit in grenzüberschreitenden Verwaltungsverfahren konnte verbessert werden. Mittlerweile sind die Mechanismen der DS-GVO nicht mehr neu und ihre Handhabung konnte mit den gemeinsamen Erfahrungen der Mitgliedstaaten aus den ersten beiden Geltungsjahren weiter gestärkt werden. Insgesamt sind die internationalen Verwaltungsverfahren aufgrund des hohen Koordinationsaufwandes jedoch im Vergleich zu nationalen Verwaltungsverfahren wesentlich zeitaufwändiger. Auch wenn es bei der Zusammenarbeit in die richtige Richtung geht und wir unseren Betrag leisten: Wir haben nach wie vor keinen einheitlichen konsequenten europäischen Vollzug.

Die erste Herausforderung für das neue Jahr steht mit dem Brexit bereits fest. Die Stabsstelle hat für diesen Fall bereits Vorkehrungen getroffen, damit auch die davon betroffenen Verwaltungsverfahren, die Baden-Württemberg tangieren, ordnungsgemäß fortgeführt werden können. Es ist sehr empfehlenswert, dass sich deutsche Unternehmen hier nach alternativen EU-Dienstleistern umschauen.

Schulungen

Zur fortlaufenden Fortbildung des Hauses bietet die Stabsstelle Europa weiterhin regelmäßig Inhouse-Schulungen für alle Mitarbeitenden an, die seit Pandemiebeginn erfolgreich auf Online-Formate umgestellt wurden. Daneben halten die Referentinnen der Stabsstelle regelmäßig Vorträge im Rahmen des Programms des neu gegründeten Bildungszentrums BIDIB. Letzterem wird in Zukunft auch das von der Stabsstelle entworfene Format der Online-Schulungen zur Verfügung gestellt werden, um dieses weiter erfolgreich fortzuführen und in Zukunft noch mehr datenschutzinteressierte Personen zu begeistern.

>> Weitere Informationen

FaQ zur Abgrenzung der Verantwortlichkeit und des Konzepts zur Auftragsverarbeitung
https://www.baden-wuerttemberg.datenschutz.de/faq-zur-abgrenzung-der-verantwortlichkeiten-und-des-konzepts-der-auftragsverarbeitung/

Richtlinien zur Auftragsverarbeitung der EU
https://www.baden-wuerttemberg.datenschutz.de/faq-zur-abgrenzung-der-verantwortlichkeiten-und-des-konzepts-der-auftragsverarbeitung/

Handlungsprogramm des Coordinated Supervision Committee für die Aufsicht über europäische IT-Großsysteme und Agenturen
https://edpb.europa.eu/sites/edpb/files/files/file1/20200720_workprogramcscfinal.pdf

Präsentation von K. Vogt – Referentin der Stabsstelle Europa zum Thema „Nutzung sozialer Medien durch öffentliche Stellen“
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/12/201016_Herbstkonferenz_Nutzung-sozialer-Medien-durch-oeffentliche-Stellen_DS-GVO_copyright-Stabstelle-Europa.pdf

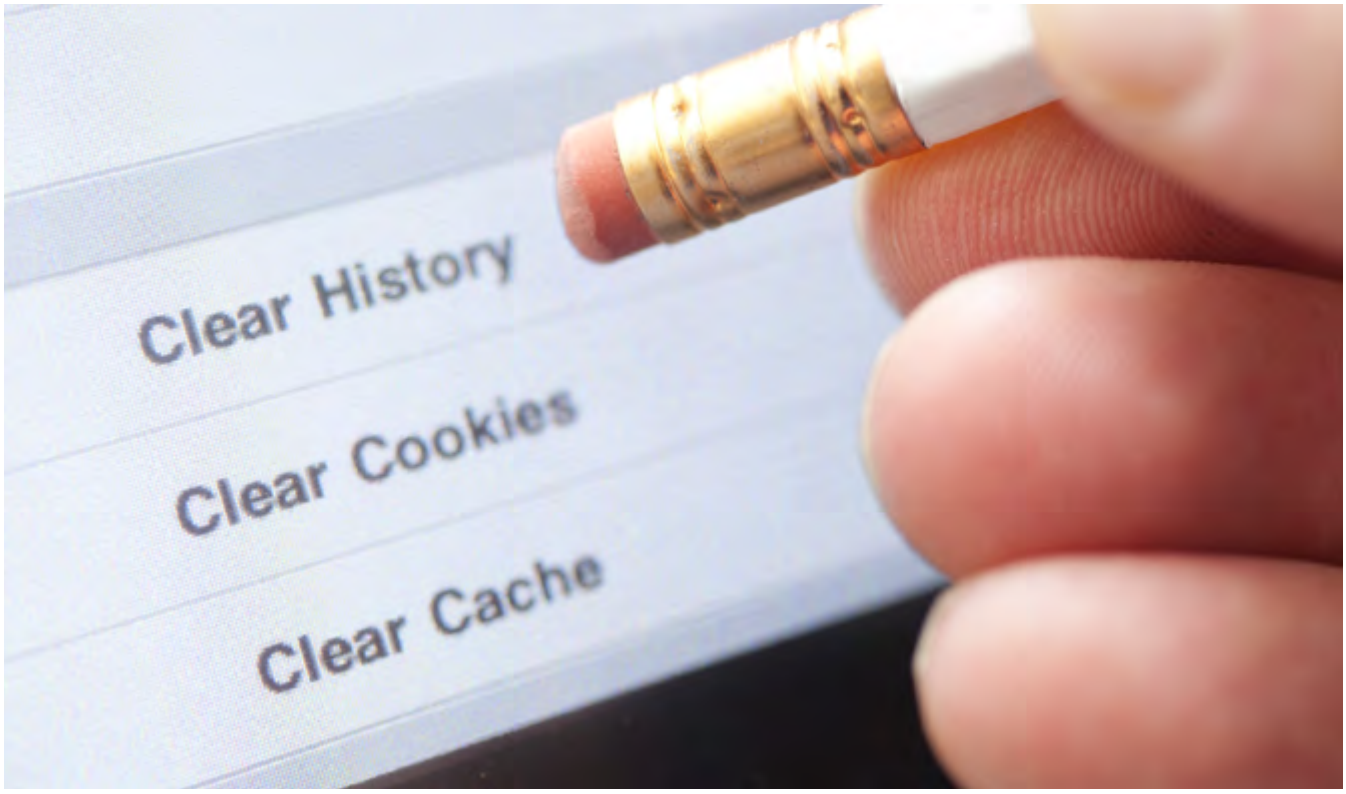
5. Prüfung von Tracking auf Medien-Webseiten

Wer das Internet nutzt, kennt Cookie-Banner. Das sind die Texte, die mal mehr, mal weniger störend vor, neben oder unter den eigentlichen Inhalt der Webseite gesetzt werden. Die Nutzer_innen sollen allerlei Informationen zur Kenntnis nehmen und irgendwie damit einverstanden sein.

Viele Menschen sind davon nur noch genervt und fragen sich, was das soll. Oft heißt es dann, „der Datenschutz" verlange dies. Um es deutlich zu sagen: Tut er nicht. „Der Datenschutz" will ausdrücklich nicht, dass Nutzer_innen entnervt auf irgendetwas klicken und so vermeintlich eine Einwilligung aussprechen. „Der Datenschutz" will, dass Nutzer_innen einfach, klar und übersichtlich informiert werden, damit sie auf dieser Grundlage selbst entscheiden können, ob sie ihre personenbezogenen Daten preisgeben oder eben nicht. Nervige Cookie-Banner sind unnötig und vor allem eins: nervig. Das sehen wir Datenschützer wie die meisten Nutzer_innen.

Aber warum braucht es Cookie-Banner dann? Wenn Unternehmen personenbezogene Daten verarbeiten wollen, dann müssen sie dies kenntlich machen. Wenn ein Unternehmen personenbezogene Daten will, muss es auch sagen, welche und zu welchem Zweck.

Mit Cookie-Bannern versuchen Webseitenbetreiber, sich Datenverarbeitungen erlauben zu lassen, die ohne Einwilligung gar nicht zulässig wären. In der Regel wollen sie etwa das Surfverhalten beobachten, Rückschlüsse über die Person daraus ziehen, sogenannte Profile der Nutzer_innen erstellen, und beides an Unternehmen weitergeben, oft auch weiterverkaufen. Würden Webseitenbetreiber auf informations- und einwilligungspflichtige Datenverarbeitungen verzichten, könnten wir das Internet nutzen, ohne ständig auf der Hut sein zu müssen, welche rechtlichen Erklärungen man uns gerade in den Mund bzw. vor die Maus legt. Und das passiert auch noch selten auf rechtmäßige Weise, denn viele Cookie-Erklärungen sind unvollständig, unverständlich oder schlicht falsch. Noch einmal in aller Deutlichkeit: Wenn sich Unternehmen darauf beschränken, nur solche Daten der Nutzer_innen zu verarbeiten, welche für die Nutzung der Webseite erforderlich sind, dann bedarf es keiner Einwilligung. Die nervigen Cookie-Banner werden uns nur deswegen in dieser Form angezeigt, weil der Webseitenbetreiber mehr Informationen über uns sammeln möchte, als er „eigentlich" braucht.



© jdwfoto_clear cookies – stock.adobe.com

Zahlreich vorhanden, aber kaum zu verstehen: Die Erläuterungen in Cookie-Bannern.

©Tarik Vision – stock.adobe.com

Cookie-Banner: Webseitenbetreiber wollen eine Erlaubnis für Datenverarbeitungen, die ohne Einwilligung gar nicht zulässig wären.

Im Sommer 2020 haben wir daher zeitgleich mit anderen deutschen Aufsichtsbehörden in einem groß angelegten Verfahren begonnen, im ersten Schritt redaktionelle Online-Angebote auf die rechtskonforme Einbindung von Tracking-Technologien zu prüfen. Die Prüfung wurde länderübergreifend vorbereitet und wird in enger Zusammenarbeit der beteiligten Landesdatenschutzbehörden innerhalb des jeweiligen Zuständigkeitsbereiches durchgeführt. Dazu haben wir die laut der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) zwölf reichweitenstärksten redaktionellen Online-Medien angeschrieben und einen umfangreichen Fragenkatalog übermittelt.

Wir wollten wissen:

- Welche eingebundenen Dienste von Drittanbietern einschließlich Auftragsverarbeitern genutzt werden (z. B. Zählpixel, Analysedienste, Marketingdienste, Trackingdienste, Kartendienste, Wetterdienste, Chatdienste),
- Wie die jeweilige Website mit anderen Webseiten kommuniziert,
- Welche Informationen, Objekte oder sonstigen Elemente auf den Endgeräten der Nutzer gespeichert werden

Wir sind noch mitten in der Prüfung. Erste vorläufige Ergebnisse zeigen: Mancher Verlag bindet über 250 verschiedene Drittdienste an über 1.200 Endpunkten ein und setzt dafür über 500 verschiedene Cookies ein oder nutzt andere Tracking-Techniken wie Fingerprinting. Das sieht spannend aus.

Und heißt konkret: Mit einem entnervten Klick und der vermeintlichen Einwilligung genehmigt sich der Verlag die umfassende Verarbeitung von personenbezogenen Daten. „Der Datenschutz“ fordert nun, dieses transparent zu machen. Es ist an den Verlagen, den Nutzer_innen darzulegen, warum bis zu 500 Cookies eingesetzt oder hunderte Drittdienste eingebunden werden.

Wir werden die Prüfung abschließen und das Gespräch mit den Verlagen suchen. Bevor es diese Cookie-Banner gab, gab es Cookies und Drittanbieter auf den Webseiten der Verlage. Mit den nervigen Cookie-Bannern wurde dies zumindest in Teilen transparent gemacht. Es wird sicherlich lohnend sein, den Weg der Nutzer_innen-Information weiter zu verfolgen und auch daran zu arbeiten, wirksame Einwilligungen möglich zu machen, die nicht nervig, sondern datenschutzkonform sind.

Verantwortliche sollten, unabhängig vom Ausgang dieses Prüfverfahrens, so sie nicht auf einwilligungsbedürftige Verarbeitungen bei Internetangeboten und Apps verzichten möchten, großen Wert darauf legen, dass eine Einwilligung tatsächlich frei und wirksam erfolgen kann. Das bedeutet die Einholung einer vorherigen, informierten und transparenten, freiwilligen, aktiv für den Einzelfall und separat von anderen Erklärungen eingeholten sowie widerruflichen Einwilligung.

>> Weitere Informationen

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

Orientierungshilfe der Aufsichtsbehörden für Anbieterde von Telemedien
https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

6. Aktuelles aus der Bußgeldstelle

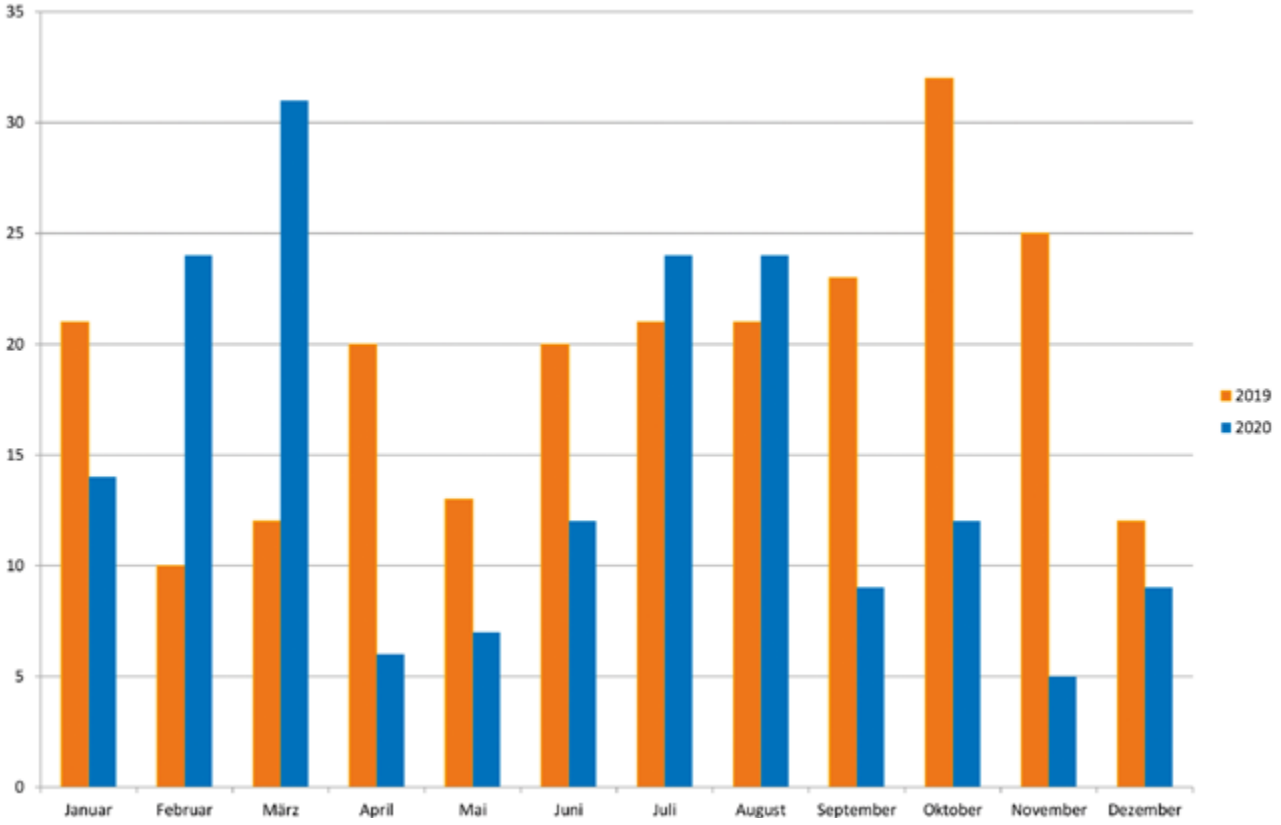
Vom 01.01.2020 bis zum 31.12.2020 wurden bei der Bußgeldstelle insgesamt 174 neue Verfahren anhängig. Während die Anzahl der Neueingänge in den Monaten vor Ausbruch der Corona-Pandemie in Deutschland noch über den Eingangszahlen der Vorjahresmonate lag, gingen die Eingangszahlen ab dem Monat April spürbar zurück und lagen erst in den Sommermonaten wieder auf einem zum Vorjahr vergleichbaren Niveau, bevor sie im Herbst wieder deutlich abnahmen.

Im Berichtszeitraum hat die Bußgeldstelle 19 Bußgeldbescheide erlassen. Ein solcher Bescheid ist der Schlusspunkt eines umfangreichen Prüfverfahrens. Diese Bescheide richteten sich sowohl gegen Einzelpersonen als auch gegen kleine, mittlere und größere Unternehmen. Dabei standen häufig Verstöße gegen die technischen und organisatorischen Maßnahmen gem. Art. 32 DS-GVO im Zentrum der Vorwürfe. Insgesamt wurden Bußgelder in Höhe von 1.670.050 Euro zuzüglich Gebühren in Höhe von 16.088 Euro festgesetzt.

AOK – heilende Wirkung eines Bußgeldes für eine Krankenkasse

Mitte Juni haben wir gegen die AOK Baden-Württemberg ein Bußgeld in Höhe von 1.240.000,- Euro verhängt, weil sie technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten nicht in ausreichendem Umfang implementiert hatte. Es handelt sich dabei um das bisher höchste in Baden-Württemberg verhängte Bußgeld und um das erste Bußgeld gegen eine öffentliche Stelle.

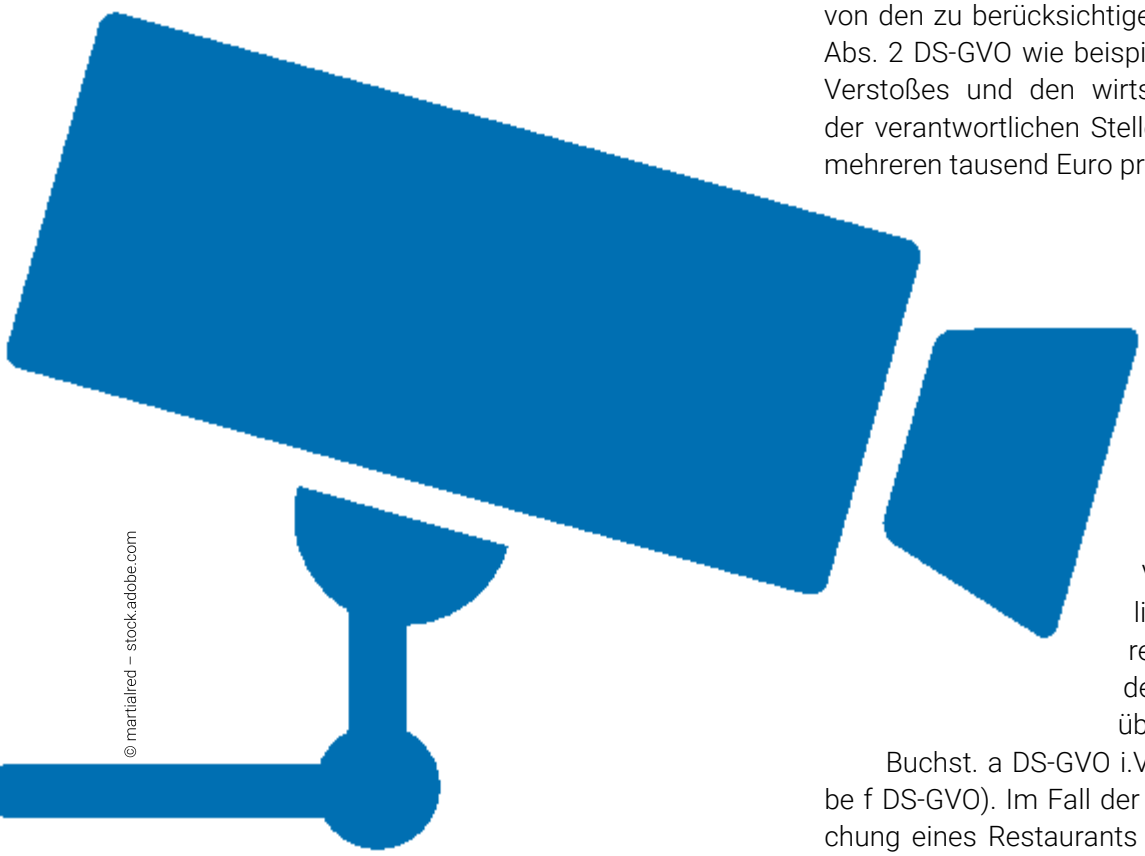
Durch monatelange Ermittlungsarbeit der Bußgeldstelle konnte nachgewiesen werden, dass bei Gewinnspielen, welche die AOK in den Jahren 2015 bis 2019 durchgeführt hatte, personenbezogene Daten wie die Kontaktdaten und die Krankenkassenzugehörigkeit von Gewinnspielteilnehmern erhoben und ohne deren Einwilligung an die Vertriebsabteilung der AOK zur Neukundenakquise übermittelt worden waren. Auf diese Weise wurden personenbezogene Daten von mehr als 500 Gewinnspielteilnehmern ohne deren Einwilligung zu Werbezwecken verwendet. Versichertendaten waren hiervon nicht betroffen. Neben weiteren investigativen Maßnahmen vollzog die Bußgeldstelle mit personeller Unterstützung der Kriminalpolizei die zeitgleiche Durchsuchung mehrerer Niederlassungen



© LfDI BW

der AOK Baden-Württemberg und wertete anschließend circa 12.000 beschlagnahmte Gewinnspielkarten und weitere Beweismittel aus. Dank des offenen Umgangs mit den eigenen Versäumnissen seitens der AOK und der sehr guten Zusammenarbeit mit unserer Behörde konnte es gelingen, die technischen und organisatorischen Maßnahmen im Vertriebsbereich der AOK in relativ kurzer Zeit auf ein gutes und datenschutzkonformes Niveau anzuheben.

Das Verfahren zeigt dabei nicht nur, dass Datensicherheit eine Daueraufgabe ist, welche die regelmäßige Überprüfung und Anpassung der technischen und organisatorischen Maßnahmen abhängig von der Entwicklung der tatsächlichen Verhältnisse erfordert. Vielmehr dokumentiert das Verfahren auch, dass öffentliche Stellen den gleichen Anforderungen an eine rechtskonforme Verarbeitung von personenbezogenen Daten wie private Verantwortliche unterliegen und dass bei Datenschutzverstößen durch öffentliche Stellen, soweit die entsprechenden Voraussetzungen hierfür vorliegen, auch eine Sanktionierung durch Bußgelder in Betracht kommen kann.



© martialred – stock.adobe.com

Herausforderung Videoüberwachung

Wegen rechtswidriger Verarbeitung personenbezogener Daten durch Videoüberwachung des öffentlichen Raumes hat die Bußgeldstelle seit Erstellung des letzten Tätigkeitsberichts mehrere Bußgelder verhängt. So haben wir unter anderem im November 2019 wegen der umfangreichen Videoüberwachung eines Restaurants mit 350 Sitzplätzen und insgesamt 24 Videokameras ein Bußgeld in Höhe von 5.000 Euro festgesetzt. Hierbei handelte es sich zwar um einen schwerwiegenden Fall einer rechtswidrigen Videoüberwachung, jedoch nicht um einen Einzelfall. So gingen im Berichtszeitraum bei der Bußgeldstelle eine Vielzahl von Anzeigen wegen der Videoüberwachung des öffentlichen, aber auch des privaten Raums ein.

Die mit Bußgeldern belegten Verstöße reichten von der Videoüberwachung des Gehwegs mit einer Videokamera bis zur Totalüberwachung des Restaurants mit 24 Kameras, von der Aufzeichnung von Verkehrsteilnehmern durch eine Dash-Cam bis zum Eingriff in die Intimsphäre durch Überwachung von Umkleiden. Die verhängten Bußgelder lagen dabei, abhängig von den zu berücksichtigenden Kriterien des Art. 83 Abs. 2 DS-GVO wie beispielsweise der Schwere des Verstoßes und den wirtschaftlichen Verhältnissen der verantwortlichen Stelle, zwischen 250 Euro und mehreren tausend Euro pro Verstoß.

Zwar kann die Verarbeitung personenbezogener Daten durch den Einsatz von Videokameras im öffentlichen Raum durchaus zulässig sein, wenn die Verarbeitung zur Wahrung der berechtigten Interessen der Verantwortlichen erforderlich ist und nicht die Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen (Art. 5 Abs. 1 Buchst. a DS-GVO i.V.m. Art. 6 Abs. 1 Buchstabe f DS-GVO). Im Fall der geahndeten Videoüberwachung eines Restaurants vom November 2019 war die Videoüberwachung jedoch nicht zur Wahrung der vom Verantwortlichen verfolgten Interessen erforderlich. Dieser begründete die Videoüberwachung unter

anderem mit dem Schutz des offen zugänglichen Buffets vor unbefugten Eingriffen durch Dritte, wie Vergiftungen durch Konkurrenten. Erforderlich ist eine Maßnahme zur Interessenswahrung aber nur, wenn ein Grund, etwa eine Gefährdungslage, hinreichend durch Tatsachen oder die allgemeine Lebenserfahrung belegt ist (BVerwG, Urteil vom 27.03.2019, Az. 6 C 2.18, Rz. 26).
Da ein solcher Eingriff bisher nicht erfolgt war und auch keine entsprechende konkrete Gefährdungslage vorgetragen oder ersichtlich war, war auch die Videoüberwachung nicht aus diesem Grund erforderlich. Auch die vom Verantwortlichen vorgebrachte Begründung des Schutzes des Eigentums der Gäste vor Diebstahl, insbesondere wenn diese ihren Platz und damit ihre Wertgegenstände verlassen, um sich am Buffet zu bedienen, vermochte die Videoüberwachung nicht zu rechtfertigen. Zwar stellt der Diebstahlschutz ein grundsätzlich berechtigtes Interesse dar, welches auch – obwohl solche Diebstähle dem Verantwortlichen nicht bekannt waren – durch die allgemeine Lebenserfahrung belegt sein kann. Jedoch ist eine Videoüberwachung nur dann erforderlich, wenn gleichzeitig dem damit verfolgten Interesse nicht ebenso gut durch eine andere gleich wirksame, aber schonendere Maßnahme Rechnung getragen werden kann.

Schonender als die Videoüberwachung sind insbesondere Maßnahmen, die das informationelle Selbstbestimmungsrecht der Besucher_innen der öffentlich zugänglichen Räume nicht berühren (BVerwG, a.a.O.). Dies gilt insbesondere vor dem Hintergrund des mit der Videoüberwachung des Gastraumes einhergehenden schwerwiegenden Eingriffs in das Grundrecht auf informationelle Selbstbestimmung der betroffenen Personen, hier der Gäste und Mitarbeitenden. Denn in einem Restaurant verweilen Gäste typischerweise länger, weshalb eine ständige Videoüberwachung solcher Bereiche auch eine erhebliche Beeinträchtigung des Persönlichkeitsrechts darstellt (vgl. AG Hamburg, Urteil vom 22. April 2008 – 4 C 134/08), die nur dann gerechtfertigt sein kann, wenn den berechtigten Interessen nicht in anderer Weise zumutbar Rechnung getragen werden kann. Eine die Persönlichkeitsrechte der betroffenen Personen nicht verletzende und gleichzeitig mindestens ebenso wirksame Maßnahme wäre vorliegend z.B. das Aufstellen von abschließbaren Spinden und Schließfächern für die Gäste oder eine Garderobe gewesen, an welcher ein Mitarbeiter Kleidungsstücke und Wertgegenstände gegen Ausgabe einer Garderobenmarke verwahrt.
Das durch unsere Bußgeldstelle im aktuellen Berichtszeitraum erstmals verhängte Bußgeld im siebenstelligen Bereich gegen die AOK Baden-Württemberg reiht sich ein in eine Vielzahl von vergleichbar hohen oder sogar höheren Bußgeldbeträgen, die seit Wirksamwerden der DS-GVO von deutschen und anderen europäischen Datenschutzaufsichtsbehörden gegen Verantwortliche verhängt wurden. Die Erwartung, dass die Bußgeldregelungen der DS-GVO zu deutlich höheren Bußgeldern führen würden, hat sich also bestätigt.
Dennoch verhängen wir Bußgelder stets mit Augenmaß und zugeschnitten auf den jeweiligen Einzelfall, was etwa durch die Bandbreite der verhängten Bußgelder bei unzulässigen Videoüberwachungen ersichtlich wird. An einem Wettlauf um möglichst hohe Beträge oder möglichst viele Bescheide beteiligen wir uns ausdrücklich nicht. Vielmehr zeigt die Anzahl der Bußgeldbescheide, dass eine Sanktionierung nach wie vor nur in Einzelfällen erfolgt, wenn Datenschutzverstöße auch unter Berücksichtigung sonstiger Abhilfemöglichkeiten gemäß Art. 58 Abs. 2 DS-GVO sanktionsbedürftig erscheinen. Auch belegen unsere praktischen Erfahrungen, dass immer mehr Verantwortliche die Notwendigkeit und den Mehrwert geeigneter Formen der Verarbeitung von personenbezogenen Daten erkennen, bevor wir als Aufsichtsbehörde damit befasst werden.

7. Exit – Abschied vom Vereinigten Königreich und Twitter

Brexit – Folgen für den Transfer personenbezogener Daten

Der Austritt des Vereinigten Königreichs (UK, bestehend auch England, Schottland, Wales und Nordirland) aus der Europäischen Union war zunächst zum 29. März 2019 vorgesehen und erfolgte nach weiteren Verlängerungen zum 31. Januar 2020. In dem Austrittsabkommen vom 24. Januar 2020 war eine Übergangsphase bis zum 31. Dezember 2020 vorgesehen, in der die langfristigen Beziehungen zwischen dem Vereinigten Königreich und der Europäischen Union neu ausgehandelt werden sollten. In dieser Übergangsphase behielt die DS-GVO trotz des zum 31. Januar 2020 erfolgten Austritts des UK aus der EU weiterhin ihre Gültigkeit im Vereinigten Königreich. Es bedurfte daher in dem Übergangszeitraum auch keiner besonderen Schutzmaßnahmen, wenn personenbezogene Daten in das Vereinigte Königreich übermittelt wurden. Außerdem konnten Unternehmen mit einer Niederlassung in der EU vom Kooperationsverfahren der Zusammenarbeit nach Artikel 56 und 60 der Datenschutz-Grundverordnung profitieren.

Kurz vor Weihnachten verkündeten die EU und das Vereinigte Königreich nun eine Einigung, welche auch die Frage des zukünftigen Datentransfers in die UK umfasst. Soweit ersichtlich soll nun innerhalb eines halben Jahres entweder ein Angemessenheitsbeschluss der Europäischen Kommission zugunsten von UK ergehen oder ein anderer Transfermechanismus etabliert werden. Ohne politische Einigung zwischen dem Vereinigten Königreich und der EU bis zur Jahresmitte 2021 ist diese für verantwortliche Stellen in Europa vergleichsweise komfortable Situation danach Geschichte. Wie bei einem Transfer personenbezogener Daten in beliebige andere Drittstaaten auch bedarf es dann für einen Transfer personenbezogener Daten neben den allgemeinen datenschutzrechtlichen Voraussetzungen (etwa nach Artikel 6 der DS-GVO, sogenannte erste Stufe) auch eines Transfer-Instruments nach Kapitel 5 der DS-GVO (sogenannte zweite Stufe).

Solange die Europäische Kommission keine Angemessenheitsentscheidung nach Artikel 45 für das UK erlassen hat, kommen als Transfer-Instrument insbesondere die Standarddatenschutzklauseln der Europäischen Kommission, verbindliche interne Datenschutzvorschriften (sogenannte Binding Corporate Rules, BCR) oder die Fallgruppen des Artikel 49, zum Beispiel ausdrückliche Einwilligungen der betroffenen Personen in Betracht.

Die Aufsichtsbehörden der Europäischen Mitgliedstaaten haben sich im Berichtszeitraum ausführlich mit den Folgen des Brexit auf dem Gebiet des Datenschutzes befasst. Schwerpunktmäßig ging es dabei zum einen um die weitere Behandlung bereits laufender Zusammenarbeitsverfahren nach Artikel 56 und 60 der DS-GVO (sogenannte One Stop Shop-Verfahren), an denen die Datenschutzaufsichtsbehörde des Vereinigten Königreichs als federführende oder beteiligte Aufsichtsbehörde mitgewirkt hat. Insoweit ist entscheidend, ob der Verantwortliche über eine oder mehrere andere Niederlassungen außerhalb des UK in der EU verfügt. In diesem Fall kann das One Stop Shop-Verfahren unter Federführung der Datenschutzaufsichtsbehörde am Ort der anderen Niederlassung(-en) in der EU fortgesetzt werden. Existiert keine andere Niederlassung in der EU und wird eine solche auch nicht kurzfristig vom Verantwortlichen eröffnet, kann das One Stop Shop-Verfahren mangels (Haupt-) Niederlassung des Verantwortlichen oder Auftragsverarbeiters in der EU nicht fortgesetzt werden. Die Zuständigkeit für solche Verfahren geht auf alle europäischen Aufsichtsbehörden über, in deren Hoheitsgebiet Betroffene ihren Wohnsitz haben, auf welche die Verarbeitungstätigkeiten des Verantwortlichen Auswirkungen haben oder ausgerichtet sind (Artikel 55 Absatz 1 i. V. m. Erwägungsgrund 122 DS-GVO).

Weiter haben sich die Aufsichtsbehörden der Mitgliedstaaten mit den Folgen des Brexit auf verbindliche Unternehmensrichtlinien befasst, die von der Datenschutzaufsichtsbehörde des Vereinigten Königreichs, dem Information Commissioner`s Office (ICO) genehmigt wurden. Insoweit gilt: Eine vom ICO vor dem Wirksamwerden der DS-GVO am 25. Mai 2018 erteilte Genehmigung von BCR noch unter der Geltung der Datenschutzrichtlinie aus dem Jahr 1995 (Richtlinie 95/46/EG) gilt zunächst weiterhin. Die 33 verbindlichen Unternehmensrichtlinien, um die es dabei geht, müssen jedoch an die neue Situation angepasst werden. So muss zum Beispiel ein haftendes Unternehmen in der EU bestimmt und es müssen Neuregelungen zur Zuständigkeit europäischer Gerichte getroffen werden.

© Markus Mainka – stock.adobe.com

Der Brexit belastet viele Unternehmen, auch weil es bislang keine klare und dauerhafte Regelung für den Datentransfer gibt.

Für verbindliche Unternehmensrichtlinien, die der Information Commissioner (ICO) nach Wirksamwerden der DS-GVO genehmigt hat, ist dagegen eine neue Genehmigung durch eine europäische Aufsichtsbehörde erforderlich, weil die alte Genehmigung des ICO mit dem Ende der Übergangsphase ihre Wirksamkeit verliert. Die neue federführende Aufsichtsbehörde am neuen Hauptsitz des Unternehmens in der EU soll auch bereits begonnene aber noch nicht abgeschlossene Genehmigungsverfahren des ICO übernehmen und weiterführen

Es bleibt zu hoffen, dass sich im Zuge des Brexits auch geeignete Sicherheiten für den Datenschutz ergeben, da ansonsten auf deutsche und europäische Unternehmen erhebliche Unsicherheiten beim Datentransfer ins Vereinigte Königreich warten – und auch über einen Wechsel der Handelspartner nachgedacht werden muss.

>> Weitere Informationen

Hinweise des Europäischen Datenschutzausschusses der EU für vom „Information Commissioner`s Office" genehmigte Binding Corporate Rules

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_informationnoteforgroupswithicoasbcrlead-sa_20200722_de.pdf

Übersicht zu allen Fragen rund um den Brexit, FAQs und eine allgemeine Guideline
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/statement-on-data-protection-and-brexit-implementation-what-you-need-to-do/

Twexit – Der Ausstieg aus Twitter

Wie bereits im vergangenen Tätigkeitsbericht 2019 angekündigt, sind wir bei Twitter ausgestiegen und haben den Account @lfdi_bw zum 31. Januar 2020 zurückgegeben. Seit November 2017 twitterte der Landesbeauftragte als einzige deutsche Datenschutz-Aufsichtsbehörde mit einem offiziellen Account über eigene News, kommentierte das aktuelle Datenschutz-Geschehen, tauschte sich in Diskussionen mit anderen Datenschützer_innen aus und war auch für unmittelbare Fragen ansprechbar. Der Account war erfolgreich - 3.000 abgesetzte Tweets und mehr als 5000 Follower stehen dafür.

Doch bereits die Facebook-Fanpage-Entscheidung des Europäischen Gerichtshofs vom 5. Juni 2018 (Az. C-210/16) verhieß für Social Media-Nutzer_innen nichts Gutes. In diesem Urteil erklärte das Gericht, dass auch Betreiber einer Fanpage neben dem Plattformbetreiber selbst als Verantwortliche im Sinne von Artikel 4 Nr. 7 DS-GVO anzusehen sind. Bei Datenschutzverstößen können sie demnach also nicht mehr alleine auf den Plattformbetreiber verweisen, sondern sind für die datenschutzkonforme Umsetzung vielmehr (mit) zuständig. Das führt auch dazu, dass zwischen den beiden gemeinsam Verantwortlichen ein Vertrag gemäß Artikel 26 DS-GVO abgeschlossen werden muss, in dem die Wahrnehmung der Pflichten durch die Parteien, wie beispielsweise die Information gegenüber Betroffenen, transparent und eindeutig geregelt werden muss.

Da solche Verträge in datenschutzgerechter Form nicht vorlagen und bis heute nicht vorliegen, war und ist für öffentliche sowie private Betreiber von Fanpages klar: Der Social Media-Auftritt kann so nicht in rechtskonformer Weise betrieben werden! Noch verstärkt durch ein Urteil des Bundesverwaltungsgerichts vom 11. September 2019 (Az. 6 C 15.18), das nicht nur die datenschutzrechtliche Verantwortlichkeit des Fanpagebetreibers bestätigt, sondern zugleich den Aufsichtsbehörden das Auswahlermessen zuspricht, zur Beseitigung von Rechtsverstößen beim Betrieb der Plattform wahlweise den Plattformbetreiber oder den Accountinhaber als „Störer“ in die Pflicht zu nehmen, blieb für den Betrieb des LfDI-Accounts bei Twitter kein Raum mehr.

© LfDI BW

Digitale Kommunikation ist datenschutzkonform möglich – zum Beispiel auf Mastodon.

Wenn auch grundsätzlich eine Verhandlungsbereitschaft seitens der Social Media-Betreiber durchaus erkennbar ist, so sind die meisten dieser Plattformen nach wie vor nicht datenschutzkonform nutzbar. Viele sammeln Daten von angemeldeten Nutzer_innen – und auch Nichtnutzer_innen (!) – und übermitteln Daten an Dritte, legen aber weder diese Vorgänge noch die verwendeten Technologien, die betroffenen Datenarten, Verarbeitungszwecke oder Empfänger hinreichend offen. Die Verarbeitungen erfolgen zudem oft ohne Rechtsgrundlage, wobei insbesondere die hohen Anforderungen an das Einholen einer Einwilligung nach Artikel 4 Nr. 11 DS-GVO nicht erfüllt werden. Und vor allem mangelt es zumeist an der Möglichkeit, als Accountinhaber_in selbst die geforderte und notwendige Vereinbarung nach Artikel 26 DS-GVO mit dem Betreiber abzuschließen.

Außerdem ergeben sich durch das am 16. Juli 2020 ergangene Urteil des Europäischen Gerichtshofs zu „Schrems II" (Az. C-311/18) nochmals aktuelle weitere Herausforderungen bei der Frage nach einer datenschutzkonformen Nutzung von Social Media-Plattformen wie Facebook und Twitter. In seiner Entscheidung erklärt das Gericht das EU-US-Privacy Shield für unwirksam, da das nationale amerikanische Recht insbesondere aufgrund der Zugriffsmöglichkeit seitens US-Sicherheitsbehörden kein mit der EU vergleichbares Datenschutzniveau darstellt. Dies hat die weitreichende Folge, dass das EU-US-Privacy Shield beim Datentransfer in die USA nicht mehr als Rechtsgrundlage herangezogen werden kann. Wie wir wissen, sitzen die Mutterkonzerne der meisten großen Social Media- Plattformen jedoch gerade in den USA. Häufig werden Daten auf Servern bei den Mutterkonzernen gehostet oder sind über Cloud-Lösungen mit diesen verbunden. Öffentliche Stellen, die dem Vorbehalt des Gesetzes unterliegen und in besonderem Maße rechtsstaatlichem Handeln unterworfen sind, müssen hier sehr sorgfältig und streng vorgehen – bislang führen wir zwar Gespräche mit den öffentlichen Stellen in Baden-Württemberg, grundlegenden Veränderungen sind jedoch bislang nicht zu beobachten. Aber auch Unternehmen und Vereine, die Social Media-Plattformen nutzen, sind hier gleichermaßen gefragt. Denn hier stellt sich ganz speziell die Frage, wie die Datenverarbeitung, die zwischen Fanpage-Betreibern und Social Media-Plattform stattfindet, die wiederum mit amerikanischen (Mutter-)Konzernen interagieren, datenschutzkonform möglich ist. Die Standarddatenschutzklauseln, welche der Gerichtshof in ebendiesem Urteil grundsätzlich weiterhin als rechtswirksam erachtet, müssen um „geeignete Garantien" zur Einhaltung eines angemessenen Datenschutzniveaus erweitert werden (mehr dazu in Kapitel 4). Eine genaue Prognose, was dies für die Fanpage-Betreiber auf Social Media Plattformen bedeutet, kann zum jetzigen Zeitpunkt jedoch noch nicht abgegeben werden. Es bleibt abzuwarten, welche Entscheidungen hier auf europäischer Ebene getroffen werden.

Einmal mehr stellt sich damit aber die Frage nach Alternativen zu Twitter und Co. Und da sieht es weiterhin nicht besonders komfortabel aus: Eine datenschutzkonforme Alternative zu Facebook ist weit und breit nicht in Sicht, Facebook ist jedenfalls in Europa quasi ein Monopolist, was sich negativ auf deren Veränderungsbereitschaft auswirken dürfte. Bei Twitter gibt es zwar mit Mastodon einen funktionstüchtigen Konkurrenten mit datenschutzkonformer dezentraler Struktur – dem fehlt es allerdings noch an Reichweite. Als Vorreiter sehen wir hier das Staatsministerium Baden-Württemberg, das als erstes im vergangenen Jahr einen Mastodon-Account eröffnet hat. Wir haben unseren Mastodon-Account Ende des vergangenen Jahres freigeschaltet – mit erstaunlich positiver Resonanz der Community. Auch weiterhin besteht gerade im öffentlichen Sektor die Chance, durch Aufbau einer eigenen staatlichen Plattform eine autarke und rechtmäßige Alternative zu schaffen. Mit unserem Server auf Mastodon bieten wir öffentlichen Stellen – Ministerien, Kommunen, Universitäten und weitere – an, sich bei uns einen Account einzurichten: stabil, einfach, rechtskonform. Private Nutzer_innen können sich bei anderen Instanzen einen Account anlegen und uns und den für sie besonders interessanten öffentlichen Stellen folgen – ohne dafür mit ihren persönlichen Daten bezahlen zu müssen.

Datenschutzkonforme Plattformen mit einem vergleichbaren Wirkungskreis sind bislang also leider noch nicht in Sicht. Dies betrifft alle öffentliche Stellen, Behörden und Hochschulen. Auch hier stellt sich die drängende Frage, wie man mit der Situation umgehen kann, da von Kommunen bis Hochschulen zumeist mehrere Social Media-Kanäle parallel genutzt werden, um mit Bürger_innen oder etwa Studierenden in Kontakt zu bleiben, Bürgernähe zu schaffen und wichtige Informationen einem möglichst breiten Zielpublikum zukommen zu lassen. So nachvollziehbar und sinnvoll die Gründe auch sind, warum Soziale Medien eingesetzt werden, die rechtliche Lage bleibt unumstößlich

und verbietet streng genommen die Nutzung der Monopolisten. Daher haben wir mehrfach das Gespräch mit Ministerien und Hochschulen gesucht, um über die Lage zu informieren und zu diskutieren, wie zum Beispiel im Arbeitskreis Datenschutz im Juni 2020 im Ministerium für Finanzen. Darüber hinaus veranstalteten wir gemeinsam mit der Hochschule der Medien (HdM) Stuttgart eine Online-Diskussion („Öffentlichkeitsarbeit ohne Likes, Tweets und Follower – Ist die Nutzung von Social Media durch Behörden und Hochschulen noch zulässig?"), um die verschiedenen Sichtweisen auf das Thema gemeinsam zu erörtern. Die Diskutanten aus Staatsministerium, Kommunen, Hochschulen und der Landesbeauftragte verständigten sich nach einer kontroversen Diskussion, weiterhin gemeinschaftlich das Thema zu bearbeiten.

Auch stehen wir mit einem Start-Up in Kontakt, welches schon jetzt die Möglichkeit bietet, die bestehenden Social Media-Kanäle der öffentlichen Stellen datenschutz- und benutzerfreundlich auf einer Plattform mitzulesen – auch, wenn dies die geschilderte Problematik der gemeinsamen Verantwortlichkeit nicht beseitigt, erscheint das Unternehmen auf einem guten Weg, sich durch die Weiterentwicklung seines Produkts zu einem hilfreichen Netzwerk zu entwickeln. Dieses kann so viel Anreiz bieten, sich nur dort und damit datenschutzkonform mit Informationen öffentlicher Stellen zu versorgen und mit diesen und anderen Nutzer_innen zu interagieren, so dass die eigentlichen Social Media-Kanäle der öffentlichen Stellen getrost zu vernachlässigen wären.

Bis es soweit ist bauen wir unsere eigenen Kommunikationskanäle aus. Wir haben für unseren Newsletter 4.500 Abonnenten, einen eigenen Podcast zum Datenschutz „Datenfreiheit!", von dem bereits 6 Folgen produziert und veröffentlicht wurden; und wir kommunizieren mit großem Einsatz über unseren neuen Mastodon-Account https://bawü.social/@lfdi (@lfdi@bawü.social). Mit unserem Twitter-Ausstieg ist die Welt jedenfalls nicht untergegangen – wir bleiben weiterhin kommunikativ und ansprechbar.

>> Weitere Informationen

Vertragsmuster zur Vereinbarung gemäß Art. 26 Abs. 1 S. 1 Datenschutz-Grundverordnung (DS-GVO)
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/05/190521_Vertragsmuster-Art-26.docx

Online-Diskussion mit der Hochschule der Medien (HdM) Stuttgart
„Öffentlichkeitsarbeit ohne Likes, Tweets und Follower – Ist die Nutzung von Social Media durch Behörden und Hochschulen noch zulässig?")

Info und Anmeldung Newsletter des Landesbeauftragten
https://www.baden-wuerttemberg.datenschutz.de/oeffentlichkeitsarbeit-ohne-likes-tweets-und-follower/

Podcast Datenfreiheit!
https://www.baden-wuerttemberg.datenschutz.de/datenfreiheit/

Mastodon
https://bawü.social/@lfdi

8. Bildungszentrum

Das Bildungszentrum Datenschutz und Informationsfreiheit Baden-Württemberg wurde am 1. Juli 2020 unter dem Motto „Datenschutz und Informationsfreiheit zum Anfassen“ gegründet. Ermöglicht wurde die Gründung dieses Forums für Datenschutz und Informationsfreiheit durch den Landtag. Wir haben Mittel und Stellen erhalten, um unser Bildungsangebot auszuweiten. Und die sehr positive Resonanz auf die Arbeit des Bildungszentrums bestätigt den eingeschlagenen Weg, niederschwellig und nah an den Akteuren im Land, Dienstleister für den Datenschutz und die Informationsfreiheit zu sein.

Mit dem Bildungszentrum wurde für Bürger_innen, Vereine, Verbände, Unternehmen, Behörden und zivilgesellschaftliche Gruppen eine Anlaufstelle geschaffen, die den Beratungsansatz der Landesbehörde innovativ weiterführt und fortsetzt. Auch wenn Rechtsfragen einen Schwerpunkt bilden, deckt das Bildungsangebot nicht nur rein rechtliche, sondern auch politische, soziologische oder ethische Fragestellungen ab.

Die gewählten Veranstaltungsformate verweisen auf die Vielfältigkeit der Themen, die behandelt werden sollen: Klassische Präsenzveranstaltungen wie Workshops, Schulungen, Vorträge und Konferenzen werden durch digitale Bildungsangebote wie Onlineveranstaltungen oder Videos ergänzt. Nach einem für ursprünglich für Herbst 2020 vorgesehenen Umzug der Behörde, der nun in den kommenden Monaten erfolgen soll, werden dem Bildungszentrum eigene Seminarräume mit moderner Veranstaltungstechnik zur Verfügung stehen.

Das Bildungszentrum profitiert als rechtlich nicht selbstständige Einrichtung von dem Fachwissen der Behördenmitarbeitenden. Neben fünf zusätzlichen Stellen, die wir für das Bildungszentrum erhalten haben, bringen sich auch die übrigen Referent_innen der Behörde mit ihrem Know-how ein.
Der Start des Bildungszentrums stieß auf sehr viel positive Resonanz. Es gab viel Zustimmung und Unterstützung – gerade auch von den Fraktionen unseres Landtags –, wir haben auch bereits zahlreiche Kooperationsangebote erhalten. Das zeigt: Der Bedarf an einem solchen Zentrum ist da! Angebotene Präsenzveranstaltungen waren so stark nachgefragt, dass sie schnell ausgebucht waren. Den verschobenen Umzug vom Herbst ins kommende Jahr konnten wir anfangs noch kompensieren. Doch die 2. Welle der Corona-Pandemie machte unseren Planungen einen dicken Strich durch die Rechnung. Alle für das Jahr 2020 vorgesehenen Präsenzveranstaltungen mussten abgesagt werden. Es ist derzeit offen, ab wann vor Ort wieder Veranstaltungen angeboten werden können. Doch das Bildungszentrum stellt sich dieser Herausforderung und baut nun das digitale Bildungsangebot mit unterschiedlichen Formaten noch schneller aus. Auch die Inhalte der abgesagten Präsenzveranstaltungen werden soweit wie möglich in digitaler Form angeboten, etwa als Online-Veranstaltungen. Wo dies nicht möglich ist, sollen die geplanten Präsenzveranstaltungen im Laufe des Jahres 2021 nachgeholt werden.

Wichtig für unsere Arbeit hier ist es, dass wir Anregungen aufnehmen. Wir sind eine lernende Einrichtung, die sich den Bedürfnissen und aktuellen Erfordernissen anpasst. Wir reagieren zügig auf gesetzliche Änderungen, nehmen unmittelbar auf, wenn Unternehmen Fragen zur datenschutzrechtlichen Praxis haben und unterstützen weiterhin die vielen Vereine und ehrenamtlich Engagierten, die ebenfalls aufgrund der Pandemie vermehrt digital arbeiten und hier datenschutzkonform aktiv sein wollen.

>> Weitere Informationen
Zum Veranstaltungsangebot des BIDIB
https://www.baden-wuerttemberg.datenschutz.de/offene-veranstaltungen/

© LfDI BW
Das Bildungszentrum erfreut sich großer Nachfrage.

9. Datenschutz als KULTuraufgabe

Datenschutz so ganz anders

In der Vergangenheit haben wir im Zusammenhang mit „Datenschutz als KULTuraufgabe" gerne nachgefragt, welche Assoziationen Bürger_innen haben, wenn sie an eine Behörde denken, deren Hauptaufgabe es ist, sich mit dem Thema Datenschutz zu befassen. Zu weiten Teilen sind die Antworten genauso ausgefallen, wie es viele vermuten würden (und wie wir es befürchtet haben).

Viele assoziierten Datenschutz mit Paragraphen und Erklärungen, die derzeit bei jedem Kontakt, sei es bei einem Arztbesuch oder auch bei Online-Einkäufen, abzugeben sind. Man macht in der jeweiligen Alltagssituation ganz eigene Erfahrungen mit dem Thema Datenschutz, aber die Wenigsten verbinden damit etwas Positives oder sogar etwas Spannendes oder Unterhaltsames.

Doch im Laufe des vergangenen Jahres haben wir mit großer Freude festgestellt, dass die Antworten auf Fragen nach den Assoziationen zum Thema Datenschutz eben nicht mehr wie zuvor befürchtet ausfallen, sondern dass sich in der Wahrnehmung der Bürger_innen etwas Grundlegendes verändert hat. Wir merken dies auch daran, dass unsere Veranstaltungen und unsere Kooperationen ein wachsendes Publikum erreichen.

Zwischenzeitlich erreichen uns Anfragen und Nachrichten, die deutlich zum Ausdruck bringen, dass unser Veranstaltungsformat, Datenschutz als KULTuraufgabe, und die daraus resultierenden Aktionen, in anderen Behörden, von anderen Institutionen und Unternehmen und von Bürger_innen genau verfolgt und die neuen Veranstaltungen bzw. Veröffentlichungen bereits erwartet bzw. geradezu eingefordert werden – und all das weit über die Grenzen von Baden-Württemberg hinaus.

War es doch ein mutiger Ansatz, das Thema Datenschutz auf einer kulturellen und teilweise künstlerischen Ebene zu transportieren. Insbesondere, weil dieser Ansatz zu Beginn die Gemüter erregt hat – einige haben diesen Neustart belächelt und skeptisch beäugt, andere wiederum haben ihn von Anfang an mit Spannung verfolgt.

Zwischenzeitlich dürfte hinlänglich klar sein, dass mit dem ungewöhnlichen Ansatz – Daten zum KULTurgut zu erklären, nicht nur eine Änderung der Kommunikation und der Wahrnehmung in der Gesellschaft einhergeht. Es geht vielmehr darum, auch eine Erweiterung der Zielgruppe zu erreichen und Datenschutz als Alltagspraxis und Kulturtechnik zu erkennen. Plötzlich wird es möglich, mit Menschen ins Gespräch zu kommen und sie für ein Thema zu sensibilisieren, für das sie sich bisher nicht interessiert haben – oder es sogar ausdrücklich ablehnten. Viele von ihnen hätten es nicht einmal in Erwägung gezogen, einen klassischen Vortrag zum Thema Datenschutz zu besuchen oder an einer Fachkonferenz dazu teilzunehmen. Unser besonderer und gleichzeitig unkomplizierter Ansatz konnte allen – unabhängig von gesellschaftlicher Stellung, Ausbildungsgrad oder kulturellem Hintergrund – einen Zugang zu einem komplexen und abstrakten Thema verschaffen und dabei eine Menge an Vorurteilen, die mit diesem Thema verknüpft wurden, abbauen. Letztendlich konnten wir damit ein Fundament legen für eine kritische und gut informierte Auseinandersetzung mit den wirklich grundlegenden Fragen des Datenschutzes im Alltag. Und genau das ist es, worum es in der DS-GVO geht. In Artikel 57 der DS-GVO ist geregelt, dass die Öffentlichkeit durch die Aufsichtsbehörden zu beraten, zu informieren, zu sensibilisieren und aufzuklären ist. Besonders werden hier spezifische Maßnahmen für Kinder hervorgehoben. Aus diesem Grund haben wir das Jahr 2020 zum Jahr der Kinderrechte und des Kinderschutzes erklärt.

Auch dieser Bereich unserer Arbeit litt unter Corona-Pandemie. Datenschutz als KULTuraufgabe hat den Auftrag, bestehende Kontakte mit Bürger_innen

© Alexas_Fotos_pixabay

Datenschutz ist unsere Kulturaufgabe.

aufrechtzuerhalten und neue Kontakte zu initiieren und möglich zu machen. Dazu ist es unerlässlich, im wahrsten Sinne des Wortes greifbar, sichtbar und tatsächlich präsent zu sein – all das, was durch den ersten Lockdown im Frühjahr dieses Jahres vollständig und später weitestgehend unterbleiben sollte. Natürlich wäre es einfach gewesen, Datenschutz als KULTuraufgabe einfach so lange ruhen zu lassen, bis sich die durch die Pandemie begründete Ausnahmesituation wieder gelegt hat – aber das haben wir nicht getan. Das ist einfach nicht unser Ding! Also haben wir uns der Herausforderung gestellt und Datenschutz als KULTuraufgabe digitalisiert.

Herbstkonferenz Datenschutz

Im Oktober 2020 waren wir ein weiteres Mal Schirmherr der Herbstkonferenz Datenschutz. Veranstalter dieser von unserer Behörde initiierten Fachtagung ist der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.. Die Schirmherrschaft übernehmen zudem die beiden bayrischen Kollegen Michael Will, Präsident des Bayerischen Landesamtes für Datenschutzaufsicht, und Prof. Dr. Thomas Petri, bayrischer Landesbeauftragter für Datenschutz. Wie bereits in den vergangenen beiden Jahren blickten wir die ersten beiden Tage der Konferenz intensiv auf das Verhältnis von „Wirtschaft“ und „Aufsicht“, getreu unserem Motto „Wirtschaft trifft Aufsicht“ – auch in der Pandemie.

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.

Geplant war diese Datenschutzkonferenz zunächst als Hybridveranstaltung. Die im Vorfeld der Herbstkonferenz erneut ansteigenden Infektionszahlen haben uns jedoch gezwungen, das Veranstaltungsformat abzuändern. Eine Präsenzveranstaltung erschien nicht mehr realisierbar. Plan B war eine Live-Übertragung der Rednerbeiträge aus einem eigens dafür eingerichteten Studio. Doch die stetig steigenden Infektionszahlen machten auch diesen Plan zunichte. Uns blieb nur noch die Veranstaltung abzusagen oder Plan C auszurufen. Letztendlich haben wir uns für Plan C entschieden und alle Vortragenden von ihrem jeweiligen Aufenthaltsort zugeschaltet. In Anbetracht von rund 150 Teilnehmenden an jedem der drei Tage und Referent_innen im Inland und verschiedenen europäischen und außereuropäischen Ländern war dies nicht nur eine technische Herausforderung. Eine solche Resonanz für eine Veranstaltung in digitaler Form ist bemerkenswert und macht auch in der Digitalversion einmal mehr deutlich, dass der Austausch zwischen Unternehmen und Behörden mit den Aufsichtsbehörden in der „Datenschutz-Szene“ nicht mehr wegzudenken ist. So werden wir dieses Format auch in diesem Herbst fortführen.

Die Herbstkonferenz Datenschutz bietet Fachvorträge, Diskussionen, Expertengespräche, Handlungsleitfäden, 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 und werden fortgesetzt.
Erstmalig präsentieren wir im Nachgang zu der Herbstkonferenz die Präsentationen unserer Behörde auf unserer Homepage. Wir werden diese Praxis beibehalten und im Laufe der Zeit damit ein Nachschlagewerk in Form einer „Experten-Bibliothek“ etablieren.

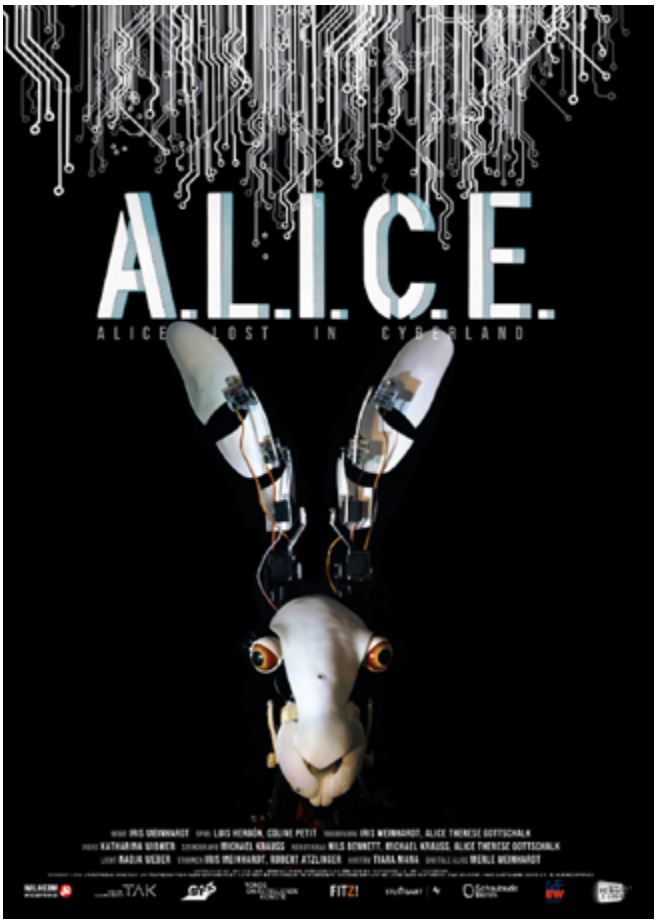
Spotlights

Um mit den Bürger_innen in Austausch zu bleiben haben wir mit unseren „Spotlights“ dazu eingeladen, sich und gute Projekte auf unserer Homepage zu präsentieren. Die Idee hinter den „Spotlights“ ist, mit vielen verschiedenen kurzen Spots zu erzählen, wie es Einzelnen von uns in dieser so ganz anderen Zeit der Pandemie ergangen ist, welche Erfahrungen gemacht, welche Erkenntnisse gewonnen oder welche Dinge dabei kreativ geschaffen werden konnten. Ganz bewusst sollten bei den „Spotlights“ nicht die Erörterung rechtlicher (Datenschutz-)Fragen im Vordergrund stehen, sondern KULTurelle bzw. zwischenmenschliche Themen beleuchtet werden.

Datenschutz ist kein Thema, das einen eng begrenzten Lebensbereich betrifft – an dieser Stelle beginnt und an einer anderen genau definierten Stelle endet. Datenschutz ist in erster Linie der Schutz der Freiheit, die Förderung der Selbstbestimmung und damit ein Bürgerrecht. Datenschutz gewährleistet jedem Einzelnen von uns ein Recht auf Bestimmung, Erfindung, Veränderung und Neukonzeption des Bildes von uns selbst und auf unsere ganz eigene Privatsphäre.

Einige der Spotlights erlauben uns einen Blick hinter die Kulissen, einen kleinen Blick in die jeweilige Privatsphäre des anderen. Auch das ist nämlich Freiheit - entscheiden zu können, welchen Einblick ich anderen gewähre, ob überhaupt und wenn ja, wieviel ich von mir und meiner Privatsphäre preisgebe. Dabei sind wunderbare Momentaufnahmen entstanden, die wir von Ende Mai bis Ende Juli 2020 wöchentlich, immer mittwochs präsentiert haben – denn: Mittwoch war bei uns Spotlight-Tag!

Einen ähnlichen Gedanken hatte auch die Behörde der Datenschutzbeauftragten des Kantons Zürich. Dr. Dominika Blonski hat im Sommer 2020 nachgefragt, welche Themen die Menschen in Corona-Zeiten beschäftigen und dazu einen Videowettbewerb ausgerufen. Im Rahmen einer gemeinsamen, grenzüberschreitenden und damit internationalen Zusammenarbeit der Aufsichtsbehörden konnten wir die Gewinnerbeiträge des Videowettbewerbs der Schweizer Kollegen Ende September 2020 auf unserer Homepage unter dem Motto „Spot an … die Zweite! Datenschutz als KULTuraufgabe digital & international“ präsentieren.



© Meinhardt & Krauss

Ein voller Erfolg: „Alice lost in Cyberland“.

Alice lost in Cyberland

Wir wussten, dass wir damit ein sehr schönes Projekt begleiten, aber die enorme Resonanz hat uns dann doch überrascht. Mit „A. L. I. C. E. Alice lost in cyberland“ (Spotlight Nummer sieben) haben uns die Figurenspielerin und Regisseurin Iris Meinhardt, der Regisseur und Videokünstler Michael Krauss und der Komponist und Musiker Thorsten Meinhardt einen kleinen Einblick in ihre künstlerische Arbeit und die Welt des modernen Figurentheaters gewährt. „A. L. I. C. E. Alice lost in Cyberland“ basiert auf der (Kinder-) Geschichte „Alice im Wunderland“ von Lewis Carroll. Meinhardt & Krauss ist es gelungen, den (Kinderbuch-)Klassiker aus dem Jahr 1865 auf beeindruckende Weise in ein Robotermärchen zu transformieren: Wie der aktuelle Titel bereits vermuten lässt, bewegt sich „Alice im Cyberland“, in einer Welt, die nur allzu viel Potential bietet, um sich in ihr zu verlieren und „das scheinbar Unwirkliche für wahr zu nehmen“. Ist das nicht eine der zentralen Frage, die uns alle und insbesondere uns Freiheitsschützer, aktuell ganz besonders umtreibt?

A.L.I.C.E bietet in ihrer Verschmelzung von phantasievollem Figurentheater und digitalisierter (Kinder-) Geschichte jede Menge Anknüpfungspunkte und Gesprächsstoff über das Thema Datenschutz, Freiheit und Privatsphäre und all das in einem digitalen (Kinder-)Zimmer. Wir freuen uns sehr, dass Alice und das Kaninchen unser Portfolio von Datenschutz als KULTuraufgabe auf so spannende und surreale Art bereichert.

Im Rahmen unserer Spotlights ist dabei eine Kooperation mit Meinhardt & Krauss entstanden, die wir auch im nächsten Jahr, soviel kann bereits verraten werden, mit einem weiteren (digitalen) Kinderprojekt fortsetzen werden, das an „Alice lost in Cyberland“ in spielerischer Form anknüpft. In den vergangenen Jahren sind einige Kooperationen entstanden, die sich erfreulicherweise als besonders nachhaltig erweisen. Kinder, Jugendliche und junge Erwachsene werden so auf das Spannungsfeld aufmerksam, das zwischen stetig zunehmender Öffentlichkeit und dem Wert der Privatsphäre und der informationellen Selbstbestimmung besteht.

Eine frühzeitige Diskussion über die Bedeutung des Datenschutzes ist gerade für die „digital natives“ elementar. Sie bewegen sich spielend leicht in der digi-

talen Welt und sind gleichzeitig extrem betroffen. Es muss unser gemeinsames gesellschaftliches Ziel sein, unseren Nachwuchs so gut zu informieren, zu schulen und fortzubilden, dass er oder sie sich in einer digitalen Welt nicht nur souverän, sondern auch sicher bewegen kann – und das ist nicht nur in technologischer Hinsicht gemeint.

Datenschutz geht zur Schule

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 aus. Die Initiative sensibilisiert Schüler_innen zu einem bewussten Umgang mit dem Internet und den sozialen Medien. Wie in den vergangenen Jahren haben wir auch in diesem Jahr parallel dazu die Kolleg_innen der anderen Datenschutzaufsichtsbehörden zu einer gemeinsamen und koordinierten Aktion über die Ländergrenzen hinweg eingeladen. Die länderübergreifende Abstimmung und Koordination lag dabei wie bisher in Baden-Württemberg. Bedauerlicherweise konnten wir die geplanten Präsenzveranstaltungen in den Schulen aufgrund der ansteigenden Infektionszahlen leider nicht durchführen.

Doch auch hier lassen wir uns durch die aktuelle Situation nicht entmutigen. Als absehbar wurde, dass uns die Thematik der Pandemie und die damit verbundenen Einschränkungen bei Präsenzveranstaltungen noch einige Zeit begleiten werden, haben wir den Vertretern der Initiative „Datenschutz geht zur Schule" vorgeschlagen, online verfügbare Videos für eine Version „Datenschutz geht zur Schule – digital" zu produzieren. Auch hier sind schon die ersten Zeichen erkennbar, dass unsere bisherige länderübergreifende Zusammenarbeit der Aufsichtsbehörden auch in digitaler Form ihre Fortsetzung finden kann. Geplant ist eine Produktion von mehreren themenbezogenen Einzelbausteinen zum Ende des ersten Quartals 2021. Als „Hauptdarsteller" der Videos sind Vertreter_innen der Aufsichtsbehörden und aus der Gruppe der ehrenamtlich Aktiven von „Datenschutz geht zur Schule" vorgesehen.

Kooperation mit der Dualen Hochschule Baden-Württemberg

Die seit mehreren Jahren bestehende Kooperation mit der Dualen Hochschule Baden-Württemberg (DHBW) konnten wir zu erfreulicherweise auch in diesem Jahr fortführen. „privacy by dhbw" stellt sich der Frage, wie Menschen für den Datenschutz sensibilisiert und mit welchen technischen Werkzeugen sie dabei unterstützt werden können.

Wieder einmal mehr konnten die Studierenden unter der fachkundigen Anleitung von Professor Dr. Tobias

© smolaw11 – stock.adobe.com

Kinder sollten einen bewussten Umgang mit dem Internet und Sozialen Medien erlernen.

Straub, Michael Schlegel und Ivana Marevic beweisen, dass Datenschutz kein trockenes und abstraktes Thema bleiben muss. Die Wirtschaftsinformatik-Studierenden des 5. Semesters nahmen die Herausforderung mit kreativer Leidenschaft an und zeigten im Rahmen eines Wettbewerbs, dass Unternehmenstrainings zum Thema Datenschutz und Datensicherheit nicht nur langweilige Pflichtübungen sein müssen. Den studentischen Teams ist es gelungen, Datenströme und Datenübertragungen zu visualisieren. Darüber hinaus erarbeiteten sie verschiedene Schulungskonzepte u. a. für einen sicheren E-Mail-Versand.

Eine Jury – besetzt mit Martina Strifler aus der Behörde des Landesbeauftragten, Dr. Rolf Häcker (Landtag Baden-Württemberg), Tobias Birk (PROFI AG) und Christoph Haas (UKBW) – hatte die schwierige Aufgabe, unter mehreren sehr guten Arbeiten einen Gewinner zu ermitteln. Letztlich fiel die Entscheidung zugunsten eines von Studierenden entwickelten Spiels. Datenschutz kann auch zum Gegenstand eines „serious game“ und zu „virtual reality“ werden. Das mit einer 3D-Brille spielbare Spiel „solve the privacy issues“, das als Escape Room konzipiert ist, überzeugte die Jury durch seine technisch professionelle Umsetzung und die Tatsache, dass datenschutzrechtlich relevante Sachverhalte auf unterhaltsame und spielerische Art und Weise vermittelt werden können.

Die sehr erfolgreiche Kooperation mit der Dualen Hochschule Baden-Württemberg führen wir auch im aktuellen Semester fort.

Datenschutz kinderleicht
„Ach wie gut, dass niemand weiß …“

Nachdem wir so wunderbare Erfahrungen mit unseren Kooperationspartnern Duale Hochschule Baden-Württemberg und der BvD-Initiative „Datenschutz geht zur Schule“ bei der Sensibilisierung von Jugendlichen und jungen Erwachsenen sammeln konnten, war es an der Zeit, auch ein Konzept für die Kleinsten zu entwickeln. Unter dem Motto „Datenschutz kinderleicht“ haben wir uns in diesem ungewöhnlichen Jahr daran gewagt, einen ersten Teilaspekt des Themas für Kinder im Kindergartenalter aufzubereiten. Wir haben das Märchen „Rumpelstilzchen“ künstlerisch interpretiert und kleinen Kindern auf spielerische Weise die Bedeutung des eigenen Namens vermittelt. Ein Kinderlied durfte natürlich nicht fehlen, und dankbar sind wir dafür, dass die Wiener Sängerin und Komponistin Daniela Flickentanz, die unserem Haus ja schon länger und wunderbar inspirierend verbunden ist, sich an diesem Projekt beteiligt hat. Eine Präsentveranstaltung war pandemiebedingt nicht möglich, mit „Datenschutz kinderleicht – Teil 1 – Rumpelstilzchen“ wird demnächst aber eine Toolbox inklusive eines Videos auf unserer Homepage zur Verfügung gestellt.

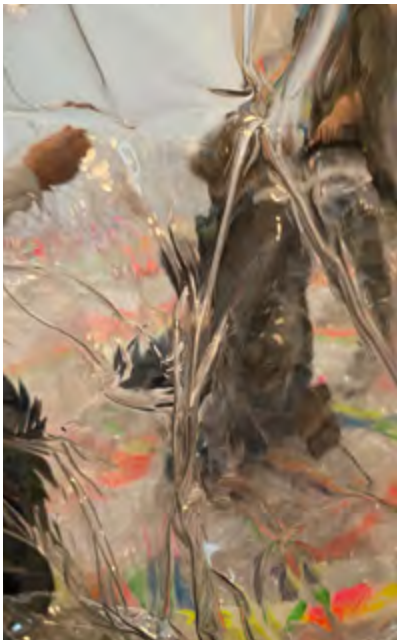
Online-Tagung mit der HdM Stuttgart: „Daten schützen – Kinder schützen.“

Zum Abschluss unserer Arbeit im vergangenen Jahrhaben haben wir das Thema „Daten schützen – Kinder schützen!“ fortgeführt. Zusammen mit Hochschule der Medien, Institut für Digitale Ethik, Stuttgart, haben wir im Dezember eingeladen zur Online-Tagung „Daten schützen – Kinder schützen. Datenschutz und Überwachung in Familie und Alltag“.

Hier haben wir darüber diskutiert, wie der spezielle Schutz von Kindern im Zuge des immer stärker datengeprägten Alltags sichergestellt werden kann. Eltern tracken ihre Kinder, Spielzeug überwacht die Kinder, im Netz sind Kinder oftmals unterwegs ohne zu wissen, wie sie sich und ihre Daten schützen. Gerade für die Jüngsten ist es wichtig, denn: Ohne ein Recht auf Vergessenwerden ist es sehr wahrscheinlich, dass im Netz öffentlich gemachte Informationen über Jahrzehnte auffindbar bleiben. Wissen Kinder das? Können sie absehen, was das bedeutet? Wir wollten mit einer Tagung für diese Themen sensibilisieren und darauf hinwirken, dass ein bewusster Umgang mit personenbezogenen Daten zum Schutz der Kinder an Bedeutung gewinnt.

Wie es auch schon im Rahmen des gemeinsamen Kunstprojekts „Social Distance Stacks“ mit Florian Mehnert zum Ausdruck gebracht wurde: Soziale Distanz führt dazu, dass wir vermehrt in digitaler Form kommunizieren und auch handeln und dies führt unweigerlich zu viel, viel mehr Datenspuren als vor der Pandemie (mehr dazu weiter unten). Und all das gilt nicht nur für die „Großen“, es gilt für uns alle – für Jugendliche, für Kinder und teilweise auch schon für Kleinkinder. Das Thema wird akut, sobald Kinder in der Lage sind, einen PC, ein Tablet oder ein Smartphonezu bedienen, dazu müssen sie nicht unbedingt auch schon lesen und schreiben können.

Die angebotenen Vorträge haben das Themengebiet aus psychologischer, juristischer, ethischer und teil-



© Florian Mehnert

Datenspurensuche: Making of „Social Distance Stacks“ vom Konzeptkünstler Florian Mehnert.

weise auch philosophischer Sicht vielfältig beleuchtet. Dabei ist ein Aspekt ganz besonders in den Vordergrund zu stellen: Kinder entdecken die Welt, in der sie leben, und sie sehen sie auch mit ganz anderen Augen als wir Erwachsenen. Kinder sind und waren schon immer Pioniere und das gilt in heutiger Zeit insbesondere auch für die digitale Welt. Nicht umsonst sprechen wir von „digital natives".

Es sollte zu unseren Hauptaufgaben gehören, die kleinen Pioniere auf ihrer Entdeckungsreise durch die (digitale) Welt zu begleiten und sie dabei bestmöglich zu schützen. Eine der großen Fragen dabei lautet: Wie können wir den Schutz, den wir Kindern und Jugendlichen in der analogen Welt angedeihen lassen, in die digitale Welt transferieren?

Social Distance Stacks

Den sonst als eher trüb und neblig geltenden Monat November hat der Konzeptkünstler Florian Mehnert zur Datenspursuche genutzt. Mitarbeitende der Behörde wurden in riesige, durchsichtige PVC-Luftblasen eingepackt und gemeinsam fotografiert. Vor der eigentlichen Foto-Session wurde das gesamte Treppenhaus des Gebäudes Königstraße 10 a, Stuttgart mit bunt gesprayten und damit sichtbar gemachten Datenspuren ausgelegt. Unter dem Motto „Social Distance Stacks – Datenschützer gehen in Corona-Zeiten den Datenspuren nach" verdeutlichte Florian Mehnert auf sehr anschauliche Art, dass soziale Distanz nicht nur zu vermehrter digitaler Kommunikation führt, sondern damit unweigerlich auch zu einem erheblichen Anstieg der Datenspuren, die wir dabei hinterlassen.

>> Weitere Informationen

Übersicht über alle Angebote und Veranstaltungen
https://www.baden-wuerttemberg.datenschutz.de/datenschutz-als-kulturaufgabe

„Spotlights"
https://www.baden-wuerttemberg.datenschutz.de/spotlights/#alle-spotlights)

Präsentationen der BvD Herbstkonferenz 2020
https://www.baden-wuerttemberg.datenschutz.de/jetzt-online-verfuegbar-praesentationen-der-bvd-herbstkonferenz-datenschutz-und-behoerdentag-2020/

Spot an … die Zweite! Datenschutz als KULTuraufgabe digital & international
https://www.baden-wuerttemberg.datenschutz.de/videowettbewerb-dsb-zh-2020/#alle-videos

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

„Daten schützen – Kinder schützen" – Kooperation mit der Hochschule der Medien Stuttgart
https://www.baden-wuerttemberg.datenschutz.de/ideepolis2020-daten-schuetzen-kinder-schuetzen/

Kooperationsprojekte mit der Dualen Hochschule Baden-Württemberg (DHBW)
https://studium.dhbw-stuttgart.de/winf/studierendenprojekte/privacy-by-dhbw/

https://studium.dhbw-stuttgart.de/winf/studierendenprojekte/privacy-by-dhbw/solve-the-privacy-issues-serious-game/

10. Datenschutz-Vielfalt, veranschaulicht von Fall zu Fall

10.1 Neues aus dem Amt I: Innere Sicherheit, Justiz, Kommunalwesen,

Auskunft durch den Verfassungsschutz

Dass wir uns mit dem Landesamt für Verfassungsschutz in juristische Grundsatzdiskussionen verstricken, kommt eher selten vor. Ein in der Sache eher weniger spektakulärer Fall einer Bürgerin, der die Auskunft durch das Landesamt über die zu ihrer Person gespeicherten Daten verweigert wurde, führte aber dann doch zu einer längeren Auseinandersetzung, in die auch das Innenministerium eingeschaltet wurde, und die bis heute noch nicht ganz ausgestanden ist. Es geht um Folgendes:

§ 13 Absatz 3 Satz 1 des Landesverfassungsschutzgesetzes (LVSG) räumt Bürger_innen grundsätzlich einen Anspruch darauf ein, vom Landesamt für Verfassungsschutz Auskunft darüber zu erhalten, was dort über sie gespeichert ist. Formal setzt dieser Anspruch voraus, dass man auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an der Auskunft darlegt. Diese Einschränkungen des Auskunftsanspruchs sollen den Verwaltungsaufwand reduzieren und eine gezielte Ausforschung des Erkenntnisstands des Landesamts verhindern. Uns Datenschützern gefällt diese sehr restriktive Regelung natürlich nicht – aber so sieht es momentan aus. Tatsächlich lässt sich gerade das besondere Interesse an der Auskunft nur schwer begründen; ein solches wurde von der Rechtsprechung bisher nur in wenigen Fallkonstellationen anerkannt (Arbeit als Journalist, Stellung als Abgeordneter). Regelmäßig scheiterte der Auskunftsanspruch deshalb allein daran. Umso mehr kommt dem Umstand Bedeutung zu, dass nach Auffassung der Rechtsprechung selbst dann, wenn die formalen Voraussetzungen des § 13 Absatz 1 Satz 1 LVSG nicht vorliegen und deshalb eine Auskunft nicht erteilt werden muss, es dem Landesamt immer noch freisteht, diese trotzdem zu erteilen (dürfen statt müssen). Dem Landesamt ist insoweit ein Ermessen eingeräumt, dass es jedenfalls ausüben und über das es auch Rechenschaft ablegen muss. Darauf hat jede und jeder einen Anspruch.

Diese Freiheit, Auskunft auch noch erteilen zu können, auch wenn es hierzu nicht verpflichtet ist, hatte das Landesamt in der jüngerenVergangenheit aufgrund eines aus unserer Sicht fehlerhaften Verständnisses einer verwaltungsgerichtlichen Entscheidung nicht gesehen. Soweit deshalb Auskunftsanträge allein wegen Fehlens der formalen Voraussetzungen des § 13 Absatz 1 Satz 1 LVSG abgelehnt wurden, war dies fehlerhaft. Tatsächlich hätte man bei sorgfältiger Prüfung feststellen können, dass es eine ganze Reihe höchstrichterlicher Entscheidungen gibt, die klarstellen, dass ein solcher Anspruch auf ermessensfehlerfreie Entscheidung besteht. So stellte das Bundesverwaltungsgericht bereits im Jahr 1990 fest, dass dann, wenn sich ein Anspruch auf Auskunft über die zur eigenen Person gespeicherten Daten weder dem Grundgesetz noch einfachgesetzlichen Bestimmungen entnehmen lasse, der betroffenen Person gleichwohl die Auskunftserteilung nicht schlechthin verwehrt sei. Soweit nicht ein gesetzliches Auskunftsverbot eingreife, stehe sie vielmehr im pflichtgemäßen Ermessen der Behörde:

„Es besteht daher Übereinstimmung in Rechtsprechung und Literatur darüber, dass die Auskunftserteilung durch die von der Auskunftsverpflichtung freigestellten Behörden in deren Ermessen liegt." (Bundesverwaltungsgericht, BVerwGE 84, 375-390).

Diese Rechtsprechung setzte sich in der Folge fort. So schreibt das Bundesverfassungsgericht in seinem Beschluss vom 10. Oktober 2000 (1 BvR 586/90, 1 BvR 673/90):

„§ 15 Abs. 1 BVerfSchG [Anm.: § 15 Abs. 1 Satz 1 BVerfSchG entspricht wortgleich dem § 13 Abs. 1 Satz 1 LVSG] macht die Auskunftspflicht von dem Hinweis auf einen konkreten Sachverhalt und von einem besonderen Auskunftsinteresse abhängig. […] Aber auch soweit [die Beschwerdeführerin] keine näheren Angaben macht, ist § 15 Abs. 1 BVerfSchG nicht zu entnehmen, dass das Bundesamt für Verfassungsschutz ihren Antrag ohne weiteres ablehnen dürfte. Nach dem einfachgesetzlichen Regelungsgehalt, der unter Beachtung der Grundrechtsvorgaben auszulegen und anzuwenden ist, entfällt in einem solchen Fall lediglich die Auskunftspflicht (vgl. auch die Beschlussempfehlung und den Bericht des Innenausschusses, BT-Drucks. 12/4094, S. 3, 11 ff.). Das verbleibende Ermessen, Auskunft zu erteilen, ist nach Maßgabe des Zwecks der Regelung auszuüben."

Bis heute hat sich diese Rechtsprechung gehalten. Im Urteil des Bundesverwaltungsgerichts vom 24. März

2010 (6 A 2/09) steht unter Hinweis auf die genannte Entscheidung des Bundesverfassungsgerichts:

„Soweit die Voraussetzungen des § 15 Abs. 1 BVerfSchG nicht vorliegen, entfällt lediglich die gesetzliche Auskunftspflicht. Das verbleibende Ermessen, Auskunft zu erteilen, ist in einem solchen Fall nach Maßgabe des Zwecks der Regelung auszuüben."

Und im Urteil vom 15. Juni 2016 (6 A 7/14) führt das Bundesverwaltungsgericht aus:

„Das durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG gewährleistete Grundrecht auf informationelle Selbstbestimmung wird bei einem fehlenden Zugang zum Wissen Dritter über die eigene Person berührt und verschafft seinem Träger auch Rechtspositionen, die den Zugang zu den über ihn gespeicherten persönlichen Daten betreffen. Subsidiär zu dem gesetzlich normierten Auskunftsanspruch tritt daher ein aus dem informationellen Selbstbestimmungsrecht herzuleitender Anspruch des Betroffenen auf ermessensfehlerfreie Entscheidung über sein Auskunftsbegehren gegenüber dem Bundesnachrichtendienst. Der Regelungsgehalt der gesetzlichen Vorschriften erschöpft sich in der Normierung einer Auskunftspflicht und lässt das verbleibende Ermessen, Auskunft zu erteilen, unberührt (vgl. …). Dies gilt zum einen in den Fällen, in denen die Voraussetzungen für die Pflicht zur Auskunftserteilung nach § 7 Satz 1 BNDG i.V.m. § 15 Abs. 1 BVerfSchG nicht vorliegen, muss aber mit Blick auf das informationelle Selbstbestimmungsrecht zum anderen in gleicher Weise gelten, wenn – wie hier – die Auskunftspflicht an der gesetzlichen Ausschlussregelung des § 15 Abs. 3 BVerfSchG scheitert. Der subsidiäre Anspruch auf ermessensfehlerfreie Entscheidung über das Auskunftsbegehren kann sich grundsätzlich auch auf die Herkunft und die Empfänger von Übermittlungen personenbezogener Daten erstrecken (…)." (zuletzt ebenso: BVerwG, Beschluss vom 28. Juli 2020 – 6 B 62/19 –, juris; OVG NRW, Urteil vom 31. Juli 2019 – 16 A 1009/14 –, juris).

Es kostete einige Mühe, das Landesamt von diesem Verständnis des § 13 Absatz 1 LVSG zu überzeugen, letztlich führte es aber doch dazu, dass das Landesamt seine Praxis änderte und nun bei Fehlen der formalen Voraussetzungen des § 13 Absatz 1 Satz 1 LVSG auch das Ermessen ausübt. So weit, so gut!

© BillionPhotos.com – stock.adobe.com

Der Verfassungsschutz darf Auskunftsersuchen nicht per se ablehnen.

So ganz wollte das Landesamt dann aber doch nicht beidrehen und änderte seine Argumentation. Es stellte sich nun auf den Standpunkt, es handle sich hier nicht um ein „freies" (kann), sondern um ein „intendiertes" (soll) Ermessen. Ein „Für und Wider" brauchte dabei nur dann abgewogen zu werden, wenn der Fall so geartet sei, dass ganz bestimmte konkrete Anhaltspunkte für die Angemessenheit einer Ausnahme vorliegen (atypischer Sonderfall). Hierzu beruft sich das Landesamt auf Gerichtsentscheidungen, die diese Rechtsauffassung allerdings (unserer Auffassung nach) nicht stützen.

Zwar gibt es durchaus Rechtsprechung zu Auskunftsregelungen in den Verfassungsschutzgesetzen, die von einem intendierten Ermessen ausgehen. Allerdings geht es bei diesen Normen um solche, denen ein (inhaltliches) Geheimhaltungsinteresse zugrunde liegt. So etwa § 13 Absatz 1 Satz 3 LVSG:

„Das Landesamt für Verfassungsschutz ist nicht verpflichtet, über die Herkunft der Daten und die Empfänger von Übermittlungen Auskunft zu erteilen."

Hier ist es in der Tat vertretbar, von einem Vorrang des Geheimhaltungsinteresses gegenüber einem unspezifischen Auskunftsinteresse eines Betroffenen auszugehen. Anders dagegen in den Fällen des § 13 Absatz 1 Satz 1 und 2 LVSG. Diese haben (lediglich) zum Ziel, einen im Hinblick auf das Informationsinteresse unverhältnismäßigen Verwaltungsaufwand zu vermeiden und Ausforschungsgefahren zu begegnen. Hier ist eine Vorfestlegung der Entscheidung durch den Gesetzgeber weder erfolgt noch begründbar. Deshalb haben wir gegenüber dem Landesamt weiter vertreten, dass es verpflichtet ist, in Fällen, in denen ein Auskunftsanspruch daran scheitert, dass die formalen Voraussetzungen des § 13 Absatz 1 Satz 1 LVSG nicht vorliegen, auch ohne Anhaltspunkte für das Vorliegen eines „atypischen Sonderfalles" zu prüfen, ob sich der Verwaltungsaufwand gemessen an dem Informationsinteresse des Auskunftsbegehrenden konkret als verhältnismäßig oder unverhältnismäßig darstellt. Dabei sehen wir uns durch neuere Gerichtsentscheidungen gestärkt. So führt das OVG NRW in seinem Urteil vom 31. Juli 2019 (16 A 1009/14) aus:

„Insoweit folgt der Senat nicht der vom Verwaltungsgericht Köln [...] geäußerten Auffassung, dass die Rechtsprechung des Bundesverwaltungsgerichts zu einem intendierten Ermessen im Bereich des § 15 Abs. 3 BVerfSchG auf den Bereich des § 15 Abs. 1 BVerfSchG übertragbar sei. [...] Vor diesem Hintergrund genießt das Geheimhaltungsinteresse im Regelfall Vorrang vor dem Interesse des Betroffenen an einer Auskunft über die Herkunft und die Empfänger seiner Daten. Dass dieser Vorrang allenfalls in atypischen Ausnahmefällen nicht greift, rechtfertigt die Annahme von intendiertem Ermessen im Bereich des § 15 Abs. 3 BVerfSchG und stellt zugleich den entscheidenden Unterschied zu den mit § 15 Abs. 1 BVerfSchG verfolgten Zielen dar, die nicht mit einer vergleichbaren Regelmäßigkeit zu einer ablehnenden Entscheidung führen müssen und das Ermessen hinsichtlich der Auskunftserteilung nicht vorstrukturieren."

Weiter führt es zur Gefahr der Ausforschung aus:

„Soweit das Bundesamt in seinem Widerspruchsbescheid vom 12. August 2009 meint, der Gesetzgeber sei im Rahmen des § 15 Abs. 1 Satz 1 BVerfSchG davon ausgegangen, dass bei jedem Auskunftsersuchen eine latent vorhandene, abstrakte Ausforschungsgefahr bestehe, der zu begegnen sei, so dass es bei seiner Ermessensausübung nicht auf konkrete Anhaltspunkte für eine Ausforschungsgefahr ankomme, besagt die hierfür vom Bundesamt zitierte Entscheidung des Bundesverfassungsgerichts genau das Gegenteil. Danach stellt im Rahmen der Ermessensentscheidung des Bundesamtes die Begegnung von Ausforschungsgefahren einen legitimen Belang dar, „sofern die gestellten Anforderungen mit Rücksicht auf die konkrete Erfüllung der jeweiligen Aufgabe erforderlich und im Hinblick auf das jeweilige Informationsinteresse verhältnismäßig sind."

Weiter heißt es:

„Die Möglichkeit, jeden Antrag, mit dem Auskunft über sämtliche zur Person gespeicherten Daten begehrt wird, pauschal abzulehnen, ergibt § 15 Abs. 1 BVerfSchG nicht."

Auch das Bundesverwaltungsgericht geht in seinem Beschluss vom 28. Juli 2020 (6 B 62/19) lediglich bei dem § 13 Absatz 1 Satz 3 LVSG entsprechenden § 15 Absatz 3 BVerfSchG von einem intendierten Ermessen aus:

„Daher kann daraus nicht geschlossen werden, der Gesetzgeber habe den allgemein anerkannten Er-

messensanspruch ausschließen oder auf besonders gelagerte Ausnahmefälle beschränken wollen."

Weiter heißt es:

„[Das] Interesse, einen unverhältnismäßigen Aufwand für die behördeninterne Suche nach Daten zu vermeiden, [...] ist nach seiner Bedeutung nicht mit dem Interesse an dem Schutz der nachrichtendienstlichen Arbeitsweise vergleichbar, das nach der Wertung des Gesetzgebers den generellen Vorrang der Geheimhaltung der Herkunft von Daten und deren Weitergabe rechtfertigt. [...] hat das § 15 Abs. 1 Satz 2 BVerfSchG zugrunde liegende Interesse, einen übermäßigen Aufwand für die Suche nach Daten in den Aktenbeständen zu vermeiden, ein erheblich geringeres Gewicht. Die damit bezweckte Arbeitsentlastung des Bundesamts ist nicht gleichermaßen existenziell für die Gewährleistung der nachrichtendienstlichen Aufgabenerfüllung. Die Ablehnung [aus Gründen übermäßigen Aufwands] setzt allerdings eine fallbezogene Abwägung mit der Bedeutung des Auskunftsinteresses voraus."

Mit dieser Entscheidung hat das Bundesverwaltungsgericht der Verfassungsschutzbehörde gleichzeitig auch den Wind aus den Segeln genommen, indem es klarmacht, dass der für die Bearbeitung von Auskunftsansprüchen zu erbringende Verwaltungsaufwand nicht per se zu einer Ablehnung des Antrags führen darf. Allein ein hoher Verwaltungsaufwand kann regelmäßig nicht rechtfertigen, betroffenen Personen pauschal ihre Datenschutzrechte zu verweigern. Das Landesamt für Verfassungsschutz kann hier grundsätzlich keine Sonderstellung gegenüber anderen Verwaltungsbehörden für sich beanspruchen.

© were – stock.adobe.com

Datenschutz braucht Kontrolle.

Angesichts des zwischenzeitlichen teilweisen Einlenkens besteht die berechtigte Erwartung, dass sich das Landesamt für Verfassungsschutz diese Rechtsprechung zu Herzen nimmt und dem verfassungsrechtlichen Auskunftsinteresse der Bürger_innen in seiner Auskunftspraxis künftig die Bedeutung zumisst, die ihm zukommt. Wir werden weiter genau dafür eintreten.

Was lange währt, wird endlich gut? – Licht und Schatten beim neuen Polizeigesetz

Am 17. Januar 2021 tritt das neue Polizeigesetz (vom 6. Oktober 2020, GBl. S. 735) in Kraft. Mit einer Verzögerung von mehr als zweieinhalb Jahren kommt der Landesgesetzgeber damit seiner Verpflichtung nach, die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (kurz: JI-Richtlinie) fristgerecht zum 6. Mai 2018 umzusetzen. Dass die lange Dauer des Umsetzungsprozesses (die JI-Richtlinie war immerhin schon am 6. Mai 2016 in Kraft getreten, man hatte also bereits zwei Jahre „Vorlaufzeit") nicht allein der Schwierigkeit der Materie geschuldet war, darf angenommen werden. Bedauerlich, dass die notwendige Anpassung der gefahrenabwehrrechtlichen Datenverarbeitungsbefugnisse der Polizei offenbar (wieder einmal) zum Gegenstand politischer Verhandlungen geworden war. Im Bereich der Strafverfolgung war man da wesentlich schneller: Das Gesetz zum Schutz personenbezogener Daten bei der Verarbeitung durch die Justizbehörden des Landes zu Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten und Ahndung von Ordnungswidrigkeiten oder zum Zwecke der Strafvollstreckung sowie durch die Behörden des Landes zum Zwecke der Ahndung von Ordnungswidrigkeiten (kurz: Landesdatenschutzgesetz für Justiz- und Bußgeldbehörden – LDSG-JB) trat (immerhin ein Jahr nach Ablauf der Umsetzungsfrist) bereits am 6. Juni 2019 in Kraft!

Die Hoffnung, dass die lange Phase der Umsetzung dafür genutzt werde, auch für die Polizei ein modernes, anwenderfreundliches Polizei-Datenschutzrecht zu schaffen, erfüllte sich nur zum Teil. Dabei wird

nicht verkannt, dass die Umsetzung der europarechtlichen Vorgaben sowie die Anpassung an die aktuelle Rechtsprechung des Bundesverfassungsgerichts keine leichte Aufgabe darstellte. Von daher soll an dieser Stelle auch einmal durchaus anerkennend erwähnt werden, dass hier ein ordentliches Stück Arbeit geleistet wurde und man sich erkennbar bemüht hat, unter den gegebenen Rahmenbedingungen allen Anforderungen gerecht zu werden. Völlig ist das aber leider nicht gelungen. Unsere schon im Rahmen unserer Beteiligung im Gesetzgebungsverfahren vorgebrachte Kritik bezog und bezieht sich insbesondere auf Folgendes:

• Anstatt die allgemeinen Datenverarbeitungsregelungen in einem Abschnitt zusammenzufassen, wurden sie ohne wirklich nachvollziehbaren Grund auseinandergerissen, so dass man bei der konkreten Anwendung im Gesetz hin- und herspringen muss – anwenderfreundlich geht anders.

• An vielen Stellen wird durch Verweisungen auf andere Normen Bezug genommen. Das Zusammenwirken der verschiedenen Tatbestandsmerkmale und dieser Verweisungen ergibt im Gesamtgefüge der gewählten Regelungstechnik Mängel an hinreichender Normenbestimmtheit und Normenklarheit.

• Teilweise ergibt sich aus dem Text nicht unmittelbar, unter welchen Voraussetzungen die Norm verfassungskonform anzuwenden ist; erst durch Hinzuziehung der Gesetzesbegründung wird dies deutlich. Diese hat aber nicht jede Polizeibeamtin/jeder Polizeibeamte täglich zur Hand. Fehlinterpretationen sind damit vorprogrammiert. Es ist unerfindlich, weshalb der Gesetzgeber die Normanwender solchermaßen im Dunkeln tappen lässt. Und eigentlich sollen ja die Bürger_innen die Gesetze verstehen und anwenden können.

• Einzelne Paragrafen sind derart komplex, dass sie auch für Datenschutzexperten nur schwer zu verstehen sind (bspw. § 15). Auch der schiere Umfang einzelner Bestimmungen dürfte die Praxis in der Anwendung vor manche Probleme stellen (bspw. § 49 mit 8 Absätzen, wobei allein Absatz 8 insgesamt 13 Sätze enthält). Den Ruf, ziemlich kompliziert zu sein, haben die Datenschützer auch wegen solcher überkomplexer Regulierungen (die wir gar nicht initiiert oder gefordert haben).

Neben diesen formalen Gesichtspunkten, die das Risiko falscher Normanwendung und damit von Datenschutzverstößen in sich bergen, haben wir aber auch inhaltlich das eine oder andere kritisiert:

• So sollen die Datenverarbeitungsregelungen etwa auch gelten, soweit die Polizei im Rahmen der Verfolgung von Straftaten oder Ordnungswidrigkeiten tätig wird. Hier sehen wir keine Gesetzgebungskompetenz des Landes. § 500 der Strafprozessordnung schreibt für den Bereich der Strafverfolgung vielmehr die alleinige Anwendbarkeit des Teils 3 des Bundesdatenschutzgesetzes vor.

• Die Datenverarbeitungsregelungen sollen nicht nur für die Polizeidienststellen gelten, sondern auch für die Einrichtungen für den Polizeivollzugsdienst (Präsidium Technik, Logistik, Service der Polizei, Hochschule der Polizei). Zu den Aufgaben dieser Einrichtungen gehört jedoch nicht die Gefahrenabwehr, so dass zu fragen ist, wozu sie dann berechtigt sein sollen, Daten zu verarbeiten, die im Rahmen der Gefahrenabwehr anfallen.

• Die beharrliche Weigerung, das Datengeheimnis als gesetzliche Vorgabe in das Polizeigesetz aufzunehmen, ist nicht nachvollziehbar. Gerade die in den letzten Monaten wiederholt festgestellten Fälle unberechtigter Datenabrufe aus polizeilichen Datenbeständen hätte es dringend erfordert, den Beschäftigten des Polizeivollzugsdiensts durch eine entsprechende ausdrückliche gesetzlich Regelung nochmals deutlich vor Augen zu führen, wann und wo ihre Berechtigung zur Nutzung personenbezogener Daten endet. Die Weigerung mit dem Hinweis auf die dienstliche Verschwiegenheitspflicht zu begründen, geht ins Leere, da schon die Kenntnisverschaffung als solche unzulässig ist. Das, so zeigt es die Praxis, scheint einigen Polizeibeamtinnen und Beamten aber nicht in aller Deutlichkeit klar zu sein.

• Ein gravierender Mangel besteht darin, dass der Datenschutzaufsichtsbehörde wirksame Befugnisse vorenthalten werden, um gegen Datenschutzverstöße durch die Polizei wirksam einzuschreiten. Das Gesetz beschränkt sich auf die Möglichkeit, auf Gesetzesverstöße hinzuweisen und die Polizei aufzufordern, diese abzustellen. Die mangelhafte Umsetzung des Artikels 47 der JI-Richtlinie verstößt gegen die Umsetzungspflicht und ist damit europarechtswidrig. Es ist völlig klar, welche Konsequenzen sich für uns daraus erge-

ben. Ebenso klar ist, wie der Europäische Gerichtshof über solche Umsetzungsmängel urteilen wird.

Fazit also: Licht und Schatten, wobei zu hoffen bleibt, dass es gelingt, die Schatten in der Praxis zunehmend aufzuhellen. Wir werden von unserer Seite bemüht sein, die Fackel des Datenschutzes hochzuhalten, um auch in diesem sensiblen Bereich Sicherheit für die handelnden Akteure wie für die betroffenen Bürger_innen herzustellen.

Ist eine private Stelle verpflichtet, der Polizei Auskünfte zu erteilen?

Diese Frage wurde uns in den vergangenen Monaten häufig gestellt. Oftmals handelte es sich dabei um Unternehmen, die im Zusammenhang mit strafrechtlichen Ermittlungen um Auskunft, z. B. über einen ihrer Kunden ersucht wurden. Die Polizeibeamt_innen hatten den Unternehmen dabei jeweils die Kopie eines von einer Staatsanwaltschaft stammenden Schreibens vorgelegt, das an ein Polizeipräsidium gerichtet war. Diese uns von den Unternehmen weitergereichten Schreiben stammen zwar von verschiedenen Staatsanwaltschaften, sind inhaltlich jedoch gleichlautend. In den Schreiben beauftragt die jeweilige Staatsanwaltschaft die Beamt_innen eines Polizeipräsidiums unter Hinweis auf die Verpflichtung der Polizei zur Erforschung von Straftaten, die für die Sachverhaltsaufklärung erforderlichen Auskunfts- und Herausgabeersuchen zu stellen. Die allgemein gehaltenen Ausführungen beziehen sich nicht auf einen konkreten Einzelfall.

Wichtig für die angefragten Unternehmen ist dies: Aus diesen Schreiben ergibt sich keine Verpflichtung Privater, der Polizei im Rahmen von Ermittlungsverfahren Auskunft zu erteilen. Gemäß § 163 Absatz 1 Strafprozessordnung (StPO) ist die Polizei zwar berechtigt, Ermittlungen jeder Art durchzuführen (die mit einem weniger intensiven Grundrechtseingriff verbunden sind und deshalb nicht von einer speziellen Eingriffsermächtigung erfasst werden) und alle Behörden um Auskunft zu ersuchen. Eine Auskunftsverpflichtung der Polizei gegenüber ergibt sich aus dieser Vorschrift jedoch nur für Behörden und ausschließlich bei Gefahr im Verzug. Bis vor wenigen Jahren bestand für Zeugen lediglich die Pflicht, bei staatsanwaltschaftlichen Vernehmungen zu erscheinen. Erst seit der am 24. August 2017 in Kraft getretenen Änderung des § 163 Absatz 3 StPO ist ein Zeuge verpflichtet, auf Ladung vor Ermittlungspersonen der Staatsanwaltschaft – hierbei handelt es sich um bestimmte Beamten des Polizeidienstes – zu erscheinen und zur Sache auszusagen. Voraussetzung ist jedoch, dass dieser Ladung ein konkreter einzelfallbezogener Auftrag der Staatsanwaltschaft zugrunde liegt. Bei den uns vorgelegten Schreiben handelt es sich nicht um derartige Aufträge im Sinne des § 163 Absatz 3 StPO.

Das von den Staatsanwaltschaften verwendete Schreiben erweckt bei den Angesprochenen oftmals den falschen Eindruck, dass private Stellen aufgrund dieses Schreibens verpflichtet seien, der Polizei gegenüber Auskunft zu erteilen. Dies ergibt sich aus den bei uns eingehenden Anfragen. Wir haben daher das Justizministerium gebeten, die Staatsanwaltschaften darüber zu unterrichten, dass das verwendete Schreiben missverständlich ist und daher umformuliert werden sollte. Das Justizministerium hat sich in seinem Antwortschreiben zwar unserer Rechtsauffassung angeschlossen, dass es sich bei dem Schreiben mangels Einzelfallbezugs nicht um Aufträge gemäß § 163 Absatz 3 StPO handelt. Eine Umformulierung hält das Justizministerium dagegen nicht für erforderlich. Das ist bedauerlich, denn öffentliche Stellen sollten Bürger_innen gegenüber nicht den Anschein erwecken, über Befugnisse zu verfügen, die ihnen von Gesetzes wegen nicht zustehen. Und schon der Plan, Unsicherheit bei Privaten über ihre Mitwirkungspflichten zu schaffen und zu nutzen, wäre unserem Rechtsstaat nicht angemessen.

Falls ein Unternehmer auf ein bloßes Auskunftsersuchen freiwillig Angaben machen will, ist dies seine Entscheidung, für die er die (auch datenschutzrechtliche) Verantwortung trägt. Die Berechtigung, der Polizei auf

© Karl-Heinz H – stock.adobe.com

Die Polizei darf nicht immer Auskunft verlangen.

Ersuchen personenbezogene Daten eines Kunden zu übermitteln, kann sich aus § 24 Absatz 1 Nummer 1 des Bundesdatenschutzgesetzes (BDSG) ergeben. Nach dieser Vorschrift ist die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen z. B. dann zulässig, wenn sie zur Verfolgung von Straftaten erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen. Wendet sich die Polizei mit einem Auskunftsersuchen an einen Unternehmer, sollte dieser der Polizei dementsprechend erst einmal dahingehend antworten, dass er das Ersuchen vor einer freiwilligen Beantwortung prüfen muss. Im Falle der Übermittlung empfehlen wir, die insoweit angestellten Überlegungen zu dokumentieren; gegenläufige Interessen der von der Ermittlung Betroffenen kann der Unternehmer übrigens nur dann kennen und in seine Abwägungsentscheidung einbeziehen, wenn er die Betroffenen zuvor befragt (was die Polizei regelmäßig nicht möchte und ggf. ihr Auskunftsersuchen lieber zurückzieht). Im Übrigen ist § 24 Absatz 2 BDSG zu beachten, soweit es um sensitive Daten im Sinne des Artikels 9 der DS-GVO geht.

Eine Verpflichtung, die betroffenen Personen über die Offenlegung ihrer Daten gegenüber Strafverfolgungsbehörden gemäß Artikel 13 Absatz 3 der DS-GVO zu informieren, besteht nach der Ausnahmeregelung in § 32 Absatz 1 Nummer 5 BDSG nicht in jedem Fall – ist aber (solange es nicht mit dem Ziel der Strafvereitelung erfolgt) auch nicht verboten.

Die Revanche

Dass auch Polizeibeamt_innen das Menschliche nicht abgeht, ist nicht neu und bedarf eigentlich keiner Erwähnung. Dumm nur, wenn es allzu menschlich wird und dabei der Verstand aussetzt. So in einem Fall, der uns, was selten genug vorkommt, zu einer Beanstandung veranlasste.

Ein Bürger wandte sich an uns und trug Folgendes vor: Seine Ehefrau habe bei einem Polizeirevier Strafanzeige gegen einen Nachbarn wegen Bedrohung erstattet. Der die Anzeige aufnehmende Polizeibeamte habe dabei deutlich erkennen lassen, dass er den Beschuldigten kenne. Er habe deshalb versucht, die Erstatterin der Anzeige dazu zu bewegen, von der Anzeige abzusehen. Diese sei hierauf aber nicht eingegangen. Im Zuge der weiteren Vernehmung zur Person habe der Beamte wohl den Verdacht gewonnen, dass die Anzeigeerstatterin und deren Ehemann gegen melderechtliche Bestimmungen verstoßen haben könnten. Deshalb habe er bei der zuständigen Gemeinde eine Ordnungswidrigkeit angezeigt und dieser auch gleich das komplette Protokoll, das er über die im Rahmen der Strafanzeige erfolgte Zeugenvernehmung angefertigt hatte, zugeleitet.

Das um Stellungnahme zu dem Vorgang ersuchte Polizeipräsidium brauchte geraume Zeit, um uns dann mitzuteilen, der Beamte könne sich an nichts mehr erinnern und Akten lägen auch keine mehr vor. Über den Beschwerdeführer – der sich mittlerweile gegen das wegen eines Verstoßes gegen die melderechtliche Pflicht, den Wechsel seines Wohnsitzes der Meldebehörde anzuzeigen, verhängte Bußgeld gewehrt hatte – konnte dann doch noch eine Kopie der Unterlagen gerettet werden. Diese belegten eindeutig, dass der Vortrag des Beschwerdeführers den Tatsachen entsprochen hatte. Das Polizeipräsidium, dem wir diese Unterlagen zur Prüfung der datenschutzrechtlichen Seite des Vorgangs zugeleitet hatten, kam letztlich zum Ergebnis, dass der Beamte zwar nicht berechtigt gewesen sei, die komplette Vernehmung an die Gemeinde zu senden, im Übrigen sei sein Vorgehen aber nicht zu beanstanden gewesen. Insbesondere sei die Anzeige einer Ordnungswidrigkeit hier zulässig gewesen. Wie man zu diesem Ergebnis gekommen war, wurde nicht erklärt. Eine Auseinandersetzung mit der von uns zuvor schriftlich und mündlich dargestellten Rechtslage schenkte man sich.

Es stand hier außer Zweifel, dass der Verdacht einer Ordnungswidrigkeit erst im Zuge der Durchführung eines Strafverfahrens, nämlich aufgrund der Angaben der als Zeugen vernommenen Anzeigeerstatter entstanden war. Mit Anzeigeerstattung hatte das Strafverfahren begonnen. Nach § 477 Absatz 1 der Strafprozessordnung dürfen personenbezogene Daten aus Strafverfahren von Amts wegen den zuständigen Behörden für Zwecke der Verfolgung von Ordnungswidrigkeiten zwar übermittelt werden, soweit diese Daten aus der Sicht der übermittelnden Stelle hierfür erforderlich sind. Allerdings entscheidet nach § 480 Absatz 1 Satz 1 StPO hierüber die Staatsanwaltschaft. Deren Entscheidung war hier aber nicht eingeholt worden. Der Polizeibeamte hat vielmehr eigenmächtig und offenbar aus Ärger darüber, dass er die Betroffenen nicht davon abbringen konnte, gegen seinen Bekannten Anzeige zu erstatten, unter

Missachtung seiner fehlenden Zuständigkeit und damit unzulässig personenbezogene Daten übermittelt. Der Versuch des Polizeipräsidiums, dies nachträglich mit Bezugnahme auf Datenübermittlungsbefugnisse nach dem Polizeigesetz zu rechtfertigen, konnte aufgrund des Vorrangs der strafprozessualen Bestimmung hier nicht verfangen.

Das aus unserer Sicht nonchalante Hinweggehen des Polizeipräsidiums über die Rechtsgrundlagen der Datenverarbeitung bewog uns letztlich, dies gegenüber dem Innenministerium zu beanstanden. Wie schon Konfuzius sagte: „Wer einen Fehler macht und versucht, diesen Fehler zu verdecken, der begeht einen zweiten Fehler."

Das Führungszeugnis

Nicht Wenige waren schon einmal mit der Forderung konfrontiert, ein Führungszeugnis, früher bekannt als polizeiliches Führungszeugnis oder Unbescholtenheitszeugnis, vorzulegen. Seine rechtliche Grundlage findet dieses Zeugnis im Bundeszentralregistergesetz (BZRG). Das Führungszeugnis gibt Auskunft darüber, was zur eigenen Person im Bundeszentralregister eingetragen ist. Dieses beinhaltet im Wesentlichen strafgerichtliche Verurteilungen sowie bestimmte Entscheidungen von Verwaltungsbehörden und Gerichten, durch die beispielsweise wegen Unzuverlässigkeit, Ungeeignetheit oder Unwürdigkeit die Beschäftigung, Beaufsichtigung, Anweisung oder Ausbildung von Kindern und Jugendlichen verboten wird.

In einem Fall, der uns eine Weile beschäftigt hat, ging es um Folgendes:

In einer Gemeinde hat sich eine Flüchtlingshilfeorganisation gebildet. Dabei handelt es sich um gemeinsame Initiative der politischen Gemeinde und Kirchen, die von zahlreichen Ehrenamtlichen unterstützt und getragen wird. Selbsterklärtes Ziel ist es, eine „Willkommenskultur" zu etablieren und für die Geflüchteten, die in der Gemeinde leben, Angebote zu schaffen, die eine Integration erleichtern.

Ein Bürger, der sich ehrenamtlich an der Arbeit der Flüchtlingshilfe beteiligen wollte, hatte jedoch Bedenken hinsichtlich der Forderung der Gemeinde, als Voraussetzung hierfür erst einmal ein erweitertes Führungszeugnis vorzulegen. Dazu muss man wissen, dass ein erweitertes Führungszeugnis erheblich mehr sensitive Informationen erhält als ein einfaches Zeugnis. Aus diesem Grund stellt das Bundeszentralregistergesetz auch weitergehende Anforderungen an die Vorlage solcher Zeugnisse. So wird es etwa nur dann erteilt, wenn dies gesetzlich ausdrücklich vorgesehen ist oder wenn jemand im weitesten Sinne

© stokkete – stock.adobe.com

Eine Gemeinde darf nicht pauschal von Ehrenamtlichen ein erweitertes Führungszeugnis verlangen.

Umgang mit Minderjährigen hat. So dürfen sich die Träger der öffentlichen Jugendhilfe nach § 72a des Sozialgesetzbuchs (SGB) - Achtes Buch (VIII) Kinder- und Jugendhilfe - bei der Einstellung oder Vermittlung und in regelmäßigen Abständen von den Personen, die Aufgaben in der Kinder- und Jugendhilfe wahrnehmen, ein solches erweitertes Führungszeugnis vorlegen lassen. Dabei hat, wer einen Antrag auf Erteilung eines erweiterten Führungszeugnisses stellt, nach § 30a Absatz 2 BZRG eine schriftliche Aufforderung vorzulegen, in der die Person, die das erweiterte Führungszeugnis vom Antragsteller verlangt, bestätigt, dass die gesetzlichen Voraussetzungen für ein solches erweitertes Führungszeugnis vorliegen. Gar nicht so einfach also.

Im konkreten Fall war es so, dass die Gemeinde pauschal von jeder Person, die sich im Rahmen der Flüchtlingshilfe ehrenamtlich betätigen wollte, ein solches erweitertes Führungszeugnis einforderte. Da es hierfür keine gesetzliche Grundlage gab, insbesondere § 72a SGB VIII nicht zutraf, verlegte man sich auf individuelle Einwilligungen. Die hierfür verwendeten Vordrucke entsprachen jedoch in keiner Weise den gesetzlichen Anforderungen an eine wirksame datenschutzrechtliche Einwilligung. Unter Einwilligung ist jede Willensbekundung zu verstehen, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden (BGH, Urteil vom 28. Mai 2020 – I ZR 7/16 –). „In Kenntnis der Sachlage" bedeutet,

„dass der für die Verarbeitung Verantwortliche der betroffenen Person eine Information über alle Umstände im Zusammenhang mit der Verarbeitung der Daten in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zukommen lassen muss, da dieser Person insbesondere die Art der zu verarbeitenden Daten, die Identität des für die Verarbeitung Verantwortlichen, die Dauer und die Modalitäten dieser Verarbeitung sowie die Zwecke, die damit verfolgt werden, bekannt sein müssen. Solche Informationen müssen diese Person in die Lage versetzen, die Konsequenzen einer etwaigen von ihr erteilten Einwilligung leicht zu bestimmen, und gewährleisten, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird" (EuGH, Urteil vom 11.11.2020 - C-61/19 -).

Solche Informationen fehlten vollständig. Auch wurde den Betroffenen nicht, wie § 30a BZRG verlangt, die schriftliche Aufforderung zur Beibringung des erweiterten Führungszeugnisses an die Hand gegeben, die bestätigte, dass die gesetzlichen Voraussetzungen für die Erteilung eines solchen Zeugnisses vorlagen. Schließlich konnte auch nicht überzeugend dargelegt werden, dass es – jedenfalls generell – solcher Zeugnisse bedurft hätte. Vorgetragen wurde hierzu nur, dass in allen Bereichen und Projektgruppen ein unmittelbarer und hinreichender Kontakt zu Kindern und Jugendlichen bestehe. Weder war dies zu belegen, noch kam es im Ergebnis darauf an. Hierzu kann auf folgende Ausführungen im Urteil des Landesarbeitsgerichts Hamm (Westfalen) vom 25. April 2014 (10 Sa 1718/13) verwiesen werden:

„§ 30a BZRG trägt dem Umstand Rechnung, dass es bei bestimmten beruflichen oder ehrenamtlichen jugend- und kindernahen Tätigkeiten ein Bedürfnis für ein erweitertes Führungszeugnis gibt, weil sich Menschen mit pädophilen Neigungen bewusst Betätigungsfelder mit einer Nähe zu Kindern und Jugendlichen suchen. Damit es nicht zu Lücken beim Schutz von Kindern und Jugendlichen kommt, ist ein Führungszeugnis auch für Personen vorgesehen, die in einer der Beaufsichtigung, Betreuung, Erziehung oder Ausbildung vergleichbaren Weise die Möglichkeit haben, Kontakt zu Minderjährigen herzustellen. Hierunter können beispielsweise Hausmeister an Schulen oder Bademeister in einem öffentlichen Schwimmbad fallen (BT-Drs. 16/12427, S. 8). Andererseits darf die Auslegung und Anwendung des § 30a BRZG nicht zu einer uferlosen Verpflichtung zur Vorlage von Führungszeugnissen führen. Denn stets sind auch die grundgesetzlich geschützten Interessen des betroffenen Arbeitnehmers zu berücksichtigen. Erforderlich ist stets die Bedingung, dass die jeweilige Berufsgruppe bestimmungs- oder arbeitsplatzgemäß Kontakt mit Kindern und Jugendlichen hat, der zu einer besonderen Gefahrensituation werden kann."

Tätigkeiten jedenfalls, bei denen es nicht „bestimmungs- oder arbeitsplatzgemäß", sondern mehr oder weniger zufällig zu Kontakten mit Minderjährigen kommen kann, können damit allenfalls im Einzelfall die Forderung nach Vorlage eines Führungszeugnisses begründen, wenn Tatsachen zur Annahme berechtigen, dass es dabei zu besonderen Gefahrensituationen kommt. Andernfalls steht das Grundrecht auf Datenschutz einer solchen Forderung entgegen.

Es bedurfte hier erst der Intervention unsererseits beim Bürgermeister, ehe die Verwaltung beidrehte und uns mitteilte, dass auf die Erhebung erweiterter Führungszeugnisse bei ehrenamtlich in der Flüchtlingshilfe tätigen Personen künftig verzichtet werde.

Die „Liste der Auffälligen" – Fortsetzung folgte

Vor einem Jahr hatten wir über die sogenannte Liste der Auffälligen berichtet, welche die Stadt Tübingen angelegt hatte, um behördenintern Informationen über Asylbewerber streuen zu können, die wegen Rohheitsdelikten auffällig geworden waren. Insbesondere die zögerliche Haltung der Stadt, uns im Bemühen um eine Klärung der datenschutzrechtlichen Berechtigung für das Führen einer solchen Liste zu unterstützen, bewog uns, damit an die Öffentlichkeit zu gehen. Auch wenn sich an der Grundeinstellung der Stadt auch im Berichtszeitraum nicht Wesentliches geändert hat, war es letztlich doch möglich, in einen vernünftigen Dialog zu treten. In diesem Rahmen fand im Sommer ein persönliches Gespräch zwischen dem Landesbeauftragten und dem Oberbürgermeister von Tübingen statt. Letztlich blieben die unterschiedlichen Rechtsauffassungen jedoch nicht miteinander vereinbar. Damit blieb nichts anderes übrig, als nach Recht und Gesetz zu entscheiden. Dies führte dazu, dass der Stadt untersagt wurde, bestimmte Informationen aus dem Besitz der Ausländerbehörde in die Liste aufzunehmen und bereits aufgenommene Informationen wieder zu löschen.

Diese Entscheidung wurde nicht nur vom OB, sondern auch von einigen Bürger_innen mit Verständnislosigkeit aufgenommen und zum Teil heftig kritisiert. Uns wurde vorgeworfen, der Bevölkerung sowie den Behördenmitarbeitenden den Schutz vor gewalttätigen Ausländern zu verwehren. Dabei wurde verkannt, dass die Aufgabe der Datenschutzaufsichtsbehörde darin besteht, auf die Beachtung zum Schutz des informationellen Selbstbestimmungsrechts erlassener Gesetze hinzuwirken, und dies ohne Ansehung der Person oder Herkunft. Und genau dies haben wir getan. Folgendes zur Verdeutlichung:

Der Staat mit allen seinen Ausprägungen ist bei der Verarbeitung personenbezogener Daten ganz besonders dazu verpflichtet, die hierfür gezogenen gesetzlichen Grenzen zu beachten. Denn im Gegensatz zum privaten Bereich hat die Bürgerin und der Bürger in den meisten Fällen keinen Einfluss darauf, wie Behörden mit ihren/seinen Daten umgehen. Man muss sich also darauf verlassen können, dass sich die Behörden an die Regeln halten. Dies war nach unserer rechtlichen Prüfung bei der Stadt Tübingen mit ihrer Liste der auffälligen Asylbewerber offensichtlich nicht der Fall.

Bei der gegenständlichen Liste handelte es sich um eine Excel-Tabelle. In dieser wurden personenbezogene Daten aus unterschiedlichen Bereichen der Stadtverwaltung zusammengeführt. Grundsätzlich ist es so, dass eine fachübergreifende Zusammenführung von Daten, die jeweils zu einem speziellen Verwaltungszweck von einer Fachbehörde auf einer speziellen gesetzlichen Grundlage erhoben wurden und für diesen Zweck auch legal genutzt werden, nur zulässig ist, wenn das Gesetz eine solche Zweckänderung ausdrücklich zulässt.

Hier war es so, dass in der Liste personenbezogene Daten von Asylbewerbern, welche die städtische Ausländerbehörde vom Polizeipräsidium Reutlingen erhalten hatte und weiter erhält (und erhalten darf), mit Daten aus anderen Bereichen zusammengefasst wurden. Die Datenübermittlungen durch das Polizeipräsidium erfolgen auf der Grundlage des § 87 Absatz 4 Satz 1 des Aufenthaltsgesetzes (AufenthG) allein zu ausländerrechtlichen Zwecken. Nach der Gesetzesbegründung ist die unverzügliche Unterrichtung durch die in § 87 Absatz 4 Satz 1 AufenthG genannten Stellen an die Ausländerbehörde erforderlich, damit diese ggf. eine anstehende Entscheidung über den Aufenthaltstitel aussetzen kann (vgl. BT-Drs. 11/6321, 82 f.). Die Zwecke der „Liste der Auffälligen" werden von der Stadt in ihrem datenschutzrechtlichen Verfahrensverzeichnis dagegen mit dem „Schutz der Mitarbeitenden im Integrationsmanagement (Fachabteilung Hilfe für Geflüchtete)" angegeben. An anderer Stelle wird als weiterer Zweck der Austausch relevanter Informationen über gewalttätige oder gewaltbereite Flüchtlingen genannt, um Gefährdungspotentiale rechtzeitig zu erkennen und geeignete Maßnahmen der Prävention und Intervention zu ergreifen. An wieder anderer Stelle heißt es zur Begründung: „Zudem benötigen wir Informationen über die Gewaltbereitschaft von Bewohnern städtischer Unterkünfte, um bei Verlegungen vor Gericht ausreichende Argumente zu haben." Schließlich wurde noch allgemein der „Schutz der Bevölkerung" als Verarbeitungszweck genannt. Alle diese verschiedenen Zwecke weichen von dem eigentlichen und maßgeblichen Zweck ab,

zu dem die Information der Ausländerbehörde durch die Strafverfolgungsbehörden nach dem Aufenthaltsgesetz erfolgt. Keiner dieser Zwecke ist auf Maßnahmen nach dem Aufenthaltsgesetz gerichtet. Sie sind auch nicht mit diesen Zwecken vereinbar (Artikel 6 Absatz 4 der DS-GVO). Solche Zweckänderungen sind aber nur dann rechtmäßig, wenn es hierfür eine gesetzliche Grundlage gibt. Das war und ist hier nicht der Fall.

Nach § 5 Absatz 1 des Landesdatenschutzgesetzes (LDSG) ist die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, unbeschadet der Bestimmungen der DS-GVO zulässig, wenn eine der in den Nummern 1 bis 4 näher bezeichneten Voraussetzungen erfüllt ist, soweit die Verarbeitung notwendig und verhältnismäßig ist. Allerdings tritt das Landesdatenschutzgesetz zurück, wenn es eine speziellere Rechtsvorschrift gibt, die den gleichen Sachverhalt abschließend anders regelt (§ 2 Absatz 3 Satz 1 LDSG). So ist es hier: § 5 LDSG tritt hier hinter die speziellere Vorschrift des § 19 Absatz 1 Satz 1 des Einführungsgesetzes zum Gerichtsverfassungsgesetz (EGGVG) zurück. Danach dürfen die übermittelten Daten nur zu dem Zweck verarbeitet werden, zu dessen Erfüllung sie übermittelt worden sind. § 19 Absatz 1 Satz 1 EGGVG normiert damit bundesrechtlich eine strenge Zweckbindung, die durch Landesrecht nicht gelockert oder aufgehoben werden kann (Huber AufenthG/Weichert/Stoppa, 2. Aufl. 2016, AufenthG § 87 Rn. 69).

Sie wollen es noch genauer wissen? Kein Problem: § 19 EGGVG ist gemäß § 12 Absatz 1 Satz 1 EGGVG auch für den Fall anwendbar, dass die Datenübermittlung auf der Grundlage des § 87 Absatz 4 Satz 1 AufenthG durch die Polizei übermittelt wurden. Dass § 12 Absatz 1 Satz 1 EGGVG (im hier maßgeblichen Zusammenhang) ausdrücklich nur die Staatsanwaltschaften benennt, steht dem nicht entgegen. Nach dem Wortlaut des § 87 Absatz 4 Satz 1 AufenthG trifft die Informationspflicht gegenüber den Ausländerbehörden die für die Einleitung und Durchführung eines Straf- oder eines Bußgeldverfahrens zuständigen Stellen. Weder die Polizei noch die Staatsanwaltschaft sind hier ausdrücklich benannt. Damit richtet sich die Vorschrift grundsätzlich an die Staatsanwaltschaft. Diese ist „Herrin" des Ermittlungsverfahrens. Der Polizei kommt zunächst nur die Aufgabe des ersten Zugriffs nach der Tat zu. Dass die Polizei in der Praxis in den Fällen der kleineren und oft auch mittleren Kriminalität die Ermittlungen im Regelfall zunächst komplett selbständig führt und erst nach Abschluss der Ermittlungen die dann vollständigen Akten zusammen mit einer Formblattanzeige und ggf. einem zusammenfassenden Ermittlungsbericht der Staatsanwaltschaft vorlegt, ändert an dieser gesetzlichen Zuständigkeitsverteilung nichts. Bezogen auf § 87 Absatz 4 Satz 1 AufenthG wird dies bestätigt durch Nummer 87.4.1.0 der Allgemeinen Verwaltungsvorschrift zum Aufenthaltsgesetz (VwV-AufenthaltsG), wonach die Unterrichtungspflicht (und berechtigung) die Polizei nur insoweit trifft, als sie als Ermittlungspersonen der Staatsanwaltschaft tätig wird (§ 1 II 1 der Verordnung der Landesregierung über die Ermittlungspersonen der Staatsanwaltschaft). Die Ermittlungspersonen sind Organ der Staatsanwaltschaft (Kissel/Mayer/Mayer, 9. Aufl. 2018, GVG § 152 Rn. 7), trotz der organisatorischen Eigenständigkeit sind sie der „verlängerte Arm der Staatsanwaltschaft" (Dölling/Duttge/König/Rössner, Gesamtes Strafrecht, 4. Auflage 2017, GVG § 152 Rn 2). Von daher können ihnen keine weitergehenden als der Staatsanwaltschaft selbst zustehenden Befugnisse eingeräumt werden, sie unterliegen vielmehr denselben Regeln, die für die Staatsanwaltschaft gelten. Deshalb steht auch der Wortlaut des § 12 Absatz 1 Satz 1 EGGVG, soweit dort (nur) die Staatsanwaltschaft genannt ist, der Anwendung der Vorschriften des Zweiten Abschnitts nicht entgegen, wenn die Unterrichtung der Ausländerbehörden gemäß § 87 Absatz 4 Satz 1 AufenthG durch deren Ermittlungspersonen erfolgt. Werden die Ermittlungspersonen der Staatsanwaltschaft als Organ und verlängerter Arm der Staatsanwaltschaft tätig, ist dies so zu behandeln, als würde die Staatsanwaltschaft selbst tätig. Sinn und Zweck der Regelung des § 12 Absatz 1 Satz 1 EGGVG kann es nicht sein, die Datenverarbeitung der Hilfsbeamten weniger strengen Voraussetzungen zu unterwerfen als würde die Staatsanwaltschaft selbst handeln. Andernfalls könnte dies dazu führen, dass sich die Staatsanwaltschaft ihrer datenschutzrechtlichen Pflichten entzieht, indem sie statt selbst zu handeln ihre Hilfsbeamten heranzieht bzw. agieren lässt. Eine solche Umgehung wäre erkennbar unzulässig.

Im Ergebnis greift deshalb die enge Zweckbindung des § 19 Absatz 1 Satz 1 EGGVG auch dann, wenn die Ausländerbehörden gemäß § 87 Absatz 4 Satz 1 AufenthG durch die Ermittlungspersonen der Staatsanwaltschaft unterrichtet werden.

Noch nicht überzeugt? OK: Selbst wenn man dem nicht folgen würde, lägen auch die Voraussetzungen des § 5 Absatz 1 LDSG für eine zulässige Zweckänderung hier nicht vor. Als allein denkbarer Anwendungsfall käme hier die zweite Variante der Nummer 2 in Betracht („zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich"). Hierauf beruft sich die Stadt, indem sie geltend macht, der Schutz der städtischen Mitarbeitende mache die Nutzung der ausländerrechtlichen Informationen generell erforderlich. Dies ist indes unzutreffend.

§ 5 Absatz 1 Nummer 2 2. Alternative LDSG setzt zum einen voraus, dass die Gefahr einer „schwerwiegenden Beeinträchtigung" von Rechten und Freiheiten „einer" anderen Person im Raum steht, die es abzuwehren gilt, und zum anderen, dass die konkrete Verarbeitung unter Erforderlichkeitsgesichtspunkten die ultima ratio darstellt. Hinsichtlich der Gefährdung gilt, dass deren bloße Annahme nicht ausreichend ist, es bedarf vielmehr der hinreichenden Wahrscheinlichkeit des Beeinträchtigungseintritts (Gola/Heckmann/Heckmann/Scheurer, 13. Aufl. 2019, BDSG § 23 Rn. 26, m.w.N.). Es müssen konkrete Tatsachen für eine hinreichend wahrscheinliche Schädigung der in Rede stehenden Rechtsgüter vorliegen (BeckOK DatenschutzR/Albers/Veit BDSG § 23 Rn. 31-32; Sydow, Bundesdatenschutzgesetz, 1. Auflage 2020, § 23 Rn. 25; Taeger/Gabel, DS-GVO BDSG, 3. Auflage 2019, Rn. 24). Nur dann also, wenn in jedem Einzelfall diese engen Voraussetzungen erfüllt sind, kommt eine Zweckentfremdung in Betracht.

Unserer Aufforderung, von dem betroffenen Personenkreis allgemein und von einzelnen Betroffenen im Besonderen ausgehende, auf Behördenmitarbeitende bezogene konkrete Gefährdungssituationen zu belegen, kam die Stadt nicht nach. Wir gehen daher davon aus, dass es solche konkreten Gefährdungen nicht, jedenfalls nicht bezogen auf jeden einzelnen der in der Liste erfassten Personen, gab. Eine Rechtfertigung dafür, pauschal alle Personen, die der Ausländerbehörde nach § 87 Absatz 4 Satz 1 AufenthG zu einem Zeitpunkt gemeldet werden, in dem weder die Staatsanwaltschaft noch ein Gericht den Tatvorwurf abschließend geprüft haben, in diese Liste aufzunehmen, gibt es daher nicht. Allenfalls dann, wenn ein Asylbewerber konkret durch entsprechendes Vorgehen gegen Behördenmitarbeitende aufgefallen wäre, wäre ein anderes Ergebnis denkbar. Ein solches Verhalten aber generell allen Personen zu unterstellen, die bisher bereits auch nur ein einziges Mal in der Öffentlichkeit „auffällig" geworden waren, und sie damit ungerechtfertigt zu stigmatisieren, geht deutlich zu weit und ist ungesetzlich. Dass sich der OB der Stadt Tübingen nun um eine entsprechende gesetzliche Änderung bemüht, ist völlig in Ordnung – und belegt unsere Auffassung, dass die aktuelle Rechtslage die beanstandete Listenführung nicht hergab und nicht hergibt.

Angesichts dieser Rechtslage, die für eine anderweitige Interessenabwägung keinen Raum bot, sahen wir keine andere Möglichkeit, als der Stadt die Fortsetzung ihrer unzulässigen Datenverarbeitung zu untersagen. Gesetz ist Gesetz, auch wenn dessen Folgen nicht auf ungeteilte Zustimmung treffen sollte. Und übrigens: Das Gesetz ist gut, so wie es ist.

Der Gutachterausschuss

Immer wieder erreichen uns Eingaben, in denen sich Bürger_innen sorgen, wenn es etwa darum geht, dass Grundstückskaufverträge einem Gutachterausschuss zur Verfügung gestellt werden. Die Sorge geht dahin, dass die darin enthaltenen – aus Sicht der Betroffenen sensitiven – Daten, insbesondere der Verkaufspreis, in der Gemeinde bekannt werden. Gerade in kleineren Gemeinden wird befürchtet, dass es dadurch zu Gerede komme. Ob diese Sorge generell berechtigt ist, lässt sich für uns schwer verifizieren, da wir noch in keinem Einzelfall entsprechende Erkenntnisse gewinnen konnten. Gleichwohl soll aus Sicht des Datenschutzes auf folgende Rechtslage hingewiesen werden:

Die Bildung von Gutachterausschüssen sowie deren Aufgaben und Befugnisse ist in den §§ 192 bis 199 des Baugesetzbuches (BauGB) geregelt. Ergänzend gilt die landesrechtliche Gutachterausschussverordnung (GuAVO) vom 11. Dezember 1989. Nach § 1 Absatz 1 Satz 1 GuAVO werden Gutachterausschüsse grundsätzlich bei den Gemeinden gebildet. Dabei handelt es sich jedoch nicht um Ausschüsse der Gemeinden als solche. Gemäß § 192 Absatz 1 BauGB sind sie vielmehr selbständige und unabhängige Behörden oder öffentlich-rechtliche Stellen, denen eigene hoheitliche Aufgaben übertragen sind (VG Bayreuth, Urteil vom 20. März 2014 – B 2 K 13.809 –; Sächsisches Oberverwaltungsgericht, Urteil vom 9. Mai 2014 – 1 C 12/12 –; Oberverwaltungsgericht des Landes Sachsen-Anhalt, Beschluss vom 22.Januar 2015 – 4 O 177/14 –).

Als öffentliche Stellen im Sinne des § 2 Absatz 1 Satz 1 des Landesdatenschutzgesetzes (LDSG) sind sie damit datenschutzrechtlich Verantwortliche im Sinne der DS-GVO sowie des Landesdatenschutzgesetzes (§ 2 Absatz 1 Satz 2 LDSG). § 3 Absatz 2 Nummer 1 GuAVO bestätigt dies, wobei allerdings diese Norm offenbar noch nicht (vollständig) an die aktuelle Rechtslage angepasst wurde.

Zunächst stellt das Baugesetzbuch die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten durch Gutachterausschüsse zur Verfügung. Nach § 195 Absatz 1 Satz 1 BauGB ist zur Führung der Kaufpreissammlung jeder Vertrag, durch den sich jemand verpflichtet, Eigentum an einem Grundstück gegen Entgelt, auch im Wege des Tausches, zu übertragen oder ein Erbbaurecht erstmals oder erneut zu bestellen, von der beurkundenden Stelle in Abschrift dem Gutachterausschuss zu übersenden. Nach § 197 Absatz 1 Satz 2 BauGB kann ein Gutachterausschuss verlangen, dass Eigentümer und sonstige Inhaber von Rechten an einem Grundstück die zur Führung der Kaufpreissammlung und zur Begutachtung notwendigen Unterlagen vorlegen.

Geht es dann um das Verhältnis zur Gemeinde, bei der der Gutachterausschuss gebildet ist, ist zu beachten, dass die Gemeinde einerseits und der Gutachterausschuss andererseits jeweils in unterschiedlichen Lagern stehen und deshalb personenbezogene Daten, die sie im eigenen Wirkungskreis verarbeiten, nicht ohne Weiteres miteinander austauschen dürfen. Gemäß dem vom Bundesverfassungsgericht geprägten Bild der Doppeltür (zuletzt: BVerfG, Beschluss vom 27. Mai 2020 – 1 BvR 1873/13 –) vollzieht sich ein Datenaustausch „durch die einander korrespondierenden Eingriffe von Abfrage und Übermittlung, die jeweils einer eigenen Rechtsgrundlage bedürfen. Der Gesetzgeber muss, bildlich gesprochen, nicht nur die Tür zur Übermittlung von Daten öffnen, sondern auch die Tür zu deren Abfrage. Erst beide Rechtsgrundlagen gemeinsam, die wie eine Doppeltür zusammenwirken müssen, berechtigen zu einem Austausch personenbezogener Daten." Das bedeutet, dass die Gemeinde, wenn sie Informationen vom Gutachterausschuss beziehen will, nachweisen muss, dass sie diese Informationen zwingend benötigt, um ihre Aufgaben erledigen zu können. Andererseits muss der Gutachterausschuss prüfen, ob er zur Übermittlung befugt ist. Da das Baugesetzbuch insoweit keine Regelungen enthält, gilt das Landesdatenschutzgesetz. Diese schränkt durch § 6 Absatz 1 Nummer 1 in Verbindung mit § 5 die Möglichkeiten einer Übermittlung zu anderen als den ursprünglichen Erhebungszwecken deutlich ein. Danach dürfte eine Übermittlung regelmäßig ausscheiden. Gutachter tun gut daran, hier Sorgfalt walten zu lassen, denn zu Recht weist § 3 Absatz 2 Nummer 2 GuAVO darauf hin, dass Gutachter einer besonderen Geheimhaltungspflicht unterliegen und sich im Zweifel strafbar machen, wenn sie dagegen verstoßen.

Ja, sind wir denn in China?

Besorgte Bürger wandten sich an uns, weil sie befürchteten hatten, die Einführung von Einlasskontrollen per Gesichtserkennung in das Stadtbüro ihrer Gemeinde würde zu „chinesischen Verhältnissen" führen.

Gesichtserkennung ist aus Sicht des Datenschutzes ein heikles Thema. Bei klassischen Gesichtserkennungssystemen werden biometrische Daten verarbeitet. Diese sind besonders schutzbedürftig, weil sie viel über uns verraten und hoch individuell sind. Es drängen sich die Bilder aus China auf, wo Rotlichtsünder von den Kameras an der Ampel aufgenommen und auf riesige Displays mit Namensnennung projiziert werden – zur Abschreckung und „Erziehung". Dies vor Augen kann man verstehen, dass Bürger_innen besonders sensibel reagieren, wenn der Eindruck entsteht, auch hierzulande hielten solche Methoden Einzug.

Wir haben uns daher von der Gemeinde erklären lassen, was es mit der Gesichtserkennung im Stadtbüro auf sich hat. Sie hat – wie viele andere auch – unter Berufung auf ihr Hausrecht festgelegt, dass in Zeiten der Corona-Pandemie Bürger_innen, die das Stadtbüro betreten wollen, eine Mund-Nase-Bedeckung tragen müssen, ansonsten kann ihnen der Zutritt zum Stadtbüro verwehrt werden.

Um das Hausrecht und die Hygieneregeln in der Pandemiezeit durchzusetzen, wurde die Gemeinde von einer ortsansässigen Firma für Eintrittssysteme unterstützt. Diese installierte ein Zutrittskontrollsystem mit Drehkreuz, Kamera und Monitor. Das System gibt den Weg frei, wenn die Maske richtig sitzt. Dafür sorgt die Kamera mit intelligenter Bildverarbeitung. Sie erkennt, ob ein Gesicht im Mund-Nasen-Bereich bedeckt ist oder nicht. Ist dies der Fall, öffnet sich das Drehkreuz. Erkennt das System den Mund-Nasen-Bereich, weil dieser nicht durch eine Maske verdeckt wird, blockiert das System den Zutritt.

Eine Gesichtserkennung im klassischen Sinne liegt damit nicht vor, da das System die Identifikation von Personen weder bezweckt noch ermöglicht. Insbesondere werden keine Bilder gespeichert.

Auch wenn es sich bei dem Maskenscanner um ein reines Video-Monitoring handelt, werden gleichwohl personenbezogene Daten verarbeitet. Im Landesdatenschutzgesetz ist geregelt, dass die Beobachtung öffentlich zugänglicher Räume mit Hilfe von elektronischer Einrichtungen (Videoüberwachung) sowie die Verarbeitung der dadurch erhobenen personenbezogenen Daten zulässig ist, soweit dies im Rahmen der Erfüllung einer öffentlichen Aufgabe oder in Ausübung des Hausrechts im Einzelfall erforderlich ist, um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich in öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten zu schützen und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen (§ 18 Abs. 1 Nr. 1 LDSG).

Hier handelt die Gemeinde in Ausübung ihres Hausrechts, um Leben und Gesundheit von Personen, die sich in dem Amtsgebäude (Bürgerbüro) aufhalten, zu schützen. Das Eintrittssystem mit automatischer Maskenprüfung ist jedenfalls nicht unverhältnismäßig. Insbesondere weil keine Bilddaten gespeichert werden, sahen wir keine überwiegenden schutzwürdigen Interessen der betroffenen Personen, die gegen den Einsatz des Maskenscanners sprechen würden. Der Maskenscanner wurde daher nicht beanstandet.
Letztlich konnten hier auch die Bedenken, bei baden-württembergischen Kommunen würden „chinesische Verhältnisse“ Einzug halten, ausgeräumt werden.

10.2 Neues aus dem Amt II: Gesundheits-, Sozial- und Bildungswesen

Die Auskunft im Sozialdatenschutz

Die Auskunft ist ein wichtiges und oft in Anspruch genommenes Betroffenenrecht. Dies spiegelte sich auch in der Arbeit unserer Behörde im Berichtszeitraum wieder. Sowohl Verantwortliche als auch betroffene Personen wandten sich vielfach mit Fragen bzw. Beschwerden zu der Thematik an unsere Behörde. Im Folgenden soll auf die Besonderheiten der Auskunft im Bereich des Sozialdatenschutzes eingegangen werden; im Anschluss werden noch „Fälle“ zur Auskunft aus unserer diesjährigen Praxis in diesem Bereich vorgestellt.

© DOC RABE Media – stock.adobe.com

Mit Verweis auf Artikel 15 der DS-GVO kann man zielführend nach seinen verarbeiteten personenbezogene Daten fragen.

Das Auskunftsrecht der betroffenen Person ist in Artikel 15 der DS-GVO geregelt. Danach hat eine Person regelmäßig ein Recht auf Auskunft über sie betreffende personenbezogene Daten, die der Verantwortliche verarbeitet. Außerdem hat sie Anspruch auf weitere Informationen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten (z. B. über die Zwecke der Verarbeitung ihrer personenbezogenen Daten) sowie auf (bei erstmaliger Beantragung kostenlose) Überlassung einer Kopie der gespeicherten Daten.

Im Bereich des Sozialdatenschutzes – Sozialdaten sind die personenbezogenen Daten, die beispielsweise von Jugendämtern, Jobcentern, Wohngeldstellen und Ämtern für Ausbildungsförderung zur Erfüllung ihrer Aufgaben nach dem Sozialgesetzbuch verarbeitet werden (vgl. § 67 Absatz 2 des Zehnten Buchs des Sozialgesetzbuchs, SGB X) – wurde Artikel 15 DS-GVO „modifiziert". Eine solche Abweichung von der Regelung in der Datenschutz-Grundverordnung erlaubt Artikel 23 DS-GVO, wenn bestimmte Voraussetzungen vorliegen und bestimmte Anforderungen eingehalten werden. Geregelt sind die Modifikationen in § 83 SGB X. Da § 83 Absatz 1 SGB X auf § 82a SGB X verweist, ist im Zusammenhang mit der Auskunft auch noch diese Norm von Bedeutung.

Dieses Regelungsgeflecht bedeutet für einen Sozialleistungsträger, der mit einem Auskunftsbegehren zu tun hat, dass er „sein Augenmerk" auf alle drei Normen richten muss. Das Zusammenspiel der Vorschriften soll mit dem folgenden Beispielsfall veranschaulicht werden:

Beim Jugendamt wurde eine Kindeswohlgefährdung angezeigt. Die Eltern des Kinds beantragen beim Jugendamt Auskunft dahingehend, wer der Hinweisgeber war.

Nach Artikel 15 DS-GVO hat die betroffene Person grundsätzlich ein Recht auf Auskunft in Bezug auf über sie verarbeitete personenbezogene Daten. Gemäß Artikel 15 Absatz 1 Buchstabe g DS-GVO gehören hierzu, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten. Hiervon umfasst ist, soweit dem Jugendamt bekannt, grundsätzlich – vorbehaltlich von Artikel 15 Absatz 4 DS-GVO – auch der Name des Hinweisgebers.

Gemäß § 83 Absatz 1 Nr.1 SGB X besteht allerdings das Recht auf Auskunft der betroffenen Person ausnahmsweise dann nicht, soweit die betroffene Person nach § 82a Absatz 1, 4 und 5 nicht zu informieren ist.

Nach § 82a Absatz 1 Nummer 1 Buchstabe a SGB X besteht die Pflicht zur Information u. a. dann nicht, soweit die Erteilung der Information die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

Im Beispielsfall dürfte davon auszugehen sein, dass die Erteilung der Information über den Hinweisgeber die ordnungsgemäße Erfüllung der Aufgaben des Jugendamts gefährden würde und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss. Daher besteht bei einer solchen Konstellation regelmäßig keine Pflicht zur Auskunft. Hintergrund hierfür ist, dass die Gewährung von Diskretion Voraussetzung dafür ist, dass die Jugendämter ihrer Aufgabe, eventuelle familiäre Probleme mit Auswirkung auf das Kindeswohl rechtzeitig zu entdecken und zu lösen, gerecht werden können.

Im Folgenden werden noch drei Aspekte der Auskunft dargestellt, mit denen unsere Behörde im Berichtszeitraum befasst war:

1. Von Seiten der betroffenen Person ist es wichtig, die Auskunft so zu beantragen, dass der Verantwortliche weiß, „was gemeint ist". So wird z. B. hin und wieder die „Herausgabe von Unterlagen zu meiner Person" verlangt. Ein solcher „Herausgabe"-Anspruch besteht im Datenschutzrecht nicht. Daher kann ein entsprechendes Begehr zu Missverständnissen und in der Folge zu (eigentlich unnötigen) Beschwerden bei unserer Behörde führen. Klarer ist es, beispielsweise eine Formulierung wie die folgende zu wählen: „Ich beantrage Auskunft nach Artikel 15 der Datenschutz-Grundverordnung über von mir vom Jugendamt/Jobcenter/Wohngeldstelle/Amt für Ausbildungsförderung verarbeitete personenbezogene Daten."

2. Die Auskunft ist regelmäßig innerhalb eines Monats zu erteilen. Die Frist kann um weitere zwei Monate verlängert werden, wenn dies unter Berücksichtigung der Komplexität und der Anzahl von Anträgen erforderlich ist. In diesem Fall erfolgt nach einem Monat eine Unterrichtung über die Fristverlängerung

zusammen mit den Gründen für die Verzögerung. In einer von unserer Behörde aufgrund einer Beschwerde geprüften Angelegenheit wurden diese Vorgaben, die in Artikel 12 Absatz 3 DS-GVO geregelt sind, nicht eingehalten.

3. In einer weiteren Angelegenheit erteilte ein Jugendamt, weil die betroffene Person mit einer unverschlüsselten E-Mail die Auskunft verlangt hatte, diese Auskunft ebenfalls per unverschlüsselter E-Mail. Das Jugendamt ging anscheinend davon aus, dass Artikel 15 Absatz 3 Satz 3 DS-GVO dies zulässt. Artikel 15 Absatz 3 Satz 3 DS-GVO lautet wie folgt: „Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nicht anderes angibt." Der Umstand, dass die betroffene Person die Auskunft per (unverschlüsselter) E-Mail verlangt hatte, rechtfertigt jedoch nicht, dass auch die Auskunft über die personenbezogenen Daten per unverschlüsselter E-Mail erteilt wird. Es sind angemessene Sicherheitsanforderungen zu erfüllen.

Bei der Bearbeitung eines Auskunftsbegehrs ist Einiges zu beachten. Bei Fragen kann der Datenschutzbeauftragte des Verantwortlichen Hilfestellung geben.

>> Weitere Informationen

Näheres zur Modifizierung der Auskunft im Bereich des Sozialdatenschutzes
https://dip21.bundestag.de/dip21/btd/18/126/1812611.pdf

Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/DSK-Kurzpapier-6-Auskunftsrecht.pdf).

Masernschutzgesetz in Kindertageseinrichtungen und Schulen

Nachdem das Masernschutzgesetz im März 2020 in Kraft trat, erreichten uns viele Anfragen zur Umsetzung der Nachweispflicht in Schulen und Kindertageseinrichtungen. Dabei wurde oft eine überschießende Verarbeitung personenbezogener Daten seitens der Schulen bzw. Kindertageseinrichtungen bemängelt.

Mit dem zum 1. März 2020 in Kraft getretenen Gesetz für den Schutz vor Masern und zur Stärkung der Impfprävention vom 10. Februar 2020 (Masernschutzgesetz, BGBl. I S. 148) wurde insbesondere eine Verpflichtung von Kindertageseinrichtungen und Schulen eingeführt, sich von den die jeweilige Einrichtung besuchenden Kindern und von ihren Beschäftigten – sofern diese nach 1970 geboren sind – Unterlagen über einen bestehenden Impfschutz, eine Immunität gegen Masern oder eine medizinisch begründete Impfunfähigkeit vorlegen zu lassen.

Im Einzelnen müssen die Kinder (bzw. deren Erziehungsberechtigte) und die betroffenen Beschäftigten nach den neu geschaffenen Bestimmungen in § 20 Absatz 9 des Infektionsschutzgesetzes (IfSG)

a) eine Impfdokumentation,
b) ein ärztliches Zeugnis über einen ausreichenden Impfschutz vor Masern,
c) ein ärztliches Zeugnis über Immunität gegen Masern,
d) ein ärztliches Zeugnis darüber, dass sie aufgrund einer medizinischen Kontraindikation nicht gegen Masern geimpft werde können, oder
e) eine Bestätigung einer anderen staatlichen Stelle oder einer anderen (näher bezeichneten) Einrichtung (z. B. einer anderen Kindertagesstätte oder Schule), dass dort ein Nachweis im vorbezeichneten Sinne bereits vorgelegen hat,

der Einrichtung vorlegen.

Die Vorlage muss grundsätzlich vor dem Besuch der Einrichtung erfolgen. Wird ein solcher Nachweis nicht erbracht oder ergibt sich aus dem vorgelegten Nachweis, dass ein ausreichender Impfschutz gegen Masern erst später erzielt werden kann, muss die Einrichtung dies an das zuständige Gesundheitsamt melden. Für Kinder, die bereits bei Inkrafttreten des Masernschutzgesetzes am 1. März 2020 in der Einrichtung waren, hat diese Meldung allerdings erst nach Ablauf

des 31. Juli 2021 zu erfolgen (vgl. § 20 Absatz 10 und 11 IfSG).

Datenschutzrechtlich folgt hieraus, dass die Einrichtung Einblick in die Nachweise nehmen und diese prüfen muss. Eine Ablage dieses Nachweises oder einer Kopie ist jedoch nicht zulässig, d.h. die Einrichtung darf nur vermerken, dass ein Nachweis erfolgt ist bzw. dass ein Impfschutz erst später erreicht werden kann. Nur wenn kein Nachweis erfolgt ist oder ein Impfschutz erst später erzielt werden kann, meldet dies die Einrichtung dem zuständigen Gesundheitsamt.

Allerdings erhielten wir viele Anfragen von Erziehungsberechtigten, welche davon berichteten, dass gleichwohl Kopien von den Nachweisen erstellt und abgelegt wurden. Teilweise wurden diese auch an das Gesundheitsamt weitergeleitet, wobei zuweilen vorgetragen wurde, die Gesundheitsämter hätten dies gegenüber der Schule bzw. der Kindertagesstätte angeordnet, was die Gesundheitsämter indes nicht bestätigten.

Dieses uns vielfach geschilderte Vorgehen von Einrichtungen, standardmäßig Kopien (z.T. auch die Nachweise im Original) abzulegen oder gar an das Gesundheitsamt weiter zu leiten, ist allerdings nach dem Vorgesagten nicht zulässig. Nur in der oben beschriebenen Konstellation (Unterlassen der fristgemäßen Vorlage bzw. Vorlage eines Nachweises, aus dem sich ergibt, dass ein vollständiger Impfschutz erst später erfolgen kann) darf eine Einrichtung dies dem Gesundheitsamt mitteilen; sie ist dann dazu nach § 20 Absatz 9 Satz 4 IfSG verpflichtet. Auch die vielfach geschilderte Praxis mancher Einrichtungen, bei Kindern, die bereits am 1. März 2020 ihre Einrichtungen besuchten, für die Vorlage des Nachweises eine Frist weit vor Ablauf des 31. Juli 2021 zu setzen und anzukündigen, bei Nichteinhaltung dieser von den Einrichtungen selbst gesetzten Frist das Gesundheitsamt hiervon in Kenntnis zu setzen, hat keine gesetzliche Grundlage; eine entsprechende vorzeitige Meldung an das Gesundheitsamt wäre datenschutzrechtlich unzulässig.

Es erreichten uns jedoch auch Eingaben, denen zufolge die Schulen zwar keine Kopien anfertigten, aber die Vorlage der Nachweise innerhalb der Klasse bzw. eines Elternabends erfolgen sollten. Dies ist zwar möglich, muss jedoch so organisiert sein, dass nur die für die Prüfung zuständige Person der Schule und das jeweilige Kind bzw. dessen Erziehungsberechtigte Kenntnis nehmen können. Ein Einsammeln oder ein Vorlegen vor der Klasse bzw. vor den anderen Erziehungsberechtigten beim Elternabend sollte vermieden werden, da hierbei die Gefahr besteht, dass Dritte gesundheitliche Informationen erhalten. Wir empfehlen hier die Vorlage in einem geschützten

© absent84 – stock.adobe.com

Im Zuge des Masernschutzgesetzes vom März 2020 wollten viele Eltern wissen, wie der Impfnachweis des Kindes dokumentiert wird.

Raum – idealerweise im Schulsekretariat, in dem zugleich die Erfassung in den Akten durchgeführt werden kann –, in welchem sich nur der bzw. die Vertreter_in der Schule sowie die nachweispflichtige Person aufhalten.

Das Kultusministerium hat – was grundsätzlich begrüßenswert ist – frühzeitig für die Schulen eine Handreichung und Musteranschreiben sowie weiteres Informationsmaterial herausgegeben. Darin wird insbesondere mit erfreulicher Deutlichkeit betont, dass die Schulen die vorgelegten Nachweise nicht zu archivieren haben und bei Schüler_innen, die bereits am 1. März 2020 in der Schule aufgenommen waren, sowie Personen, die bereits am 1. März 2020 in der Schule tätig waren, eine Meldung an das Gesundheitsamt erst zu erfolgen hat, wenn diese bis zum 31. Juli 2021 den erforderlichen Nachweis nicht vorlegen. Gleichwohl enthält die Handreichung (bzw. deren Anlagen), an deren Erstellung das Kultusministerium uns leider nicht beteiligt hat, auch einige datenschutzrechtlich bedenkliche Ausführungen (wie z. B. die Vorgaben, die Schulen müssten die Art des vorgelegten Nachweises vermerken oder sollten dann eine Kopie des Nachweises anfertigen und dem Gesundheitsamt übermitteln, wenn „der vorgelegte Nachweis nicht interpretiert werden“ könne). Das schon seit einiger Zeit von uns gesuchte Gespräch mit dem Kultusministerium hierüber konnte leider bislang noch nicht geführt werden.

Kurzum: In den Kindertageseinrichtungen und Schulen müssen Nachweise zur Masernschutzimpfung gezeigt werden. Eine Kopie oder Ablage der Originale ist jedoch nicht zulässig. Auch eine Meldung an das Gesundheitsamt darf nur erfolgen, wenn kein Nachweis innerhalb der jeweils anwendbaren gesetzlichen Frist vorgelegt wurde oder die Impfung erst später möglich ist. Die Vorlage in der Kindertageseinrichtung oder Schule muss so erfolgen, dass Dritte keinen Einblick haben und nicht mithören können.

>> Weitere Informationen

Hilfestellung bei der Umsetzung des Masernschutzgesetzes
https://km-bw.de/,Lde/Startseite/Service/Masernschutzgesetz

Bewertungsportale im Internet: Wenn mir deine Bewertung nicht passt, gebe ich deine Identität preis!

Zwischenzeitlich gibt es kaum mehr ein Produkt oder eine Dienstleistung, die nicht im Internet bewertet wird. Vor allem dann, wenn jemand nicht mit der Leistung eines Unternehmers oder Dienstleisters zufrieden ist, scheint das Bedürfnis zu bestehen, dies – oft auch unter einem Pseudonym - in öffentlichen Foren publik zu machen. Unternehmer oder Dienstleister, die sich hierdurch ungerecht behandelt fühlen, möchten dies wiederum richtigstellen, was absolut nachvollziehbar ist. Hierbei besteht allerdings die Gefahr, dass personenbezogene Daten des Bewertenden, wie etwa der Klarname einer unter einem Pseudonym agierenden Person, unzulässiger Weise öffentlich gemacht werden.

Für derartige Veröffentlichungen liegt regelmäßig keine Rechtsgrundlage vor, da die Abgabe einer Bewertung nicht als Einwilligung in die Offenlegung personenbezogener Daten in einer eventuellen Antwort gewertet werden kann. Besonders brisant wird es, wenn es sich bei der bewerteten Person um einen Berufsgeheimnisträger, wie etwa einen Rechtsanwalt oder Arzt handelt. In diesen Fällen kann die Veröffentlichung personenbezogener Daten des (unzufriedenen) Mandanten/Patienten eine Schweigepflichtverletzung und damit eine Straftat darstellen.

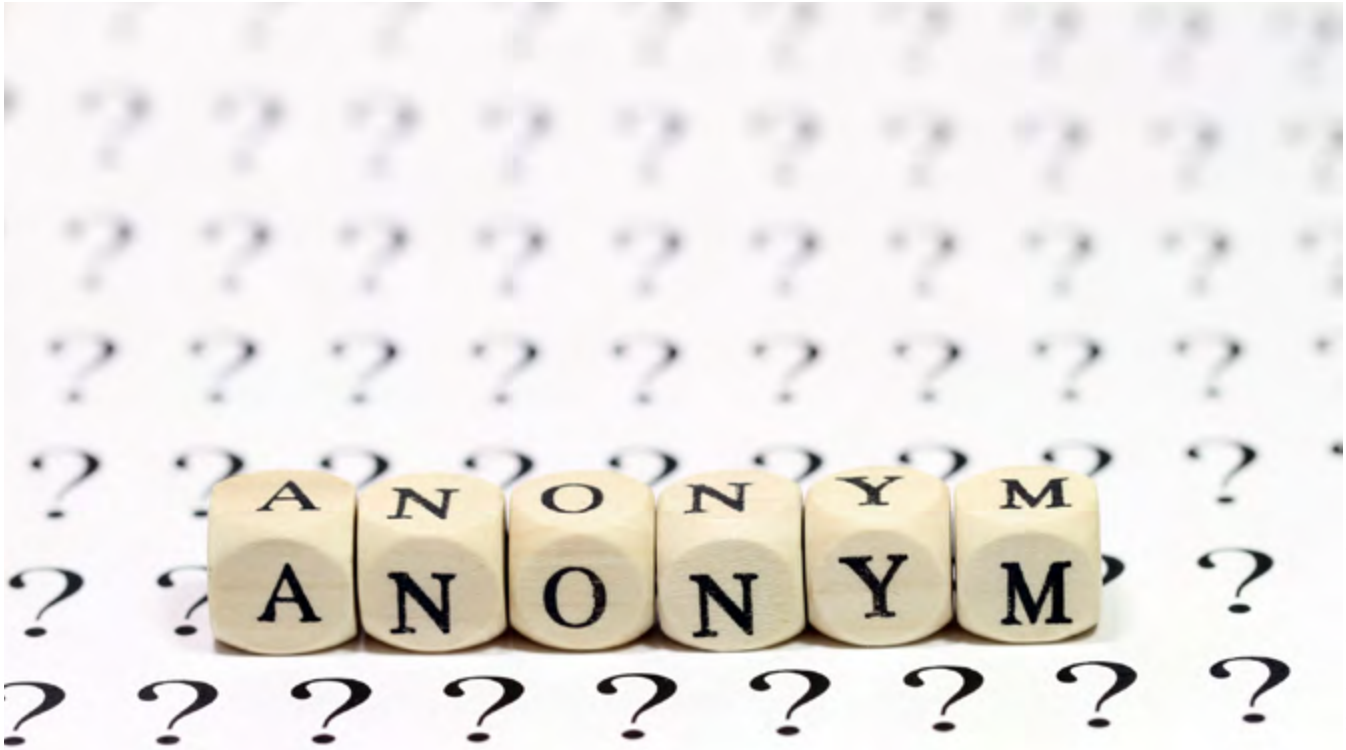
Rechtsanwälte: Namensnennung auf Biegen und Brechen

In einem der Fälle gab ein ehemaliger Mandant unter Pseudonym an, dass er den Rechtsanwalt nicht empfehle. Er habe die Rechnung seines Rechtsanwalts nicht bezahlt, woraufhin der Rechtsanwalt ihn verklagt habe. Das Gericht habe dem Rechtsanwalt aber nur einen Teilbetrag zugesprochen. Tatsächlich war der Teilbetrag jedoch Gegenstand eines gerichtlichen Vergleichs. Der Rechtsanwalt wehrte sich mit einer einstweiligen Verfügung beim Landgericht. Daraufhin änderte der ehemalige Mandant seine Bewertung ab und formulierte neutral, was das Ergebnis des gerichtlichen Verfahrens war. Die Formulierung lässt offen, ob das Gericht durch einen Vergleich oder durch ein Urteil beendet wurde. Der Rechtsanwalt konterte in verschiedenen Reaktionen unter Nennung des vollständigen Namens des Mandanten. Dabei stellte er insbesondere klar, dass es sich bei dem Teilbetrag um einen Vergleichsbetrag handelte. Im Hinblick auf die geänderte Bewertung

hat der Rechtsanwalt keine zivilrechtlichen Unterlassungs- oder Löschungsansprüche nach dem Bürgerlichen Gesetzbuch, da es sich um eine zulässige Meinungsäußerung sowie die Angabe einer wahren Tatsache handelt.

Im Sinne von Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO wird jedoch ein berechtigtes Interesse des Rechtsanwalts anerkannt, Tatsachen anzugeben, die für potentielle Kunden von Bedeutung sind, um sich ein Bild von seiner Person und seiner Arbeit zu machen. Das berechtigte Interesse gründet darauf, dass aufgrund der großen Reichweite des Bewertungsportals eine breite Öffentlichkeit auf die Bewertung zugreifen kann. Die Bewertungen können ausschlaggebend dafür sein, ob sich potentielle Kunden an den Rechtsanwalt wenden oder nicht. Die Möglichkeit der Darstellung der eigenen Sicht auf die Bewertung kann daher von nicht unerheblicher Bedeutung für den künftigen beruflichen Erfolg sein. Um gegenüber der Öffentlichkeit klarzustellen, dass er die Sichtweise des ehemaligen Mandanten nicht teilt, war es jedoch keineswegs erforderlich, diesen mit dem vollständigen Namen anzusprechen. Stattdessen hätte beispielsweise das Pseudonym verwendet werden können. Für die Öffentlichkeit dürfte es kaum von Interesse sein zu erfahren, wer sich hinter dem Pseudonym verbirgt. Jedenfalls überwiegt vorliegend das Interesse des Mandanten an der Geheimhaltung seiner Identität.
Gemäß § 43a Absatz 2 der Bundesrechtsanwaltsordnung (BRAO) ist der Rechtsanwalt zur Verschwiegenheit verpflichtet, wobei sich diese Pflicht auf alles bezieht, was ihm in Ausübung seines Berufes bekanntgeworden ist, unter Ausnahme von Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Dies gilt gemäß § 59b Absatz 2 Nummer 1 Buchstabe c BRAO i. V. m. § 2 Absatz 1 Satz 2 der Berufsordnung der Rechtsanwälte auch nach Beendigung des Mandats. Von der Verschwiegenheitspflicht umfasst ist daher bereits das personenbezogene Datum, dass der Mandant den Rechtsanwalt beauftragt hatte. Mandanten dürfen daher, nicht zuletzt aufgrund der hohen berufsrechtlichen Anforderungen an die Verschwiegenheit von Rechtsanwälten, grundsätzlich darauf vertrauen, dass ihre personenbezogenen Daten nicht an unberechtigte Dritte und erst recht nicht an die Öffentlichkeit via Internet gelangen.

Anders sieht das in diesem Fall die Rechtsanwaltskammer Stuttgart, die sich ebenfalls mit einer Beschwerde des Mandanten befasste und diese zurückwies. Obwohl wir sowohl im Rahmen der Anhörung als auch in der Begründung unserer Anordnung ausführlich darlegten, weshalb die Einschätzung der



© blende11.photo – stock.adobe.com

Negative Bewertung im Internet? Bitte nicht die Identität der Urheber offenlegen!

Rechtsanwaltskammer für die datenschutzrechtliche Bewertung nicht maßgeblich sein kann, hält der Rechtsanwalt an seiner Auffassung fest und hat die unsere Anordnung gerichtlich angegriffen. Der Antrag auf vorläufigen Rechtsschutz wurde vom Verwaltungsgericht abgelehnt. Die Entscheidung in der Hauptsache steht noch aus.

Notare: Überschießende Reaktion einer Notarkanzlei

Anders als Rechtsanwälte sind Notar_innen Träger eines öffentlichen Amtes und damit öffentliche Stellen. Aber genau wie Rechtsanwälte sind auch sie bezüglich allem, was ihnen bei Ausübung ihres Amtes bekannt geworden ist, zur Verschwiegenheit verpflichtet. Dies gilt auch für ihre Mitarbeitenden.

Unter Hinweis auf diese Verschwiegenheitspflicht wurde unsere Behörde anonym auf Äußerungen einer Notarkanzlei zu Bewertungen von Mandanten der Kanzlei auf dem Portal „Google Bewertungen" hingewiesen. Dem Schreiben waren zwei Seiten mit Bewertungen und Antworten beigefügt. Unsere Überprüfung hat ergeben, dass die vorgelegten Bewertungen und die Antworten zu diesen tatsächlich auf „Google-Bewertungen" eingestellt waren, sich die Bewertungen auf die von dem anonymen Schreiber genannte Notarkanzlei bezogen und die Antworten auch tatsächlich von dieser Notarkanzlei stammten.

In einer dieser Antworten wurde z. B. der vollständige Name samt Geburtsname und Wohnort einer Mandantin genannt, die in ihrer Bewertung lediglich ihren Vornamen und den ersten Buchstaben ihres Nachnamens genannt hatte. Weiteren Antworten war z. B. zu entnehmen, aus welchen Gründen Mandanten, die in einer Bewertung ihren Klarnamen angegeben hatten, die Notarkanzlei aufgesucht hatten.

Unsere Prüfung hat ergeben, dass diese datenschutzwidrigen Antworten ohne Wissen der Notarin von Mitarbeitern veröffentlicht wurden. Dies ändert jedoch nichts daran, dass die rechtswidrigen Veröffentlichungen aus datenschutzrechtlicher Sicht der Notarin zuzurechnen sind. Denn diese ist für die von ihren Mitarbeitenden in ihrer Notarkanzlei vorgenommenen Datenverarbeitungen und damit auch für die im Portal Google-Bewertungen offengelegten personenbezogenen Daten „Verantwortliche" im Sinne der DS-GVO. Da besteht offenbar Schulungsbedarf.

Die Problematik, dass auf unter Pseudonym abgegebene Bewertungen in unzulässiger Weise unter Nennung des Klarnamens reagiert wird, stellt sich auch bei anderen Berufsgeheimnisträgern, aber auch bei sonstigen Unternehmen und Organisationen. Uns erreichten diesbezüglich zahlreiche Beschwerden. Daher sahen wir uns veranlasst, in einer Pressemitteilung darauf aufmerksam zu machen: „Negative Bewertung im Internet? Bitte nicht die Identität der Urheber offenlegen!".

>> Weitere Informationen

https://www.baden-wuerttemberg.datenschutz.de/negative-bewertung-im-internet/

10.3 Neues aus dem Amt III: Datenschutz in der Privatwirtschaft

Auskunft heißt Auskunft – so konkret wie möglich

Das Auskunftsrecht nach Art. 15 DS-GVO ist eines der wesentlichen Rechte für die Betroffenen. Nicht ohne Grund erhalten wir daher auch viele Beschwerden, in denen dargelegt wird, dass eine begehrte Auskunft gar nicht oder aber nicht vollständig erteilt worden ist. Dies betrifft vor allem auch die Frage, an wen die Daten der Betroffenen weiterübermittelt worden sind.

In den Standardtexten ihrer Auskunftsschreiben an Betroffene nach Art. 15 DS-GVO behaupten nicht wenige Unternehmen, darunter auch ein Adresshändler, dass ihnen ein Wahlrecht im Hinblick auf Art. 15 Abs. 1 Buchst. c DS-GVO zustünde, sie also zwischen der Nennung des konkreten Empfängers (z.B. Fa. XY) oder einer Empfängerkategorie (z.B. Verlage) auswählen könnten.

Dies ist aber datenschutzrechtlich unzutreffend. Die genannte Regelung ist vielmehr so zu verstehen, dass bei erfolgten Übermittlungen über den konkreten Empfänger Auskunft zu erteilen ist, bei künftigen und geplanten Übermittlungen über die entsprechende Kategorie(en). Es ist also dem Antragsteller immer das an Informationen zu nennen, was auch an Wissen bei der verantwortlichen Stelle vorhanden ist.

Auch aus den Regelungen der Art. 5 und Art. 12 DS-GVO ergibt sich die Pflicht des Verantwortlichen, ein Höchstmaß an Transparenz zugunsten der Betroffe-

nen zu leisten. Lediglich die Nennung einer Kategorie von Empfängern reicht da nicht aus und hilft übrigens auch dem Betroffenen nicht weiter, der so konkrete Angaben wie möglich erwartet. Denn er kann (und will auch häufig) bei den genannten Empfängern sein Auskunftsrecht nach Art. 15 DS-GVO geltend machen und so weiterverfolgen, wer alles seine persönlichen Daten bekommen hat.

Dies ist auch – wörtlich – Erwägungsgrund 63 der DS-GVO („ … wer die Empfänger der personenbezogenen Daten sind …“) zu entnehmen. Wenn man überhaupt ein Wahlrecht annehmen würde, so stünde dieses allein dem Betroffenen zu, da Art. 15 DS-GVO ein Betroffenenrecht regelt.

Wir haben daher die betroffenen Unternehmen aufgefordert, ihre bisherige Praxis bei der Beauskunftung nach Art. 15 DS-GVO umgehend an die dargelegte Rechtsauffassung anzupassen. In diesem Punkt sind wir streng, auch sehen wir keinen Anlass für etwaige andere „Auslegungen“ – denn die Rechte der Betroffenen sind zu wahren!

Anforderungen an die Benachrichtigung der Betroffenen bei einer Datenpanne

Die DS-GVO sieht vor, dass der Verantwortliche die betroffene Person von einer sog. Datenpanne zu benachrichtigen hat, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für seine persönlichen Rechte zur Folge hat. Welchen Inhalt muss eine solche Benachrichtigung haben?

Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche (unverzüglich und möglichst binnen von 72 Stunden, nachdem ihm die Verletzung bekannt wurde) diese der 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). Eine solche Verletzung – auch Datenpanne genannt – kann z. B. eine an einen falschen Adressaten versandte E-Mail mit personenbezogenen Daten sein.

Hat die Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, sieht die DS-GVO zusätzlich (zur Meldung an die Aufsichtsbehörde) vor, dass der Verantwortliche unverzüglich die von der Datenpanne betroffene Person benachrichtigt. Die Benachrichtigungspflicht hat drei Ziele: Sie soll Transparenz im Hinblick auf Datenschutzverletzungen schaffen, die betroffenen Personen dabei unterstützen, Folgeschäden aufgrund der Datenschutzverletzung zu vermeiden bzw. zu minimieren, und (beim Verantwortlichen) einen Anreiz schaffen, verstärkte Anstrengungen zur Datensicherheit zu unternehmen, so dass der Norm auch präventive Funktion zukommt (vgl. Reif in Gola, Kommentar zur Datenschutz-Grundverordnung, 2. Auflage, Artikel 34 Rn. 1).

Welche Informationen muss nun eine solche Betroffenenbenachrichtigung enthalten? Zu dieser Frage haben wir im Berichtszeitraum u. a. eine Einrichtung für Kinder und Jugendliche, welche Opfer eines Hackerangriffs geworden war, beraten.

Die Antwort ergibt sich weitgehend aus der Datenschutz-Grundverordnung selbst. Nach Artikel 34 der DS-GVO in Verbindung mit Artikel 33 DS-GVO enthält die Benachrichtigung zumindest die folgenden Informationen und Maßnahmen:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten in klarer und einfacher Sprache,

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,

- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und

- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Im konkreten Fall hat die Einrichtung – in Abstimmung mit unserer Behörde – zu den einzelnen Punkten im Wesentlichen Folgendes ausgeführt:

- Die Einrichtung sei Opfer eines Hackerangriffs geworden. Ein Unbekannter habe durch den Hackerangriff Zugriff auf von der Einrichtung verarbeitete personenbezogene Daten erhalten. Im Folgenden wurde benannt, welche Arten von personenbezogenen Daten

betroffen sind (z. B. Adress- und Kommunikationsdaten, Gesundheitsdaten). Auch wurde darüber informiert, dass die Einrichtung den Zugriff auf die Daten zeitweise verloren hatte, die Daten aber wiederhergestellt werden konnten.

Allgemein ist an dieser Stelle noch zu erwähnen, dass das Gebot der „klaren Sprache" es ausschließen dürfte, die Information über die Verletzung unter einer Vielzahl anderer Informationen zu verstecken oder die Information mit Werbe- oder Verkaufsangeboten zu verknüpfen, die nicht klar von der Verletzungsinformation getrennt sind (vgl. Martini in Paal/Pauly, Kommentar zur DS-GVO, 2. Auflage, Artikel 34 Rn. 53).

Bei diesem Punkt stand die Rechtsfrage im Raum, ob – da eine Veröffentlichung der Informationen in der Tagespresse erfolgen sollte, weil individuelle Benachrichtigungen aller betroffenen Personen mit unverhältnismäßigem Aufwand verbunden waren – statt der Angabe des Namens und der Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen ein Verweis auf die Internetseite der Einrichtung und die im Impressum hinterlegten Kontaktdaten ausreichend ist. Hintergrund für diese Frage war die Sorge der Einrichtung, dass auch eine veröffentlichte Telefonnummer missbraucht werden könnte. Diesen sog. „Medienbruch" hielten wir aufgrund des doch recht eindeutigen Wortlauts der Vorschrift nicht für zulässig.

Bei der Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten hat die Einrichtung darauf hingewiesen, dass damit gerechnet werden müsse, dass die Hacker oder Dritte die Kenntnis der Daten für Straftaten (z. B. Betrug oder Erpressung) zum Nachteil der betroffenen Personen ausnutzen und insbesondere die E-Mail-Anschriften zur weiteren Verbreitung von Malware verwenden. Es wurde erläutert, dass insbesondere Personen betroffen sein könnten, die geschäftlich oder persönlich mit der Einrichtung in Kontakt stehen oder standen.

Hier riet die Einrichtung zur Vorsicht bei E-Mails mit Anhängen und bei Telefonanrufen, die Forderungen enthalten; diese E-Mails könnten auch einen nicht direkt offensichtlichen Bezug zu der Einrichtung aufweisen. Weiter wurde darüber informiert, dass der Verantwortliche nach Bekanntwerden des Hackerangriffs Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener ergriffen habe und das gesamte System aus Sicherheitsgründen heruntergefahren habe, um es neu aufzusetzen. Auch wurde mitgeteilt, dass die Einrichtung unsere Behörde unterrichtet und eine Anzeige bei der Polizei aufgegeben habe.

Die Benachrichtigung im Falle einer Datenpanne hat also gewissen Anforderungen zu genügen. Die Einhaltung dieser Anforderungen ist allerdings kein Selbstzweck, sondern hilft der betroffenen Person, das Risiko der Verletzung ihrer personenbezogenen Daten einschätzen zu können und Folgeschäden aufgrund der Datenschutzverletzung zu vermeiden bzw. zu minimieren.

Datenschutz in der Kreditwirtschaft: Fehlüberweisung mit Folgefehler

Mancher Bankkunde muss mit Verdruss zur Kenntnis nehmen, dass die Bank seine personenbezogenen Daten direkt an einen Dritten weitergibt, weil dieser ihm versehentlich Geld überwiesen hat, das er nun zurückfordert. Die Banken haben von einer solchen Weitergabe abzusehen.

Bisweilen sehen sich Kontoinhaber damit konfrontiert, dass eine bis dahin unbekannte Person (oder ein ebensolches Unternehmen) brieflich Geld von ihnen fordert, dass sie zuvor angeblich irrtümlich auf sein Konto überwiesen haben. Auf Nachfrage stellt sich sodann heraus, dass der Zahlende den Namen und die Anschrift des Bankkunden direkt von der kontoführenden Bank erhalten hat. Der hieraus erwachsende Unmut des Bankkunden ist verständlich und begründet.
Für die Weitergabe des Namens und der Anschrift des Kontoinhabers an den nur scheinbar spendablen Zahler bedarf es einer Rechtsgrundlage gemäß Artikel 6 Absatz 1 DS-GVO, an der es jedoch regelmäßig fehlt. Manche Banken berufen sich auf das Abkommen über die SEPA-Inlandsüberweisung. Nach dessen Nummer II.7 hat der Zahlungsdienstleister des Zahlungsempfängers im Fall einer Fehlüberweisung den Namen und die Anschrift der Person mitzuteilen, auf deren Konto der Überweisungsbetrag gutgeschrieben wurde, damit der Zahler oder der Zahlungsdienstleister des Zahlers seine Ansprüche gegen diese Person durchsetzen kann. Voraussetzung ist zudem, dass eine Rücküberweisung mangels Zustimmung des Zahlungsempfängers nicht möglich ist. Aus dem Abkommen ergibt sich aber allenfalls eine zivilrechtliche Pflicht, die Daten des irrtümlichen Zahlungsempfängers an die Bank des Überweisenden, nicht jedoch an diesen selbst herauszugeben.

Hierfür spricht insbesondere auch, dass die Übermittlung gemäß Nummer II.7 des Abkommens dem Zahler ermöglichen soll, seine Ansprüche gegen den falschen Zahlungsempfänger durchsetzen zu können. Solche Ansprüche sind aber nicht in jedem Fall gegeben. Wenn der Zahler den Zahlungsvorgang nicht autorisiert hat, ist sein Zahlungsdienstleister verpflichtet (nach § 675u Satz 2 des Bürgerlichen Gesetzbuchs, BGB), dem Zahler den überwiesenen Betrag zu erstatten. Sofern der Betrag einem Zahlungskonto des Zahlers belastet worden ist, hat der Zahlungsdienstleister dieses wieder auf den Stand zu bringen, auf dem es sich ohne die Belastung durch den nicht autorisierten Zahlungsvorgang befunden hätte. In einem solchen Fall hat die Bank des Zahlers einen Bereicherungsanspruch gegen den Zahlungsempfänger (Zetzsche, in: Münchener Kommentar zum BGB, 8. Auflage 2020, § 675u Rn. 36). Eine Übermittlung von Daten des Zahlungsempfängers an den Zahler ist in solchen Fällen nicht zu dessen Befriedigung erforderlich.

Eine rechtliche Verpflichtung zur Übermittlung personenbezogener Daten an den Überweisenden ergibt sich auch nicht aus § 675y Absatz 5 Satz 4 BGB. Nach dessen Wortlaut ist allein der Zahlungsdienstleister des Überweisenden verpflichtet, diesem auf schriftlichen Antrag alle verfügbaren Informationen mitzuteilen, damit der Überweisende einen Anspruch auf Erstattung des Zahlungsbetrags geltend machen kann. Diese Verpflichtung trifft hingegen nicht die Bank des irrtümlichen Zahlungsempfängers.

Banken sollten daher davon absehen, den Namen und die Anschrift oder Kontaktdaten eines Kunden, dem irrtümlich Geld überwiesen worden ist, an den Überweisenden zu übermitteln.

Ausführung von Überweisungsaufträgen ohne Kontonummer

Moderne datenschutzsensible Bankkunden überlegen sich gut, wem gegenüber sie ihre Bankverbindung offenlegen. Banken sollten daher bei der Mitteilung solcher Daten zurückhaltend sein, auch wenn diese der Ausführung eines Überweisungsauftrags dienen soll. Der Kunde einer an seinem Wohnort ansässigen Bank begab sich zwecks Veranlassung mehrerer Überweisungen in die nächstgelegene Filiale. Dort übergab er dem zuständigen Mitarbeitenden eine Liste mit den Namen verschiedener Zahlungsempfänger mit den jeweils zu überweisenden Beträgen. Den meisten dieser Zahlungsempfänger war die IBAN ihres Zahlungskontos hinzugefügt, auf dem das Geld eingehen sollte. Bei einem Namen fehlte diese Angabe jedoch. Der Überweisende wies lediglich darauf hin, dass diese Person ebenfalls Kunde der örtlichen Bank sei. Ungeachtet

© Nattakorn – stock.adobe.com

Banken sollten keine persönlichen Daten eines Kunden, dem irrtümlich Geld überwiesen wurde, an den Überweisenden übermitteln.

seiner Unvollständigkeit führte die Bank auch diesen Überweisungsauftrag aus. Dies wurde dem Überweisenden in seinem nächsten Kontoauszug bestätigt. Die Zahlungsempfängerin reagierte hierauf empört, zumal sie sich keiner Geschäftsbeziehung mit dem Überweisenden bewusst und keiner Zahlung gewärtig gewesen war.

Das Missbehagen der Zahlungsempfängerin ist aus datenschutzrechtlicher Sicht durchaus berechtigt. Mit der Ausführung des unvollständigen Überweisungsauftrags hat die Bank dem Überweisenden bestätigt, dass die Zahlungsempfängerin Inhaberin eines bei der Bank geführten Kontos war. Bereits bei dieser Angabe handelt es sich um ein personenbezogenes Datum im Sinne der DS-GVO. Dieses Datum ist dem Überweisenden spätestens durch die Mitteilung der Belastung seines Kontos zur Kenntnis gegeben worden. Darin liegt eine Verarbeitung des vorgenannten personenbezogenen Datums gemäß Artikel 4 Nr. 2 DS-GVO.

Die Bestätigung gegenüber dem Überweisenden, dass die Zahlungsempfängerin Inhaberin eines bei der Beschwerdegegnerin geführten Kontos war, ist nach Artikel 6 Absatz 1 DS-GVO unzulässig. Insbesondere kann die Übermittlung dieser Angabe nicht auf eine Interessenabwägung gemäß Artikel 6 Absatz 1 Unterabsatz 1 Buchstabe f DS-GVO gestützt werden. Ein berechtigtes Interesse der Bank an der Offenbarung des mit der Zahlungsempfängerin geschlossenen Bankvertrags ist nicht erkennbar. Ebenso wenig kommt ein berechtigtes Interesse des Überweisenden in Betracht, zumal dieser im Fall seiner von ihm behaupteten Geschäftsbeziehung mit der Zahlungsempfängerin die Möglichkeit gehabt hätte, sich bei ihr selbst nach deren Kontoverbindung zu erkundigen. Hingegen hat die Zahlungsempfängerin grundsätzlich ein schutzwürdiges Interesse daran, selbst zu entscheiden, wer von der Existenz ihres Kontos Kenntnis erhält. Dabei ist nicht zuletzt denkbar, dass sie Zahlungen bestimmter Personen generell ablehnt oder die Zahlung auf ein anderes Konto wünscht.

Banken sollten grundsätzlich die Ausführung von Überweisungen auf Konten ihrer Kunden ablehnen, wenn der Überweisungsauftrag keine IBAN enthält und sie nicht mit Sicherheit überprüfen können, ob der Überweisende tatsächlich Kenntnis von der Existenz des Empfängerkontos hat.

Nicht ohne den Veranlasser: Werbender und Adresshändler sind regelmäßig gemeinsam Verantwortliche

Auf Werbebriefen ist oft, äußerst kleingedruckt, zu lesen: Verantwortlich im Sinne der DS-GVO: Adresshändler XY, gerne mit Sitz in der Schweiz (weil dort die DS-GVO nicht gilt). Somit muss sich der/die Empfänger_in der Werbung im Hinblick auf die eigenen Betroffenenrechte mit dem Adresshändler im Ausland herumärgern, während sich der/die eigentliche Veranlasser_in bzw. Auftraggeber_in der Werbung bequem zurücklegen kann.

Mit dem Wirksamwerden der DS-GVO konnte dieser unbefriedigende Zustand beendet werden: Nach Art. 4 Nr. 7 DS-GVO ist für eine konkrete Datenverarbeitung verantwortlich, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Datenverarbeitung entscheidet. Über die Zwecke und Mittel kann nämlich nach der Rechtsprechung des EuGH auch derjenige (mit)entscheiden, der die Daten nicht selbst verarbeitet, also selbst gar keinen Zugriff auf die Daten hat (wie es im Hinblick auf das werbende Unternehmen bei der Verarbeitung der Adressdaten z.B. durch einen Lettershop, der die Daten durch den Adresshändler übermittelt bekommt, oft der Fall ist).

Im Falle der Adressvermietung war somit im Lichte der Rechtsprechung des EuGH zu Art. 26 DS-GVO (EuGH, Urteil vom 5. Juni 2018 – EU-C-210/16, Facebook Fanpages sowie EuGH, Urteil vom 10. Juli 2018 – C-25/17, Zeugen Jehovas) die Frage zu beantworten, ob das werbende Unternehmen – auch wenn es keinen Zugriff auf die zu Werbezwecken verarbeiteten Daten hat – gemeinsam mit dem Adresshändler (bzw. Adresseigner) verantwortlich ist.

Auch hier gilt natürlich zunächst der Grundsatz der Prüfung und rechtlichen Bewertung der jeweiligen Umstände des Einzelfalls. In der Regel ist aber davon auszugehen, dass eine gemeinsame Verantwortlichkeit jedenfalls immer dann vorliegt, wenn das werbende Unternehmen selbst Kriterien für die Adressauswahl festgelegt hat (z.B. Frauen ab 40 Jahren mit Hochschulausbildung; Selbständige bis 45 Jahre mit Hobbies im Sportbereich; Familien im eigenen Einfamilienhaus mit Einkommen über 3.000 Euro im Monat).
Auch die Auswahl bestimmter, vom Adresshändler (bzw. Adresseigner) vorgeschlagenen Selektionskriterien kann ausreichen, eine Verantwortlichkeit auch des Werbenden und somit eine gemeinsame Verant-

wortlichkeit von Werbendem und Adresshändler im Sinne des Art. 26 DS-GVO anzunehmen. Denn wie der Europäische Gerichtshof mehrfach entschieden hat, besteht das Ziel dieser Bestimmung darin, durch eine weite Definition des Begriffs des „Verantwortlichen" einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten (Urteil vom 13. Mai 2014, Google Spain und Google, C-131/12, EU-C-2014-317, Rn. 34).

Durch die gemeinsame Verantwortlichkeit kann nun der Betroffene seine Rechte auch gegenüber dem werbetreibenden Unternehmen geltend machen. Und auch die Datenschutzaufsichtsbehörde kann im Rahmen ihrer örtlichen Zuständigkeit das werbende Unternehmen kontrollieren. Ein verbraucherfreundlicher Fortschritt der DS-GVO.

Weitergabe von Schuldnerdaten an Auskunfteien

Immer wieder erreichen uns Beschwerden von Bürger_innen über Inkassounternehmen, die mit einer Meldung bei einer Auskunftei drohen, falls eine angebliche Forderung nicht bezahlt werde, oder welche die Daten der betroffenen Personen bereits zu Unrecht an eine Auskunftei weitergegeben haben.

Bei der Tätigkeit von Wirtschaftsauskunfteien, zum Zwecke des Schutzes von Verbraucher_innen vor Überschuldung und um die Wirtschaft vor Betrügereien zu schützen geschäftsmäßig bonitätsrelevante Daten über Unternehmen und Privatpersonen zu sammeln und zu verarbeiten, handelt es sich um einen legitimen Verarbeitungszweck (Art. 5 Abs. 1 Buchstabe b der DS GVO). Deswegen dürfen die Inkassounternehmen Angaben zu einer Person, die sich in einem Inkassoverfahren als „unzuverlässig" erwiesen hat, an Wirtschaftsauskunfteien übermitteln, vorausgesetzt, diese_r angebliche Schuldner_in ist auch tatsächlich „unzuverlässig".

Für ein berechtigtes Interesse an der Datenübermittlung spricht, wenn

- eine begründete Forderung nicht, nicht rechtzeitig oder nur unvollständig erfüllt wird, insbesondere wenn diese durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist. Bei gerichtlichen Entscheidungen kann sich die betroffene Person grundsätzlich nicht darauf berufen, der Titel sei zu Unrecht ergangen, wenn dieser ordnungsgemäß zugestellt bzw. solange er nicht wieder aufgehoben worden ist,

- dem Schuldner die Forderung und deren Fälligkeit bekannt ist, und

- keine erheblichen Einwendungen gegen die Forderung - ggf. noch im Prozess – erhoben wurden. Solche verhindern eine Einmeldung auch dann, wenn die betroffene Person bei Gericht unterlegen ist, dieses aber nicht festgestellt hat, dass die Rechnung böswillig, aus Nachlässigkeit oder wegen Mittellosigkeit nicht beglichen worden ist, bzw. diese nach der Rechtskraft des Urteils alsbald bezahlt wurde. Einwendungen sind erheblich, wenn die maßgeblichen Tatsachen substantiiert bestritten bzw. wenn gegen die Forderung vertretbare, angesichts der Rechtsordnung akzeptable Argumente vorgebracht werden.

Das Nichtbegleichen bzw. nicht rechtzeitige oder unvollständige Begleichen einer Forderung stellt aber nur ein Indiz für die Unzuverlässigkeit der betroffenen Person dar. Für die Zulässigkeit der Einmeldung bei einer Warndatei müssen noch belastbare Umstände hinzukommen, welche die Annahme begründen, dass die betroffene Person auch künftig zahlungsunwillig bzw. zahlungsunfähig sein wird und deswegen Dritte vor Geschäften mit dieser gewarnt werden sollten.

Bei der dabei anzustellenden Prognose zum zukünftigen Zahlungsverhalten der betroffenen Person spricht u.a. für deren Zahlungsunwilligkeit bzw. Zahlungsunfähigkeit, wenn bei Auskunfteien bereits Negativmerkmale gespeichert sind. Ebenfalls zu Lasten des Schuldners bzw. der Schuldnerin geht, wenn die einzumeldende Forderung grundlos zum maßgeblichen Zeitpunkt nicht oder nur teilweise erfüllt wurde, wenn die Bezahlung schleppend erfolgt ist, auch wenn die Forderung inzwischen vollständig nebst Mahnkosten und dergleichen beglichen worden ist, oder wenn die betroffene Person mangels ausreichender finanzieller Mittel nicht in der Lage war, den Zahlungsanspruch zum Fälligkeitszeitpunkt vollständig zu erfüllen. Ein weiterer Einmeldegrund kann sein, dass mit der betroffenen Person zur Begleichung ihrer Zahlungsrückstände ein Ratenzahlungsvergleich geschlossen wurde. Selbst verjährte Forderungen können den Schluss zulassen, dass die betroffene Person nicht gewillt ist, ihre Zahlungsverpflichtungen künftig rechtzeitig zu erfüllen. Auch der sorglose Umgang mit Zahlungsverpflichtungen, etwa wenn die Forderung

aus Nachlässigkeit trotz Mahnung nicht rechtzeitig beglichen worden ist, kann Anlass für die Einmeldung sein. Nicht zuletzt kann auf die Unzuverlässigkeit der betroffenen Person geschlossen werden, wenn diese beim Abschluss eines Vertrages unwahre Angaben zu ihrer Erreichbarkeit macht oder wenn sie, solange eine Verbindlichkeit noch nicht erfüllt ist, den Gläubiger nicht von diesbezüglichen Änderungen informiert. Dabei muss die betroffene Person nicht unbedingt gemahnt worden sein noch sich im Verzug befinden. Auch gibt es für die Annahme von Zahlungsunwilligkeit bzw. Zahlungsunfähigkeit keine betragsmäßige Bagatellgrenze, zumal angesichts des nicht unerheblichen Beitreibungsaufwandes Gläubiger oftmals auf zu Unrecht verweigerte Kleinstbeträge verzichten müssen.

Wenn eine Person eine von einem Inkassounternehmen geltend gemachte Forderung für unbegründet hält, ist zu empfehlen, nicht zu bezahlen. Die Person sollte allerdings gegenüber dem angeblichen Gläubiger, gegenüber den von ihm eigeschalteten Inkassounternehmen und gegenüber Rechtsanwälten jeweils genau begründen, warum sie die Zahlung verweigert, damit sie nicht bei einer Auskunftei, etwa bei der SCHUFA, als „säumiger Schuldner bzw. Schuldnerin“ eingemeldet werden kann. Dann kann die Person alle weiteren Schreiben in dieser Angelegenheit unbeachtet lassen. Sollte ihr aber ein gerichtlicher Mahnbescheid zugehen, muss sie fristgerecht Widerspruch erheben.

Künstliche Intelligenz im Personalwesen

Formen von Künstlicher Intelligenz (KI) finden zunehmend auch Einzug ins Personalwesen der Betriebe. Im Einsatz von KI stecken enorme Potentiale, dies wird unsere Gesellschaft und besonders unsere Arbeitswelt nachhaltig verändern. Entsprechend der „Nationalen Strategie Künstliche Intelligenz“ der Bundesregierung soll der Einsatz von KI vorangebracht und insbesondere die Entwicklung dieser Zukunftstechnologie massive Unterstützung finden. Der Einsatz von KI im Bewerbungsverfahren und der Personalverwaltung ist (kollektiv-) arbeitsrechtlich noch nicht gesetzlich normiert worden und es bestehen einige Unsicherheiten. Ferner verlangt der Einsatz von KI eine enorme Verantwortung und ist mit viel Vorbereitungslast für Arbeitgeber verbunden.
Viele Arbeitgeber_innen wenden sich im Wege einer Beratungsanfrage an die Behörde, da sie, gerade mit Blick auf die Kontaktbeschränkungen während der Pandemie, Auswahlprozesse effektivieren wollen und automatisiert etwa mittels einer KI-basierten Bewerberanalyse leichter vollziehen möchten. Üblicherweise werden die Motivations-/ Begleitschreiben der Bewerbung oder im Rahmen einer Sprachanalyse die Sprache der Bewerber_innen automatisiert durch einen Algorithmus analysiert und bewertet.

Ob und auf welcher datenschutzrechtlichen Grundlage sich der Einsatz von KI im Bewerbungskontext vollzieht, ist im Kern noch offen. Eine ausdrückliche gesetzliche Grundlage besteht (bislang) nicht. Da es sich um automatisierte Verfahren handelt, welche personenbezogene Daten der Bewerber_innen verarbeiten, legt die DS-GVO hierbei die Rahmenbedingungen fest. In der algorithmischen Entscheidungsfindung liegt sicherlich eine Verarbeitung von personenbezogenen Daten. Diese Verarbeitung findet automatisiert statt, sodass für eine Sprachanalyse üblicherweise Art. 22 DS-GVO zum Zuge kommt. Ferner bedarf es einer Rechtsgrundlage, wobei zunächst an die Einwilligung zu denken ist. Da sich die Bewerber_innen aber sorgen müssen, bei Nichterteilung der Einwilligung keine Berücksichtigung zu finden, erscheint die Freiwilligkeit der Einwilligung mehr als fraglich.

Die Potentiale und Möglichkeiten von KI können zudem Begehrlichkeiten wecken. Durch KI basierte Bewerberanalyse dürfen daher unter keinen Umständen überschießende Informationen, also für die Begründung des Beschäftigungsverhältnisses unerhebliche Daten zur Persönlichkeit der Bewerber_innen erhoben und analysiert werden. Die vom Bundestag eingesetzte Enquete-Kommission „Künstliche Intelligenz“ sieht jedoch ausdrücklich einen künftigen Anwendungsbereich von KI im Bereich der „Personalverwaltung“ sowie der „Bewerberauswahl“ (vgl. Enquete-Kommission, Kommissionsdrucksache 19 (27) 127 v. 25.09.2020), sodass diesbezüglich eine gesetzliche Regelung wünschenswert ist.

>> Weitere Informationen

Hinweise zur KI-gestützten Bewerberanalyse
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/04/Ratgeber-Beschäftigtendatenschutz.pdf

Löschfristen im Betriebs- und Personalratsbüro
Viele Mitarbeitervertretungen wenden sich an uns und bitten um Unterstützung bei der datenschutzgerechten Implementierung von Aufbewahrungs- oder Löschfristen für Beschäftigtendaten in ihren Gremien. Hierbei erreichten uns Anfragen sowohl von Betriebs- und Personalräten, als auch von vielen Schwerbehindertenvertretungen. Auch zwei Jahre nach Inkrafttreten der DS-GVO nehmen die Beratungsanfragen insbesondere zu Löschfristen keineswegs ab und die Relevanz bleibt auf hohem Niveau.

Im Betriebsverfassungsgesetz ist keine ausdrückliche Regelung enthalten, wie lange etwa Betriebsräte ihnen überlassene Unterlagen und Dokumente aufzubewahren oder wann sie diese zu löschen haben. Das Personalvertretungsgesetz von Baden-Württemberg sieht in § 65 Abs. 2 für Personalräte lediglich vor, dass personenbezogene Daten gespeichert werden dürfen,

„soweit und solange dies zur Erfüllung ihrer Aufgaben erforderlich ist. Nach Abschluss der Maßnahme, an der die Personalvertretung beteiligt war, sind die ihr in diesem Zusammenhang zur Verfügung gestellten personenbezogenen Daten zu löschen und Unterlagen mit personenbezogenen Daten der Dienststelle zurückzugeben".

Demnach gelten hinsichtlich der Aufbewahrung und Löschung von Beschäftigtendaten für die Mitarbeitendenvertretungen im Kern dieselben Voraussetzungen wie für die Arbeitgeber_innen, welche Daten speichern dürfen, solange dies zur Begründung, Durchführung oder Beendigung eines Beschäftigtenverhältnisses erforderlich ist. Besteht diese Erforderlichkeit nicht mehr, wandelt sich die Aufbewahrungspflicht in eine Löschpflicht. Für auf Papier und elektronisch erfasste Daten gelten dieselben Grundsätze. Ausgangspunkt für die Aufbewahrung der personenbezogenen Daten durch die Mitarbeitervertretungen ist die Erforderlichkeit der Speicherung für einen konkreten und zuvor festgelegten kollektivarbeitsrechtlichen oder sozialrechtlichen Zweck im Rahmen ihrer Gremienarbeit.

10.4 Neues aus dem Amt IV: Alles mit V – Videoüberwachung, Verkehr, Vereine

Neue Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen"
In diesem Tätigkeitsbericht sprechen wir mit verschiedenen Bezügen immer wieder über das Thema Videoaufnahmen. Weil bei nicht-öffentlichen Stellen Videoüberwachung immer wieder auftaucht haben wir unter dem Vorsitz unserer Behörde im Arbeitskreis Videoüberwachung der Datenschutzkonferenz die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen" grundlegend überarbeitet.

Täglich greift die Videoüberwachung in Rechte und Freiheiten von Personen ein, ohne dass die Mehrzahl dafür einen Anlass gegeben hat. Mit großer Streubreite wird aufgezeichnet, zu welcher Uhrzeit, an welchem Tag, in welchem Zustand, mit welchem Erscheinungsbild, wie lange und an welchem Ort sich Betroffene aufhalten, wie sie diesen Bereich nutzen, wie sie sich dort verhalten und ob sie allein oder in Begleitung sind. Bereits eine einfache Überwachungsanlage verarbeitet in erheblichem Umfang personenbezogene Daten, ohne dass der Großteil der erfassten Informationen für Überwachende je eine nützliche Rolle spielt.

Das Risiko, dass damit die Rechte von Betroffenen verletzt werden, hat sich in den vergangenen Jahren deutlich erhöht. Grund dafür sind die geringen Anschaffungskosten und die verbesserte Qualität der Technik. Moderne Kameras zeigen Bilder in höchster Auflösung. In Echtzeit können diese in der ganzen Welt eingesehen und fast unbegrenzt gespeichert werden. Mehr als ein Smartphone oder Tablet braucht es dafür oft nicht. Dabei werden Kameras nicht nur zur Sicherheit eingesetzt. Kameras erfassen und verarbeiten Daten von Personen, um personalisierte Werbung anzuzeigen oder Produkte zielgruppengenau anzubieten. Softwaregesteuerte Videotechnik vermisst in der Öffentlichkeit Gesichtszüge und Gefühlsregungen von Personen oder verfolgt das Bewegungs- oder Einkaufsverhalten von Kunden.

Die erfassten Informationen werden in Sekundenbruchteilen ausgewertet und vervielfältigt. Betroffene haben kaum Einfluss auf eine solche Erfassung und erfahren selten, was mit den Aufnahmen geschieht.

Die Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ wurde grundlegend überarbeitet und an die rechtlichen Rahmenbedingungen der seit dem 25. Mai 2018 wirksamen DS-GVO angepasst. Neu hinzugekommen sind die Abschnitte zur „Videoüberwachung in der Nachbarschaft“ und zur „datenschutzrechtlichen Bewertung von Tür- und Klingelkameras, Drohnen und Wildkameras sowie Dashcams“.

Mit der Orientierungshilfe erhalten Betroffene und Verantwortliche Informationen über die Voraussetzungen für eine datenschutzgerechte Videoüberwachung in unterschiedlichen Lebensbereichen, Muster für Hinweisschilder und eine Checkliste mit den wichtigsten Prüfungspunkten im Vorfeld einer Videoüberwachung.

>> Weitere Informationen

Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2020/09/20200903_oh_vue.pdf

Videoüberwachung in Gaststätten gibt Anlass für Vor-Ort-Kontrollen

Bereits im 33. Tätigkeitsbericht (2016/2017) haben wir von der Zunahme der Videoüberwachung in verschiedenen Lebensbereichen, darunter auch Gaststätten, berichtet und sind ausführlich auf die rechtlichen Voraussetzungen hierfür eingegangen. Nach wie vor erreichen uns Beschwerden von Gästen und Mitarbeitenden. In manchen Fällen sind Vor-Ort-Kontrollen nötig.

In einem Fall wandten sich verzweifelte Mitarbeiterinnen eines Krankenhauscafés an uns. Nachdem wir die Chefin des Cafés bereits zur Stellungnahme aufgefordert hatten, erklärte eine Mitarbeiterin glaubhaft am Telefon, dass die Leitung zwei Personen gekündigt habe, weil diese nicht in die Videoüberwachung eingewilligt hätten. Es sei in diesem Zusammenhang angekündigt worden, dass weitere „Köpfe rollen werden“. Die Beschäftigten des Cafés könnten sich der Überwachung nicht entziehen. Es handele sich um insgesammt sieben Kameras. Von externen Geräten könne über das Internet auf die Aufnahmen zugegriffen werden. In diesem Fall hielten wir eine Kontrolle für Ort für geboten, was wir der Betreiberin des Cafés auch mitteilten. Diese Ankündigung hat offenbar gewirkt. Bei unserem Besuch vor Ort war keine einzige Kamera in Betrieb. Die Leitung des Cafés erklärte, sie wolle künftig nur noch außerhalb der Arbeits- und Öffnungszeit zum Schutz vor Einbrechern überwachen. Dem steht das Datenschutzrecht nicht entgegen.

Einer Gaststätte mit gutbürgerlicher Karte statteten wir aufgrund der Beschwerde eines Gastes einen Kontrollbesuch ab. Dort mussten wir feststellen, dass der Inhaber zeitlich unbeschränkt von seinem Smartphone aus jederzeit auf Kamera-Livebilder zugreifen konnte. Eine unzulässige Verhaltens- und Leistungskontrolle der Mitarbeitenden konnte nicht ausgeschlossen werden. Abhilfe schaffte das Anbringen einer mechanischen Zeitschaltuhr an der Kamera, sodass ein Zugriff per App nur noch außerhalb der Öffnungs-und Arbeitszeiten möglich ist.

Wir erhalten Hinweise auf unzulässige Videoüberwachungen von Behörden oder erfahren davon durch Beschwerden betroffener Personen. Diese veranlassen uns auch zu Kontrollbesuchen. Gastwirte haben auch künftig mit anlassunabhängigen Kontrollen zu rechnen.

„Mein Auto sieht Dich!“ – Tesla & Co

Die Marke Tesla, Inc. steht für hochmoderne Fahrzeuge der neuesten Generation. Nicht nur, dass die Tesla-Fahrzeuge rein elektrisch unterwegs sind, der Hersteller ist auch bemüht, das vollständig autonome Fahren in nicht allzu ferner Zukunft zu ermöglichen. Jetzt schon besitzen die Modelle von Tesla viele Sensoren für teilautonomes Fahren.

Was weniger bekannt ist: Elon Musk hat sämtliche Tesla-Modelle bereits mit Fahrassistenzsystemen ausgerüstet, die auf derzeit acht kleine Kameras zurückgreifen. Diese fest mit der der Karosserie verbauten Geräte stellen somit bereits u.a. den technischen Einstieg für den teilautonomen und später den autonomen Fahrbetrieb dieser Fahrzeuge dar.

Grundsätzlich unterscheidet sich ein Fahrzeug der Marke Tesla, Inc. dadurch nicht von einem modernen Fahrzeug anderer Hersteller. Jedoch enthalten die Tesla-Fahrzeuge weitere innovative Funktionalitäten, wie zum Beispiel den „Wächtermodus“ (Sentry Mode) und eine eingebaute „Dashcam“-Funktion. Diese Funktiona-

litäten werden für den Betrieb des teilautonomen und autonomen Fahrens nicht genutzt und sind auch nicht dafür vorgeschrieben. Sie dienen einem ganz anderen Zweck: Der Wächtermodus ist eine Überwachungsfunktion und soll laut Hersteller dem Schutz vor Diebstahl und Vandalismus dienen. Bei einem parkenden Tesla sind im Wächtermodus die acht fest verbauten Kameras an der Karosserie aktiviert. Sie nehmen ständig die Umgebung rund um das Fahrzeug auf, speichern die Videobilder vorläufig ab und überschreiben sie alle 60 Minuten. Kommt es in der Nähe des parkenden Fahrzeugs zu einer verdächtigen Bewegung, wird der Warnungszustand aktiviert und die Videobilder der letzten 10 Minuten vor dem Ereignis und 30 Minuten danach werden auf einer SD-Karte in dem Fahrzeug gespeichert.

Während der Fahrt funktionieren die fest verbauten Kameras wie Dashcams. In den Tesla-Fahrzeugen wird das Verkehrsgeschehen erfasst, permanent aufgezeichnet und immer wieder nach einer Stunde überschrieben. Bei einem auslösenden Ereignis, wie z. B. Hupen oder starkem Bremsen, werden die letzten 10 Minuten dauerhaft gespeichert.

Wir erhielten in zwei Fällen von Polizeidienststellen CDs mit Videobildern von Tesla-Fahrzeugen. Es ging dabei sowohl um den Wächtermodus als auch um die Dashcam-Funktion. Die Tesla-Fahrer hatten bei der Polizei zum einen versuchten Diebstahl des Fahrzeugs und zum anderen Verstöße gegen die Straßenverkehrsordnung anderer Verkehrsteilnehmer im fließenden Verkehr angezeigt. Auf dem Videomaterial, welches den Wächtermodus betraf, war zu erkennen, dass die nähere Umgebung rund um das Fahrzeug aufgenommen wird. Jeder, der am Fahrzeug vorbeigeht, wird erfasst. Die Auflösung der Bilddateien lässt es zu, Personen eindeutig zu erkennen.

Videodaten von Personen oder Kfz-Kennzeichen im Verkehrsgeschehen sind personenbezogene Daten. Diese Daten dürfen nicht verarbeitet werden, es sei denn, es gibt eine gesetzliche Grundlage hierfür oder eine Einwilligung. Eine solche Einwilligung ist bei Videodaten aus dem Auto heraus nicht einholbar. Die Videoüberwachung aus einem Auto heraus ist immer ein Eingriff in die informationelle Selbstbestimmung der Betroffenen, die sich im Verkehrsraum bewegen.

© Andrey Popov – stock.adobe.com

Manche Autos wollen mit Kameraüberwachung Diebstahl verhindern und Sicherheit bieten – und schießen dabei über das Ziel hinaus.

Der Wächtermodus kann zwar deaktiviert werden, die Dashcam-Funktion kann aber nicht abgeschaltet und auch in ihren Einstellungen nicht abgeändert werden. Somit können aufgrund der nicht zu ändernden Voreinstellungen von Tesla die beschriebenen Funktionalitäten nicht rechtskonform betrieben werden, denn für die so erfolgenden Aufnahmen ist keine Rechtsgrundlage ersichtlich.

Bereits der BGH hatte dahingehend entschieden, dass das anlasslose und permanente Filmen einer Vielzahl von Personen mittels einer Dashcam datenschutzrechtlich unzulässig ist (vgl. Urteil vom 15. Mai 2018 (VI ZR 233/17)).

Ein datenschutzgerechter Einsatz zum Zweck der Beweissicherung bei einem Unfall mit Sach- und Personenschäden (zivilrechtliche Ansprüche) wäre laut BGH zwar möglich, wenn technische Möglichkeiten der Beschränkung des Eingriffs in das informationelle Selbstbestimmungsrecht der Verkehrsteilnehmer bestünden wie etwa nur kurzzeitige, anlassbezogene Aufzeichnungen, die erst bei Kollision oder starker Verzögerung des Fahrzeugs durch einen Bewegungssensor ausgelöst werden, ggf. durch Verpixelung von Personen oder automatisiertes und dem Eingriff des Verwenders entzogenes Löschen. Nur dann kommt eine Güterabwägung zu Gunsten des Dashcam-Betreibers überhaupt in Betracht.

Diese Zeiträume, die bei der Dashcam-Funktion von Tesla voreingestellt sind, können nicht als kurzzeitig bezeichnet werden. Auch die Speicherung der letzten 10 Minuten vor dem auslösenden Ereignis stellt keine kurzzeitige, anlassbezogene Aufzeichnung im Sinne der Rechtsprechung des BGH dar.

Noch gravierender sind die Einstellungen im Wächtermodus. Eine dauerhafte und anlasslose Überwachung des öffentlichen Bereichs rund um das geparkte Fahrzeug ist nicht statthaft.

Aus diesem Grund sind die derzeitigen Funktionen des Wächtermodus und der Dashcam in einem Tesla-Fahrzeug in Europa nicht rechtskonform einsetzbar. Wir haben die Fahrer der Tesla Fahrzeuge aufgefordert, die Funktionen des Wächtermodus zu deaktivieren und das Speichermedium für beide Funktionen zu entfernen. Die Fahrer zeigten sich einsichtig und akzeptierten die Entscheidung.

Nicht zuletzt aufgrund dieser Entscheidung ist eine Diskussion über den rechtskonformen Einsatz der Kamerafunktionen bei den Tesla-Fahrzeugen entbrannt. Es bleibt zu hoffen, dass sich dies bis zur Konzernzentrale in Kalifornien herumspricht und der Hersteller in seinen Fahrzeugen zumindest für den europäischen Markt datenschutzgerechte Funktionalitäten gewährleistet. Verantwortlich dafür bleibt aber – nach den Vorgaben der DS-GVO – der Fahrzeughalter und –führer, nicht etwa Tesla, Inc.

„Parkraumüberwachung“

Häufig erreichen uns Beschwerden, man sei von einem privaten Parkraumüberwachungsunternehmen aufgeschrieben und nun wegen „Falschparkens“ zur Kasse gebeten worden. Wie verträgt sich das mit dem Datenschutz?

Wer als Fahrer auf einen privaten Stellplatz oder in ein Parkhaus fährt, schließt „stillschweigend“ mit dem Betreiber der Parkfläche einen Vertrag ab, demzufolge er eine Vertragsstrafe zu entrichten hat, wenn er die dort geltende Parkordnung nicht einhält. Voraussetzung ist, dass die Allgemeinen Geschäftsbedingungen, welche die Vertragsstrafe vorsehen, so angezeigt werden, dass man von ihnen Kenntnis nehmen kann. Der Betreiber des Parkraums kann die Einhaltung der Parkordnung aufgrund seines Hausrechts selbst überwachen oder von einem Unternehmen überwachen lassen.

Hier die Antwort auf einige Fragen, die dazu häufig an uns gestellt werden:

Woher hat dieses Unternehmen meine Erreichbarkeitsdaten?

Das Überwachungsunternehmen kann sich die Daten des jeweiligen Fahrzeughalters über das Kraftfahrtbundesamt oder die Zulassungsstelle beschaffen. Dazu muss glaubhaft machen, dass u. U. ein Rechtsanspruch im Zusammenhang mit dem Betrieb des Fahrzeuges besteht. Dazu genügt es, wenn vorgetragen wird, dass der Halter zumindest Angaben zur Ermittlung des Fahrers machen kann.

Was darf das Unternehmen mit meinen Daten machen?

Das Unternehmen kann die Daten nutzen, um den Halter des fraglichen Fahrzeuges anzuschreiben und danach zu fragen, ob er den „Parkverstoß“ begangen

hat bzw. wer der Fahrer war, der den Vertrag abgeschlossen hat.

Muss ich als Halter den Fahrer angeben?
Nach der jüngeren Rechtsprechung des Bundesgerichtshofes muss der Halter „im Rahmen des ihm Zumutbaren" dem Unternehmen mitteilen, wer als Fahrer infrage kommt. Der Halter muss, wenn er nicht weiß oder wissen sollte, wer das Fahrzeug zum fraglichen Zeitpunkt benutzt hat, zumindest so konkrete Angaben machen, die es dem Unternehmen ermöglichen, den „Vertragspartner" zu ermitteln. Macht der Halter das nicht, muss er besagte Vertragsstrafe selbst bezahlen. Allerdings ist es nicht zulässig, wenn das Unternehmen dem Halter droht, er müsse das Entgelt stets selbst bezahlen, wenn der Fahrer letztlich nicht ermittelbar ist. Ein solcher Hinweis ist unzutreffend und verstößt auch gegen das Wettbewerbsrecht. Der Halter haftet nur, wenn er etwas verschweigt, was er sagen könnte.

Was soll ich tun, wenn ich den Parkverstoß nicht begangen habe?
Wenn Sie diesen Anspruch für unbegründet halten, empfehlen wir Ihnen, nicht zu bezahlen. Sie sollten allerdings gegenüber dem Überwachungsunternehmen, gegenüber den von ihm eigeschalteten Inkassobüro und gegenüber Rechtsanwälten jeweils genau begründen, warum Sie die Zahlung verweigern, damit Sie nicht bei einer Auskunftei, etwa bei der SCHUFA, als „säumiger Schuldner" eingemeldet werden können.

Wie lange darf das Unternehmen meine Daten nach Abschluss des Inkassoverfahrens speichern?
Nach Abschluss eines Inkassoverfahrens sind die Daten der betroffenen Person von dem Überwachungsunternehmen grundsätzlich zu löschen. Die weitere Speicherung ist für einen angemessenen Zeitraum nur zulässig, wenn die maßgeblichen Geschäftsbedingungen vorsehen, dass im Wiederholungsfall eine höhere „Gebühr" erhoben wird, oder wenn die Vertragsstrafe berechtigt war und das Unternehmen bei einem neuen Verstoß auf keinen Fall im Wege der Kulanz auf die Gebühr verzichten will. Allerdings ist das Unternehmen verpflichtet, auch nach dem endgültigen Abschluss eines Vorgangs die Daten noch für eine angemessene Dokumentationsfrist in einer Dokumentationsdatei gesperrt vorzuhalten. Diese können dann nur noch für das Finanzamt, für Datenschutzkontrollen oder für zu erwartende gerichtliche Verfahren genutzt werden, dürfen jedoch nicht mehr von den Sachbearbeitern eingesehen werden können.

Der Parkausweis für Menschen mit Behinderungen
Welche Angaben darf ein Parkausweis für Menschen mit Behinderung enthalten? Besonders heikel ist, dass die auf der Vorderseite des Ausweises stehenden personenbezogenen Daten – da der Ausweis beim Parken gut sichtbar hinter der Windschutzscheibe platziert werden muss – von „interessierten Passanten" gelesen werden können. Da nur Menschen mit Behinderung einen solchen Parkausweis erhalten, sind auch von der DS-GVO besonders geschützte Gesundheitsdaten betroffen.

Jeder kennt die mit dem Zusatzzeichen „Rollstuhlfahrersymbol" besonders gekennzeichneten Parkplätze (sogenannte Behindertenparkplätze). Zum Parken auf einem solchen Parkplatz berechtigt der blaue Parkausweis, den Menschen mit bestimmten Einschränkungen (z.B. blinde Menschen oder Menschen mit einer außergewöhnlichen Gehbehinderung) erhalten können. Daneben gibt es noch die „kleine Schwester" des blauen Parkausweises, den orangefarbenen Parkausweis. Auf diesen haben weitere Personengruppen Anspruch, z.B. Personen, die zwar nicht außergewöhnlich gehbehindert sind, aber doch unter sehr starken Einschränkungen beim Gehen leiden. Der orangefarbene Parkausweis berechtigt nicht zum Parken auf einem Behindertenparkplatz, gewährt aber beispielsweise die folgenden Berechtigungen, wenn in zumutbarer Entfernung keine andere Parkmöglichkeit besteht:

© karagrubis – stock.adobe.com

Parkplatz für Menschen mit Behinderung.

• Parken bis zu drei Stunden an Stellen, an denen das eingeschränkte Halteverbot angeordnet ist,

• Parken über die zugelassene Zeit hinaus an Stellen, an denen Parken erlaubt, aber durch ein Zusatzschild eine Begrenzung der Parkzeit angeordnet ist,

• Parken während der Ladezeiten in Fußgängerbereichen, in denen das Be- und Entladen für bestimmte Zeiten freigegeben ist,

• Parken bis zu drei Stunden auf Parkplätzen für Anwohnerinnen und Anwohner.

Welche Angaben dürfen auf der Vorderseite eines solchen orangefarbenen Parkausweises stehen? Diese Frage stellte uns eine betroffene Person: Ihr Parkausweis, den das zuständige Landratsamt ausgestellt hatte, enthalte auf der Vorderseite ihren Vor- und Nachnamen und ihre Adresse. Da der Parkausweis während des Parkens gut sichtbar hinter der Windschutzscheibe ausliegen muss, sah sie dies als „Sicherheitsrisiko" an. Das Landratsamt war anscheinend der Ansicht, dass die Angaben zu „Kontrollzwecken" erforderlich seien.

Besonders kritisch war im konkreten Fall, dass die auf der Vorderseite des Parkausweises enthaltenen Angaben nicht nur Behördenmitarbeiter, deren Aufgabe es ist, die Einhaltung der Verkehrsvorschriften zu kontrollieren, erfuhren, sondern auch „interessierte Passanten". Da den orangefarbenen Parkausweis nur bestimmte Gruppen schwerbehinderter Menschen erhalten können, erhielten die „Vorübergehenden" neben Name und ggf. Adresse zwangsläufig auch die Information, dass es sich hierbei um einen schwerbehinderten Menschen handelt.

An der Zulässigkeit der Vorgehensweise des Landratsamts hatten wir aus folgenden Gründen massive Zweifel, die wir dem Landratsamt mitteilten:

• Der blaue Parkausweis enthält nach unserem Kenntnisstand den Namen des schwerbehinderten Menschen nur auf der Rückseite. Das heißt, dieses Datum ist bei Auslage des Ausweises im Fahrzeug nicht zu sehen. Die Adresse des schwerbehinderten Menschen enthält der Ausweis nicht. Die Gestaltung des blauen Parkausweises wird augenscheinlich für Kontrollzwecke als ausreichend angesehen.

• Im Verkehrsblatt (2009, Seiten 390-392), dem Amtsblatt des Bundesverkehrsministeriums, ist ein Muster des orangefarbenen Parkausweises „bekannt gegeben". Name und Adresse des schwerbehinderten Menschen enthält der (Muster-)Parkausweis nicht. Der Ausweis wird mit einer Nummer einer (ebenfalls nummerierten) Ausnahmegenehmigung zugeordnet, die Name und Adresse des schwerbehinderten Menschen enthält. Aus Sicht des Bundesverkehrsministeriums wird dies für Kontrollzwecke demnach als ausreichend angesehen. Fraglich ist auch, ob es überhaupt zulässig ist, (durch Aufnahme weiterer Angaben) von dem Muster abzuweichen.

• Name und Adresse einer Person auf einem orangefarbenen Parkausweis, den nur schwerbehinderte Menschen erhalten, stehen in enger Verbindung mit den personenbezogenen Daten im Sinne von Artikel 9 der DS-GVO (Gesundheitsdaten) und sind daher besonders schützenswert.

Das Landratsamt hat zeitnah geantwortet, unsere Rechtsauffassung vollumfänglich zu teilen. Es kündigte weiter an, die Praxis mit sofortiger Wirkung zu ändern und den Kreis der betroffenen Personen zu ermitteln. Diesen werde ein neuer Parkausweis ausgestellt und zugesandt, „damit der datenschutzkonforme Zustand wiederhergestellt werden kann".

Das „Fehlermanagement" des Landratsamts war vorbildlich: Der Fehler wurde zeitnah eingeräumt, die Praxis mit sofortiger Wirkung geändert und allen betroffenen Inhabern des orangefarbenen Parkausweises ein neuer Ausweis ausgestellt und zugesandt. Passt so.

„Reisefieber" in pandemischen Zeiten?

Über einen eingegangenen Hinweis erhielten wir Kenntnis von einem sogenannten „Corona Sicherheitskonzept" eines Luxusfernbusunternehmens, dessen Angebot sich auf innerdeutsche Fahrstecken beschränkt. Verwiesen wurde auch auf die Homepage des Unternehmers. Demnach erfolgt bereits am Eingang des Busses mittels eines Kamerasystems eine „Intelligente Zugangskontrolle" der Fahrgäste. Diese sind bereits zu diesem Zeitpunkt im Besitz der Fahrtickets, da eine Buchung über das eigene Internetportal zu erfolgen hat unter gleichzeitiger Bezahlung des Transportpreises über einen Zahlungsdienstleister. Das Kamerasystem soll hier mit einem Körpertemperatursensor ausgestattet sein. Den Unternehmensan-

gaben zufolge misst dieses „die Temperatur der Passagiere und meldet, wenn diese über 37 Grad liegt". Der gesamte Vorgang erfolge automatisch und in Echtzeit. Mutmaßlich wird bei entsprechender Warnmeldung diesen Kunden der Zutritt zum Businnenraum untersagt.

Um zu prüfen, ob das System tatsächlich den datenschutzrechtlichen Anforderungen genügt, haben wir darum gebeten, dass uns entsprechende Informationen übersandt werden, insbesondere das gesamte Verfahren der Datenverarbeitung aufgezeigt wird.

Zu unserer Verwunderung erhielten wir einen Zweizeiler zur Antwort mit der lapidaren Aussage, die auch auf der Homepage veröffentlicht ist, dass keine persönlichen Daten der Fahrgäste aufgezeichnet würden. Mit dieser Kurzantwort gaben wir uns allerdings nicht zufrieden und wandten uns erneut an das Unternehmen. Denn die Maßnahmen sind nach unserer Meinung durchaus geeignet, in das Recht auf informationelle Selbstbestimmung einzugreifen, auch wenn es sich bei dem Innenraum des Busses um einen Bereich handelt, der dem Hausrecht des Busunternehmers unterliegt.

Für uns unstrittig stellt die Erfassung der Körpertemperatur mithilfe eines Wärmebildkamerasystems eine automatisierte Verarbeitung personenbezogener Daten im Sinne des Art. 4 Nr. 2 DS-GVO dar. Dies hängt auch nicht davon ab, ob die Aufnahmen gespeichert werden oder ob diese nur im Live-Betrieb auf dem Monitor abgebildet werden (vgl. hierzu BVerwG, Urteil vom 27.03.2019, – 6 C 2/18, Absatz 43 der Entscheidungsbegründung, in NJW 2019, 2556). Die elektronische Temperaturmessung bezweckt einzig und allein, Personen zu erkennen, die Fieber haben und möglicherweise mit SARS-CoV-2 infiziert sind. Dies stellt eine Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Nr. 15 DS-GVO dar, die aber nach Art. 9 Abs. 1 DS-GVO grundsätzlich verboten ist.

Da uns derzeit keine Tatsachen vorliegen, die einen der Ausnahmetatbestände des Art. 9 Abs. 2 DS-GVO begründen könnten, werden wir dem Unternehmen demnach auch mitteilen, dass es ein Verarbeitungsverbot für solche Gesundheitsdaten gibt.

Auch in pandemischen Zeiten ist zur Wahrung des Datenschutzes eine sorgfältige und detaillierte Überprüfung der Maßnahmen anhand der gesetzlichen Anforderungen geboten. Umgesetzt wird demnach auch der Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zum Einsatz von Wärmebildkameras bzw. elektronischer Temperaturerfassung im Rahmen der Corona-Pandemie vom 10.09.2020.

>> Weitere Informationen
https://www.datenschutzkonferenz-online.de/media/dskb/20200910_beschluss_waeremebildkameras.pdf

© ivandanru – stock.adobe.com

Körpertemperatur mit einem Wärmebildkamerasystem zu messen bedeutet die automatisierte Verarbeitung personenbezogener Daten.

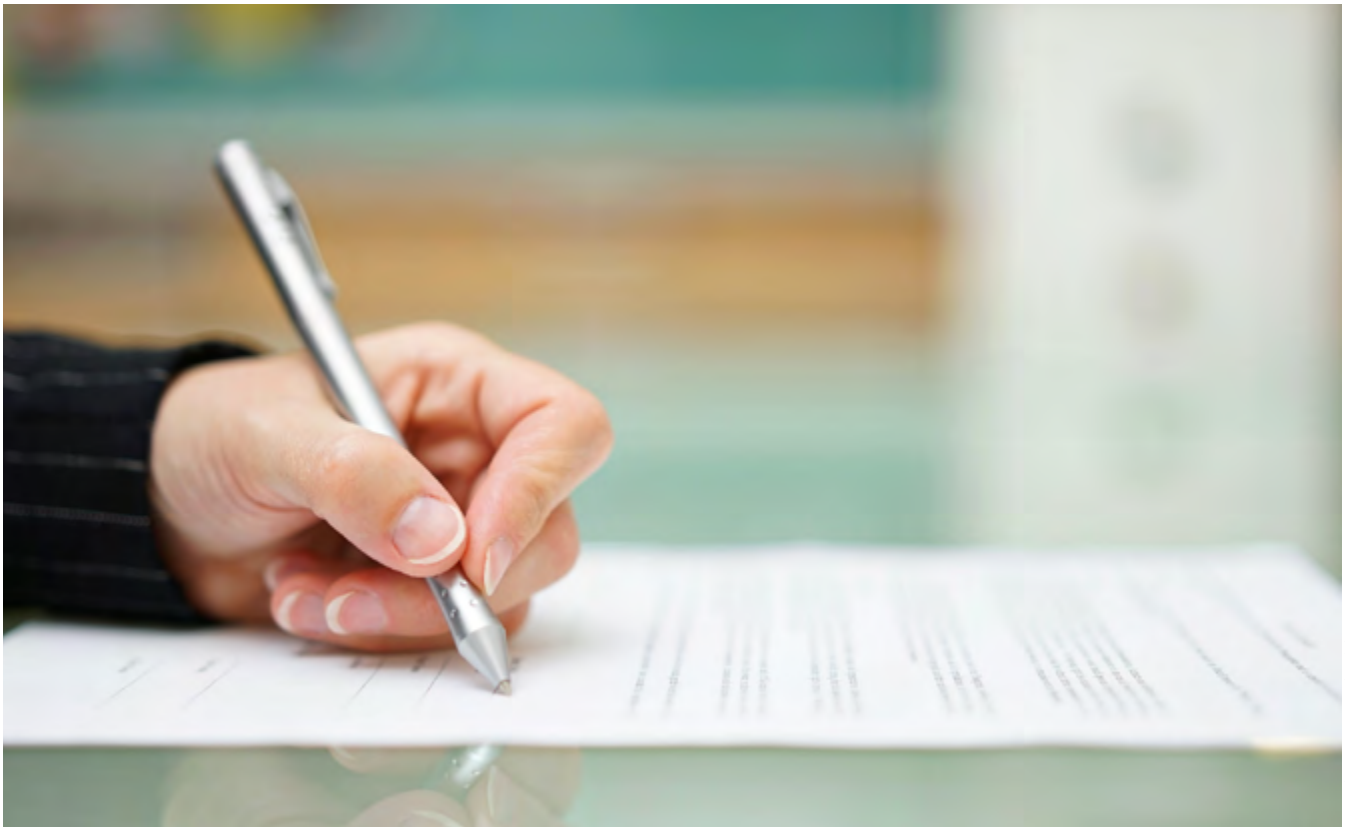
Vereine I: Zuschauer-Datenerhebung

Eine Anfrage befasste sich mit den Daten, die bei Zuschauern von Fußballspielen erhoben wurden. Diese Datenerhebung gemäß der Corona-Verordnung diente dazu, im Falle einer Infektion eine Rückverfolgung möglich zu machen. In der Praxis gestaltete es sich oftmals so, dass am Eingang des Sportplatzes eine Liste ausgelegt wurde, in die sich die Zuschauer eintragen mussten. Sofern die Zuschauer sich hintereinander auf die einzig ausliegende Sammelliste eintrugen, erhielt jeder Einsicht in die personenbezogenen Daten derer, die sich vor ihm eingetragen hatten. Diese Listen sollen oft unbeaufsichtigt, teilweise auch zum Abfotografieren geeignet gewesen sein. In einem Falle wurde der Zugang zur Veranstaltung verweigert, als sich die betreffende Person weigerte, sich in eine offene, unbeaufsichtigte Liste einzutragen.

Grundsätzlich darf eine verantwortliche Stelle die Daten nur in einer Weise verarbeiten, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung. Dazu sind geeignete technische und organisatorische Maßnahmen zu ergreifen (vgl. Art. 5 Abs. 1 Buchstabe f) DS-GVO zur „Integrität und Vertraulichkeit").

Die Verordnung des Kultusministeriums und des Sozialministeriums über Sport regelt die Sportausübung in Baden-Württemberg. Sie wurde am 25. Juni 2020 durch öffentliche Bekanntmachung des Kultusministeriums notverkündet und galt ab dem 1. Juli 2020. Sie ist seit dem 13. September 2020 nicht mehr gültig, war jedoch für unsere Antwort heranzuziehen. Die Landesregierung Baden-Württemberg hatte die Corona-Verordnung vom 1. Juli 2020 erstmals geändert. Auch gem. § 6 Absatz 2 der CoronaVO (in der dann geänderten Fassung vom 28. Juli 2020) ist zu gewährleisten, dass Unbefugte keine Kenntnis von den Daten erlangen. Diese dienen ausschließlich dem Zweck der Auskunftserteilung gegenüber dem Gesundheitsamt oder der Ortspolizeibehörde. Dies wurde von uns abschließend als Antwort mitgeteilt.

Die Datenerhebungen zur Erfüllung der Dokumentationspflichten aus der Corona-Verordnung durften zu keiner Zeit durch offen einsehbare Listen erfolgen. Die Daten sind vielmehr so zu erheben, dass sie nur dem Verein als Sportstättenbetreiber bekannt werden, nicht jedoch unbefugten Personen.



© Bacho Foto – stock.adobe.com

Auch bei Sportveranstaltungen gilt: Niemals Sammellisten auslegen zur Kontakterfassung von Besuchern.

Vereine II: Selbsterhebungs-Fragebögen bei der Tieradoption

Immer wieder wird die Situation derer ausgenutzt, die ihre personenbezogenen Daten im Austausch für eine begehrte Vereinsleistung offenzulegen haben. Dann werden schon mal „überschießende" Informationen und Daten abgefragt, was nicht mit dem Datenminimierungsgrundsatz des Art. 5 der DS-GVO vereinbar ist.

So wurde uns eine Datenerhebung eines Tiervermittlungsvereins gemeldet. Darin ging es um die Adoption eines Tieres, um die sich ein Antragsteller beworben hatte. Voraussetzung für das Einleiten des Adoptionsprozesses war dabei eine Selbstauskunft durch einen Fragebogen. In diesem Fragebogen wurden dann überschießende Informationen verlangt: Der Antragsteller sollte darin auch Fragen zu solchen Personen beantworten, die außerhalb seines Haushalts leben; auch die Übermittlung seiner Personalausweis-Nummer war dabei vorgesehen. Seine Nachfrage bei dem Verein habe ergeben, dass dies mit Vorgaben durch das Veterinäramt begründet sei. Eine Rechtsgrundlage konnte vom Verein nicht benannt werden.

Zur Erreichung des bestimmten (legitimen) Zwecks erforderlich sind hier nicht die Daten im Hinblick auf sämtliche Familienangehörigen, wie deren Anzahl oder deren Alter oder ob in der Familie (allgemein) Tierhaarallergien bekannt sind. Der Umstand, dass eine entfernt lebende Verwandte, mit der die Familie kaum Kontakt pflegt, eine Tierhaarallergie hat, wird wohl kaum ein relevantes Datum für eine am Grundsatz der Verhältnismäßigkeit und dem Grundsatz der Datenminimierung ausgerichtete Datenerhebung sein. Desgleichen erschließt sich uns der Zweck nicht, allgemein die Anzahl und das Alter aller Familienmitglieder zu erfragen und damit auch diejenigen Personen zu erfassen, die außerhalb des Haushalts bzw. des relevanten Kontakts des Antragstellers stehen. Die Übermittlung der Personalausweis-Nummer sahen wir zudem durch das Personalausweisgesetz nicht gedeckt.

Den vom Verein verfolgten legitimen Zweck sahen wir darin, dass er seinen Verpflichtungen dem Tierwohl gegenüber zu entsprechen hat. Das beinhaltet jedoch nicht, sämtliche Daten eines Antragstellers und seines familiären Umfeldes vorab „auf Vorrat" und vorbeugend zu erheben, um dann aus einer möglichst umfassenden Datenmenge jene Daten herauszufiltern, die am Aussagekräftigsten erscheinen. Eine Rechtsgrundlage für die auf das familiäre Umfeld ausgedehnte Datenerhebung bestand somit nach Art. 6 DS-GVO nicht. Informationen gem. Art. 12 ff. DS-GVO fehlten außerdem.

© lenaivanova2311 – stock.adobe.com

Tieradoption bedeutet auch Fragebögen ausfüllen.

Um dem Datenminimierungsgrundsatz der DS-GVO zu entsprechen, ist zwischen der Formulierung „im Haushalt lebende Personen" und der Formulierung „im familiären Umfeld lebende Personen" zu unterscheiden. Angaben zur Gesundheitssituation aller im familiären Umfeld lebenden Personen waren dabei nicht erforderlich. Soweit es sich um personenbezogene Daten Dritter handelt, sind diese zusätzlich nach Art. 14 DS-GVO zu informieren.

Der vom Verein zur Überprüfung verwendete Fragebogen durfte für den Antragsteller so nicht verwendet werde und wurde dementsprechend geändert.

Vereine III: Veröffentlichungen von Fotos eines Vereinsmitglieds

An einem Gebäude wurden großformatige Fotos eines Vereinsmitglieds zu Werbezwecken angebracht. Die Fotos entstanden im Zusammenhang mit einem Fotoshooting, zu dem verschiedene Mitglieder zu Werbezwecken posierten. Die betroffene Beschwerdeführerin wollte, dass Ihre Fotos von dem Gebäude entfernt werden. Trotz Aufforderung an die dafür zuständige Stelle des Vereins wurden die Fotos jedoch nicht entfernt.

Im Hinblick auf die Verarbeitung zu Werbezwecken war der Verein als für den Datenschutz Verantwortlicher heranzuziehen. Jegliche Verwendung personenbezogener Daten (Art. 4 Nr. 2 DS-GVO) setzt eine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO voraus. Hier kam nur eine Einwilligung in Frage. Die Einwilligung muss hierbei freiwillig, gut informiert und mit Hinweis auf den jederzeitigen Widerruf eingeholt werden (vgl. Art. 7 DS-GVO). Der verantwortliche Verein hatte nachzuweisen, dass die Beschwerdeführerin in die Verarbeitung ihrer personenbezogenen Daten (speziell zur Veröffentlichung ihrer Fotos an dem Gebäude) eingewilligt hatte, vgl. Art. 7 Abs. 1 DS-GVO. Art. 7 DS-GVO schreibt allerdings keine bestimmte Form für die Einwilligung vor. Somit ist grundsätzlich nach der DS-GVO auch eine mündliche erteilte Einwilligung denkbar. Hiervon ist allerdings mit Blick auf die Transparenz der Verarbeitung sowie die fehlende Möglichkeit des Nachweises abzuraten. Möglicherweise lag eine mündliche Einwilligung zu Fotoaufnahmen und deren Veröffentlichung seitens der Beschwerdeführerin vor. Dies konnte der verantwortliche Verein jedoch nicht nachweisen.

Selbst wenn eine Einwilligung vorgelegen hätte, hätte diese jederzeit, ohne die Angabe von Gründen, widerrufen werden können. Das hätte für den Verein dann auch die Pflicht zur Entfernung der Fotos zur Folge gehabt. Bei der rechtmäßigen Veröffentlichung der Fotos an dem Gebäude sind u. a. auch die Gründe entscheidend, inwiefern die Beschwerdeführerin mit einer Veröffentlichung genau an dieser Stelle zu rechnen hatte. Da sie allein durch entsprechendes Posieren zu den Fotoaufnahmen von einer Veröffentlichung auszugehen hatte, blieb zudem auch der Umfang der Veröffentlichung umstritten. Es muss deshalb möglichst konkret festgehalten und auch darüber informiert werden (Art. 13 Abs. 2 DS-GVO), wie, in welcher Form, an welcher Stelle und in welchen Medien die Veröffentlichungen (jeweils) geplant sind. Eine Rechtsgrundlage für die Fotoaufnahmen sowie das Vorliegen der Informationen nach Art. 13 DS-GVO konnte der Verantwortliche nicht nachweisen. Nach unserer Anfrage wurde daher die Entfernung der Fotos am Gebäude alsbald in Auftrag gegeben.

Vereinsmitglieder sind über Datenverarbeitungen – insbesondere Fotoaufnahmen – nach Artikel 13 DS-GVO zu informieren. Informiert der Verantwortliche transparent und umfassend über die geplanten Veröffentlichungen, geht die Erwartung der betroffenen Person in aller Regel auch dahin, dass ihre Fotos an der angekündigten Stelle unter den genannten Bedingungen veröffentlicht werden.

Vereine IV: Der Gewinner als Verlierer – die Veröffentlichung von Spenden-Daten

Anfang des Jahres 2020 erhielt ein Förderverein eine Spende für einen guten Zweck. Der Spender konnte daraufhin nicht nur seinen Namen der Presse entnehmen, sondern dort gleich auch die Höhe seines gespendeten Beitrags ersehen. Eine Einwilligung zu dieser Veröffentlichung hatte er nicht erteilt. Auf seine Anfrage beim Verein erhielt er vielmehr den Hinweis, dass er als Privatspender ja an einer Gewinnverlosung teilgenommen habe. Der Wunsch auf anonyme Bearbeitung hätte auf dem Überweisungsträger vermerkt werden müssen.

Die Teilnahmebedingungen für die Gewinn-Auslosung informierten dann tatsächlich auch darüber, dass sich der Gewinner – eines durchaus attraktiven Gewinns – automatisch mit der Veröffentlichung seiner Daten einverstanden erkläre. Dort war auch ausgeführt, was im Einzelnen veröffentlicht wird, nämlich der Name des Gewinners, sein Foto, die Berichterstattung über die Gewinnübergabe sowie die Medien, in denen die Veröffentlichungen stattfinden. Der Spender bezog diese Informationen folgerichtig auf den Fall seines Gewinns und nicht auf den Fall seiner Spende. Ein Spenden-Fall war jedoch noch lange kein Gewinner-Fall.

Die uns dann vom Verein übersandten Teilnahmebedingungen, die über deren Website abrufbar waren, unterschieden sich von den Teilnahmebedingungen, die uns der Beschwerdeführer vorlegte. Dort wurde dann noch ausdrücklich ausgeführt, dass die Spenderdaten als solche veröffentlicht würden, falls nicht auf der Überweisung (zur Spende) widersprochen würde. Gemeinsam war den Bedingungen jedoch die Koppelung der Veröffentlichung der personenbezogenen Daten des Spenders (soweit er ein tatsächlicher Gewinner ist) mit der (automatischen) Veröffentlichung der personenbezogenen Daten des Teilnehmers als Spender (ohne Gewinner zu sein). Dabei ließ der Verein „großzügig“ offen, welche Daten denn im Einzelnen vom Spender veröffentlicht würden. Mit einer ausdrücklichen und informierten Einwilligung nach Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO hatte dies alles wenig zu tun.

Als Rechtsgrundlage für eine Veröffentlichung der Spenderdaten des Beschwerdeführers wird in der Antwort auf unsere Rückfrage beim Verantwortlichen Art. 6 Abs. 1 Satz 1 Buchstabe a) DS-GVO genannt. Im Folgenden bezieht sich der Verein auf die Teilnahmebedingungen zur Gewinn-Verlosung und koppelt diese mit der Verarbeitung der Spenderdaten. Beabsichtigt der Verantwortliche jedoch, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als zu dem, für den die personenbezogenen Daten vorgesehen waren (hier die Datenverarbeitung zum Zwecke der Spende), so hat er der betroffenen Person vor dieser Weiterverarbeitung alle erforderlichen Informationen über diesen anderen Zweck (hier die Datenverarbeitung zum Zwecke der Gewinnspielteilnahme) und alle anderen maßgeblichen Informationen zur Verfügung zu stellen, vgl. Art. 13 DS-GVO. Eine Einwilligung hat dann separat zu den verschiedenen Zwecken zu erfolgen.

Es wurde daher nicht ausreichend über eine Datenverarbeitung zu den jeweiligen Zwecken gem. Art. 13 DS-GVO informiert. Außerdem dürfen nicht automatisch so verschiedene Zwecke miteinander gekoppelt werden. Vielmehr ist eine jeweils separate Einwilligungserklärung erforderlich. Die vom Verein verwendeten Teilnahmebedingungen für das Gewinnspiel durften auch nicht als konkludente Einwilligungserklärungen zur Veröffentlichung der Spenderdaten herangezogen werden. Leider konnte dies erst durch die Hinzuziehung unserer Behörde aufgeklärt werden. Aber jetzt sollte die Rechtslage allen Beteiligten klar sein.

© gustavofrazao – stock.adobe.com

... manchmal nur der Veranstalter eines Gewinnspiels.

11. Einblick in die Dienststelle

Der Informationsbedarf bei datenschutzrechtlichen Themen ist sehr hoch. Die digitale Transformation der Gesellschaft findet nicht im luftleeren Raum statt. Sie betrifft fast alle Lebensbereiche. Bürger_innen, öffentliche Stellen, Unternehmen, Verbände und Vereine sind unmittelbar betroffen und gestalten die digitale Welt aktiv mit. Digitalisierung und Datenschutz gehören zusammen, das eine funktioniert ohne das andere nicht. So eindeutig, wie Digitalisierung den Alltag bestimmt, so eindeutig ist es, dass der Umgang mit personenbezogenen Daten gut zu regeln und gut umzusetzen ist.

Die DS GVO beschreibt ein modernes Bürgerrecht: Bürger_innen entscheiden selbstbestimmt über die Art und Weise der Verwendung ihrer personenbezogenen Daten. Sie sind es, die darüber befinden, ob und wie zum Beispiel Unternehmen ihre Daten verarbeiten. Es ist die Aufgabe von öffentlichen Stellen, die Bürger_innen dazu zu befähigen, ihre Rechte auch tatsächlich wahrnehmen zu können. Unsere Aufgabe ist es, dem Bürgerrecht Datenschutz Geltung zu verschaffen. Neben der Beratung, Kontrolle, Prüfung und gegebenenfalls Sanktionen bei datenschutzrechtlichen Verstößen informieren wir umfangreich über das Bürgerrecht Datenschutz und beteiligen uns an Debatten und Diskursen zu rechtlichen, ethischen und kulturellen Fragen des Datenschutzes. Um das wirksam zu leisten nutzen wir unterschiedliche Kanäle: Wir organisieren in Eigenregie oder in Kooperationen Veranstaltungen, bringen als Referent_innen und Autoren Fachlichkeit in den Diskurs ein. Wir bieten auf unserer Homepage eine Vielzahl von Informationen und Praxishilfen an, nutzen Podcasts und Videos zur Vermittlung, unser Newsletter interessiert rund 4.500 Abonnenten. Zuletzt haben wir mit unserem eigenen Mastodon-Account wieder den direkten Kontakt zu interessierten Nutzer_innen der Sozialen Medien aufgenommen und suchen aktiv den Austausch. Wir werden unsere Arbeit intensivieren, unsere Gesprächsformate stärken und auch unser Bildungszentrum weiter fördern, welches hervorragende Arbeit leistet und sehr viel Wissen vermittelt.

>> Weitere Informationen
https://bawü.social/@lfdi
https://www.baden-wuerttemberg.datenschutz.de

Die Homepage wächst und gedeiht.

Auswirkungen der Corona-Pandemie auf den Behördenbetrieb

Frühzeitig haben im Frühjahr des Jahres Maßnahmen ergriffen, um die Beschäftigten vor möglichen Infektionen zu schützen und dadurch auch den Dienstbetrieb weiterhin weitestgehend aufrechterhalten zu können. Wir haben Schutzmasken beschafft und Hygienekonzepte erarbeitet und fortgeschrieben. In engem Austausch mit den Führungskräften des Hauses haben wir unser Vorgehen kontinuierlich angepasst. Allen, insbesondere denjenigen Beschäftigten, die zu den Risikogruppen zählen, haben wir nahegelegt, nur noch dann das Dienstgebäude aufzusuchen, wenn dies zwingend erforderlich sei. Alle Möglichkeiten des Homeoffice sollten genutzt werden, wobei dies zunächst in erster Linie diejenigen betraf, die ohnehin schon Telearbeitsvereinbarungen abgeschlossen hatten und deshalb bereits im Besitz der nötigen technischen Ausstattung waren. Unter erheblichen organisatorischen und finanziellen Anstrengungen gelang es dann nach und nach, alle Mitarbeitenden entsprechend auszurüsten, so dass, angefangen bei der Post-

stelle, über Schreibdienst und Registratur bis hin zu den Abteilungsleitungen mittlerweile alle von Zuhause arbeiten können. Dabei hat sich gezeigt, dass das Arbeiten im Homeoffice reibungslos funktioniert und der Dienstbetrieb quantitativ und qualitativ auf dem gewohnt hohen Niveau weitergeführt werden konnte.

Eine besondere Herausforderung stellte allerdings die Eingliederung und Einarbeitung der vielen neu in der Behörde hinzugekommenen Kolleg_innen dar. Dass dies angesichts der Abwesenheit des größten Teils der Mitarbeiterschaft nicht ganz einfach war, liegt auf der Hand. Durch den verstärkten Einsatz technischer Möglichkeiten, wie Online-Schulungen und virtuelle Mitarbeiter- und Abteilungsbesprechungen, können die Nachteile zwar auch insoweit gemildert werden. Gleichwohl hätten wir den Betroffenen einen günstigeren Einstand gewünscht. Hier hoffen wir auf die Geduld der „Neuen" und darauf, dass die Zeiten besser werden.

Alle getroffenen Maßnahmen, gepaart mit der Disziplin der Mitarbeitenden und dem notwendigen Quäntchen Glück, haben dazu geführt, dass bisher niemand von einer Infektion betroffen wurde. Es bleibt zu hoffen, dass es weiterhin so bleibt.

Besetzung der Neustellen

Im Jahr 2020 haben wir 10 neue Planstellen besetzt. Wir hatten keine Schwierigkeiten qualifiziertes Personal zu finden. Die Themen Datenschutz und Informationsfreiheit sind mittlerweile als Zukunftsthemen erkannt. Unsere Behörde gilt als attraktive Arbeitgeberin. Nicht zuletzt trägt das sich in den letzten Jahren gewandelte Image, weg von einer reinen Aufsichts- und hin zu einer modernen Dienstleistungsbehörde mit einem frischen Internetauftritt und einem dynamischen Team, hierzu bei. Unsere Expert_innen im Haus sind auch sehr gefragte Referent_innen. Auch andere Landesbehörden haben mittlerweile erkannt, dass es sich lohnen kann, Kolleg_innen zu beschäftigen, die für eine gewisse Zeit beim Landesbeauftragten gearbeitet haben. Hiervon zeugt, dass es gelang, etliche Beschäftigte in die Innenverwaltung, in die Gerichtsbarkeit oder in Bundesministerien zu vermitteln. Wir hoffen, diesen Weg weiter beschreiten zu können – gewinnbringend für alle Seiten.

Vorbereitung Umzug

Schon in den vergangenen Jahren wurden wir vom Parlament dankenswerterweise mit neuen Personalstellen bedacht. Diese konnten wir angesichts der

© LfDI BW

Im Monty-Python-Stil animiert und gern gesehen: Das Video „Digitalisierung und Datenschutz gehören zusammen".

gestiegenen Anforderungen an unsere Behörde auch gut einsetzen. Dabei zeigte sich aber rasch, dass wir hinsichtlich der räumlichen Gegebenheiten am bisherigen Standort zunehmend an die Grenze dessen stoßen, was den Beschäftigten noch zumutbar ist. Doppel- und Dreifachbelegungen der Dienstzimmer sind mittlerweile der Regelfall. Insbesondere auch mit Blick auf die unter Corona-Bedingungen erforderlichen Hygienestandards wurde dies zunehmend zu einer Belastung. Erfreulicherweise konnte uns der Landesbetrieb Vermögen und Bau, dem an dieser Stelle ausdrücklich für seine professionelle Arbeit gedankt wird, Ersatzräumlichkeiten anbieten, die alle unsere Bedürfnisse optimal erfüllen. So ist das neue Domizil nicht nur verkehrstechnisch bestens erreichbar, was den Beschäftigten wie auch Besuchern entgegenkommt. Die Räumlichkeiten bieten dem neu gegründeten Bildungszentrum BIDIB auch beste Rahmenbedingungen für erfolgreiche Schulungs- und Fortbildungsmaßnahmen rund um die Themen Datenschutz und Informationsfreiheit. Eigentlich wollten wir damit bereits im Jahr 2020 beginnen. Leider verzögerte sich der Umzug allerdings um circa ein Jahr gegenüber der ursprünglichen Planung, weil der Vormieter die Räumlichkeiten doch lieber selbst behalten wollte. Es kostete einige Mühe und intensive Gespräche mit den Verantwortlichen, um dann doch die – verspätete – Räumung zu erreichen. Nun kann es mit den Sanierungsarbeiten endlich losgehen und wir sehen dem Einzug im zweiten Quartal 2021 mit Ungeduld und Vorfreude entgegen.

Mobiles Arbeiten

Als „Stuttgarter" Behörde sind wir zufrieden damit, nicht nur Kolleg_innen aus dem Schwäbischen zu beschäftigen, sondern auch solche aus weiter entfernten Landesteilen oder gar aus anderen Ländern Deutschlands. Diese Kolleg_innen nehmen den mühevollen Weg auf sich, Tag für Tag mit öffentlichen Verkehrsmitteln, meist mit IC oder ICE, anzureisen. Bedingt durch die Sanierung der Bahnstrecke von Mannheim nach Stuttgart verdoppelte sich die einfache Fahrzeit für cirka ein halbes Jahr auf rund eineinhalb Stunden. Um den Betroffenen hier entgegenzukommen, wurde als neue Arbeitsform das ‚mobile Arbeiten' eingeführt. So konnte die Zeit der Zugfahrt genutzt werden, um zu arbeiten und dadurch die zeitliche Belastung durch die längere An- und Abreise etwas zu mildern. Aus den Erfahrungen hiermit und den Erfahrungen mit dem Homeoffice bedingt durch die Corona-Pandemie hat sich gezeigt, dass diese modernen Formen des Arbeitens durchaus auch für andere Beschäftigte geeignet sein kann. Gemeinsam mit dem Personalrat sind wir derzeit dabei, hier eine Dienstvereinbarung zu erarbeiten, welche die Vorzüge dieser Arbeitsform allen Beschäftigten zugutekommen lässt.

Zahlenüberblick

Nach der langen Phase der Einführung und Etablierung der DS-GVO durch intensive Beratungen von Behörden, Unternehmen, Vereinen und Initiativen sind wir im Jahr 2019 dazu übergegangen, wieder verstärkt zu prüfen und zu kontrollieren. Diese Kontrolltätigkeit nahm pandemiebedingt im Jahre 2020 erheblich ab. Die Zahl der Datenpannenmeldungen und Beschwerden hingegen stieg deutlich. Auch wurden wieder etliche Bußgeldverfahren durchgeführt. Insgesamt haben wir im Jahr 2020 Bußgelder in Höhe von rund 1,6 Millionen Euro verhängt, so viel wie noch nie. Die Zahl der Beschwerden steigt von rund 3570 im Jahr 2019 auf über 4500 im Jahr 2020. Die Zahl der Datenpannenmeldungen stieg im Vergleich zum Vorjahreszeitraum, in dem wir einen enormen Anstieg an Meldungen feststellten, noch einmal um rund 300. Beratungsanfragen reduzierten sich hingegen um rund 550. Die Zahl der Kontrollen sank von über 110 im Jahr 2019 auf etwas über 30 im Berichtszeitraum.

Der Überblick über die Entwicklungen der wesentlichen Kennzahlen unserer Behörde zeigt, dass der Datenschutz sehr große Beachtung erfährt. Wir haben erst mit Wirksamwerden der DS-GVO im Mai 2018 die Kompetenz zur Verfolgung von Datenschutzbußgeldverfahren erhalten. In den Jahren 2016 und 2017 wurden die Bußgeldverfahren noch von der zentralen Bußgeldstelle des Regierungspräsidiums Karlsruhe verfolgt. Auskunft über die Zahlen aus den Jahren 2016 und 2017 haben wir vom Regierungspräsidium nicht erhalten.

Auch im Jahr 2020 haben wir – coronabedingt unter verschärften Bedingungen – Veranstaltungen organisiert und als Referent_innen Vorträge gehalten und an Podiumsdiskussionen teilgenommen. Unser im Juli eröffnetes Bildungszentrum musste alle geplanten Präsenz-Veranstaltungen absagen. Leider war es nicht möglich, alle vorgesehenen Themen stattdessen online anzubieten. Die vier Veranstaltungen, die wir online durchführen konnten, erfreuten sich allerdings großer Nachfrage: Innerhalb weniger Tage nach

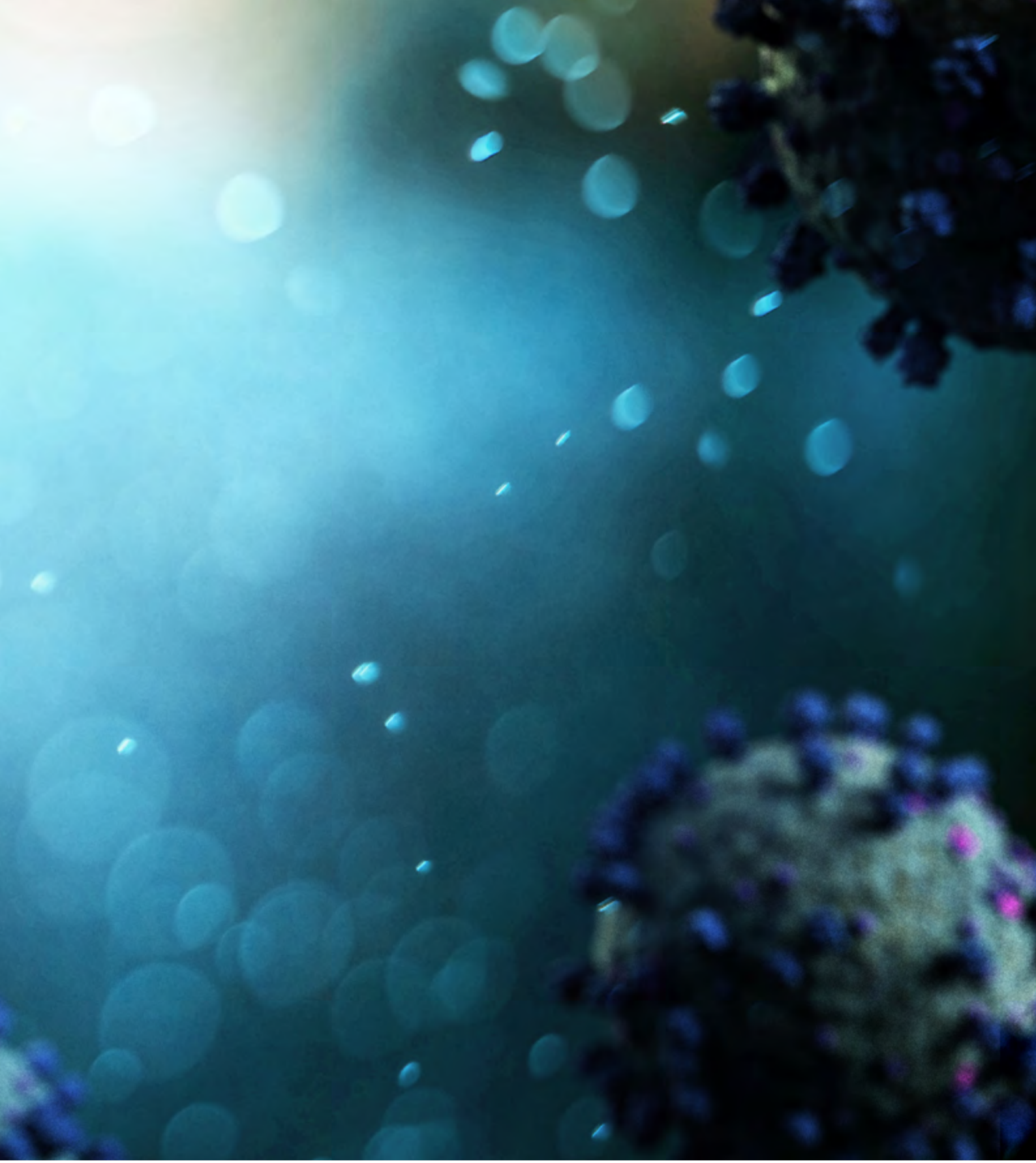
der Ankündigung waren sie komplett ausgebucht. Das zeigt uns für die Zukunft, dass wir mit dem BIDIB auf einem sehr guten Weg sind und auf große Nachfrage stoßen. Von Teilnehmenden, aber auch von anderer Stelle, wie zum Beispiel von Nutzer_innen auf unserem Social Media Kanal Mastodon, haben wir viele Themenvorschläge für Veranstaltungen erhalten. Wir freuen uns über die zahlreichen Anregungen und werden bei der Planung für das Veranstaltungsjahr 2021 versuchen, möglichst viele davon umzusetzen. Auch wurden wir als Referent_innen für (online-) Veranstaltungen anderer Institutionen angefragt, über den Datenschutz und die Informationsfreiheit zu sprechen und somit wichtige Aufklärungsarbeit zu leisten.

Insgesamt haben wir 95 Vorträge gehalten – weniger als im Jahr zuvor, im dem allein unsere Stabstelle rund 40 Mal in Schulungen aktiv war – und als Gesprächspartner an Diskussionen teilgenommen. Von Vorträgen zu Kinderrechten, der Teilnahme als Kunstprojekten, Debatten zu ethischen Fragen bis hin zu Gesprächen mit öffentliche Stellen, Unternehmen, Verbänden, Vereinen sowie unmittelbar und direkt mit der Bürgerschaft: Wir haben für das Bürgerrecht auf Datenschutz und die Freiheit des Zugangs zu amtlichen Informationen sensibilisiert und gestritten. Im Jahr 2021 wollen wir unsere Veranstaltungsformate weiter ausbauen – dann auch hoffentlich wieder in der ersehnten gemeinsamen Präsenz von Referent_innen und Teilnehmenden.

Statistische Übersicht – Zeitraum jeweils vom 01.01. – 31.12.

	2016	2017	2018	2019	2020
Beschwerden	2.048	3.058	3.902	3.757	4.782
Kontrollen	16	55	13	111	31
Beratungen [1]	1.515	1.786	4.440	3.842	3.285
Datenpannen	68	121	900	2.030	2.321
Bußgeldverfahren (eingeleitet)	-	-	138 [2]	233	174

[1] ohne telefonische Beratung
[2] Mai – Dez



© Production Perig – stock.adobe.com

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg